به نام خدا

سایبرنو تقدیم می‌کند!

نحوه نفوذ هکرها به سازمان شما

ارائه دهنده

مهندس علیرضا یوسف‌زاده

سایبرنو
Cyberno

جلسه دوم

آموزش نحوه نفوذ و تکنیک‌های افزایش سطح دسترسی در امنیت سایبری

این وبینار ضبط می‌شود و پس از پایان جلسه، از طریق پنل ایسمینار در دسترس شما خواهد بود.

پس از اتمام وبینار، فایل جلسه را می‌توانید از کانال تلگرام ما دریافت کنید.

Cyberno

smart security for smart people

مقدمه:

در دنیای امروز که فناوری‌های دیجیتال به ستون اصلی فعالیت سازمان ذها تبدیل شدهاند،

امنیت سایبری به یکی از چالش‌های حیاتی تبدیل شده است. هکرها با استفاده از روش‌های پیچیده و ابزارهای پیشرفته، تلاش میکنند تا از نقاط ضعف سیستم‌ها سوءاستفاده کرده و به شبکه‌های سازمانی نفوذ کنند. در این جلسه، به بررسی مراحل اولیه نفوذ (از جمله فیشینگ، سوءاستفاده از آسیب‌پذیری‌ها و مهندسی اجتماعی) و همچنین افزایش سطح دسترسی در سیستم‌های هدف میپردازیم. هدف این است که با شناخت تکنیک‌های مورد استفاده مهاجمان، راهکارهای دفاعی موثرتری طراحی شود. این آموزش به شما کمک میکند تا درک بهتری از مکانیزم‌های نفوذ داشته باشید.

سناریوهای مورد بررسی:

استفاده از بد افزار و دسترسی کامل به موبایل

نفوذ از طریق فیشینگ و تصاحب حساب کاربران

نفوذ از طریق وب اپلیکیشن (Initial access)

افزایش سطح دسترسی (Privilege Escalation)

حرکت جانبی (Lateral movement)

حملات فیزیکی (bad usb)

RAT چیست و چه میکند؟

RAT یا ابزار دسترسی از راه دور نرم افزاری مخرب است که به مهاجمان اجازه میدهد دستگاه قربانی را از راه دور کنترل کنند، داده‌ها را سرقت کنند (مثل SMS ، عکس‌ها، موقعیت جغرافیایی) و دستورات مخرب (فعالسازی دوربین/میکروفون) اجرا نمایند.

RATهای اندروید چگونه کار میکنند؟

با نصب APK جعلی (مثلاً به عنوان برنامه کاربردی)، دسترسی‌های گسترده (دوربین، حافظه، موقعیت) میگیرند و از طریق ارتباط Real-Timeبا سرور مهاجم (با فناوری‌هایی مثل socket.io داده‌ها را ارسال و دستورات را دریافت میکنند.

فیشینگ نوعی حمله سایبری است که کلاهبرداران با جعل هویت سازمان‌های معتبر (مثل بانک‌ها یا شرکت‌ها)، از طریق ایمیل، پیامک یا سایت‌های جعلی، سعی در دزدیدن اطلاعات حساس مانند رمز عبور یا شماره کارت دارند.

نمونه‌های بزرگ:

۱. حمله به کمپین هیلاری کلینتون (۲۰۱۶)

۲. نفوذ به سونی پیکچرز و سرقت داده‌ها (۲۰۱۴)

۳. کلاهبرداری ۱۰۰ میلیون دلاری از گوگل و فیسبوک (۲۰۱۳-۲۰۱۵)

راه مقابله: همیشه آدرس‌ها را چک کنید، روی لینک‌های ناشناس کلیک نکنید و از احراز هویت دو مرحله‌ای استفاده کنید. 🚨

نفوذ از طریق وب اپلیکیشن (Initial access):

1. نفوذ از طریق وب‌اپلیکیشن یکی از رایج‌ترین روش‌های حمله سایبری است که مهاجمان از آسیب‌پذیری‌های امنیتی در برنامه‌های تحت وب سوءاستفاده می‌کنند.
2. پس از نفوذ، مهاجمان می‌توانند به داده‌های حساس دسترسی پیدا کنند، سیستم را کنترل کنند یا بدافزار نصب نمایند.
3. پیشگیری از این حملات نیازمند استفاده از کدنویسی ایمن، تست نفوذ منظم و به‌روزرسانی مستمر سیستم‌ها است.

:Privilege escalation

۱. Privilege Escalation یعنی هکر بعد از نفوذ اولیه، از باگ‌های سیستم سوءاستفاده می‌کند تا دسترسی‌های بیشتری بگیرد مثلاً از یک کاربر معمولی به ادمین سیستم تبدیل شود.

۲. این کار با سوءاستفاده از تنظیمات غلط، آسیب‌پذیری‌های نرم‌افزاری، یا کلمات عبور ضعیف انجام می‌شود مثل اجرای کد مخرب روی یک سرویس با دسترسی بالا.

۳. نتیجه آن دسترسی کامل به سیستم است هکر می‌تواند داده‌ها را پاک کند، نرم‌افزار نصب کند، یا حتی کل شبکه را آلوده کند.

۴. شناسایی و جلوگیری از آن سخت است چون حمله شبیه فعالیت‌های عادی کاربران ادمین به نظر می‌رسد!

Lateral movement:

۱. حرکت جانبی Lateral Movement تکنیکی است که هکرها پس از نفوذ اولیه، برای جابجایی بین سیستم‌ها و حساب‌های کاربری در یک شبکه استفاده می‌کنند.

۲. هدف آن دستیابی به دسترسی بالاتر (مانند ادمین) و کنترل منابع بیشتر است، اغلب با سوءاستفاده از اعتبارهای سرقت‌شده یا آسیب‌پذیری‌های شبکه.

۳. این تکنیک باعث گسترش حمله به کل شبکه می‌شود و شناسایی آن را سخت می‌کند، چون هکر خود را به شکل کاربران یا سیستم‌های مجاز جا می‌زند.

: BadUSB

۱. حمله با سخت‌افزار مخرب: بدیوسبی BadUSB یک دستگاه USBمعمولی (مثل فلش) است که با کد مخرب برنامه‌ریزی شده تا سیستم قربانی را فریب دهد.

۲. شبیه‌سازی دستگاه‌های مجاز: می‌تواند خود را به عنوان کیبورد، ماوس یا حافظه جانبی معرفی کند و دستورات مخرب را اجرا کند.

۳. اجرای خودکار حملات: با اتصال به کامپیوتر، بدون نیاز به تعامل کاربر، می‌تواند بدافزار نصب کند، داده‌ها را سرقت کند یا سیستم را قفل نماید.

۴. خطرناک و غیرقابل تشخیص: از آنجا که در سطح سخت‌افزار عمل می‌کند، اغلب توسط آنتی‌ویروس‌ها شناسایی نمی‌شود و یک تهدید جدی برای امنیت سایبری است.

پایان!

Cyberno

smart security for smart people

با ما در ارتباط باشید

تهران، میدان رسالت، خیابان فرجام، خیابان شهید حسینعلی، پلاک ۹

۰۲۱۹۱۰۹۴۳۳۰ ۰۲۱۷۷۲۴۳۸۲۹ info@cyberno.ir