# WINDOWS INCIDENT RESPONSE

packetlife.net

## COMMAND LINE CHEAT SHEET

## General System Information

### Capturing the Date and Time

```
date /t
time /t
```

### View System Information and Variables

```
ver
systeminfo
set
```

### View Tasks, Processes, and Startup Items

```
tasklist /svc
schtasks
wmic startup list full
wmic process list full
```

### Enumerate Drivers

```
driverquery
driverquery /SI
```

### Query the Registry

```
reg query <reg key>
```

### View Files, Folders, and Attributes

```
tree /F /A <drive>
wmic fsdir where name=”<drive>:\\<folder>”
wmic datafile where name=”<drive>:\\<folder>\\<file>”
```

### Enumerate Local User Accounts and Groups

```
net user
net localgroup
net localgroup <group>
```

### Enumerating sessions, shares, mapped drives

```
net session
net share
net use
```

### Enumerating Windows Services

```
net start
sc query
sc query <service>
sc queryex state= all
```

## Misc

### Output/Append Results to a File

```
>> path\filename
```

### Query Potential Results

```
| find "<searchstring>"
```

## Networking Information

### General Networking

```
ipconfig /all
netsh int ip show config
```

### Display the Client DNS Cache

```
Ipconfig /displaydns
```

### Enumeration of the Hosts File

```
type %systemroot%\system32\drivers\etc\hosts
```

### Enumerating the NetBIOS name cache

```
nbtstat -c
```

### ARP Table Enumeration

```
arp -a
```

### DNS Forward/Reverse Lookup

```
nslookup <IP or HOSTNAME>
```

### Display the Routing Table

```
route print
netstat -r
```

### Show Windows Firewall Status

```
netsh firewall show state
netsh advfirewall show allprofiles
```

### View Network Connections (including PID and/or EXE)

```
netstat -nao
netstat -naob
```

## Using WMIC Query Language

### List the Aliases

```
wmic /?
```

### List the Attributes

```
wmic <alias> get /?
```

### List the Verb Clauses

```
Wmic <alias> /?
```

## WMIC Query Examples

```
WMIC FSDIR WHERE Name="c:\\WINDOWS"

WMIC DATAFILE WHERE Name="c:\\boot.ini"

WMIC DATAFILE WHERE "Path='\\windows\\' and
Extension='exe' and FileSize>'108032'" GET LastAccessed,
LastModified, Name, FileSize

WMIC PROCESS WHERE Name='explorer.exe' list brief
```

by Tim Mugherini