University of South Wales: Cyber University of the Year: 2019
Information Security, Privacy, Encryption, GDPR

TAGS

hacking cheat sheet

Penetration Testing Tools Cheat Sheet

25/06/2016
https://highon.coffee/blog/penetration-testing-tools-cheat-sheet/ (https://highon.coffee/blog/penetration-testing-tools-cheat-sheet/)

SMB enumeration

Also see, **nbtscan cheat sheet (https://highon.coffee/blog/nbtscan-cheat-sheet/)**.

COMMAND	DESCRIPTION
`nbtscan 192.168.1.0/24`	Discover Windows / Samba servers on subnet, finds Windows MAC addresses, netbios name and discover client workgroup / domain
`enum4linux -a target-ip`	Do Everything, runs all options (find windows client domain / workgroup) apart from dictionary based share name guessing

Other Host Discovery

Other methods of host discovery, that don’t use nmap…

COMMAND	DESCRIPTION
`netdiscover -r 192.168.1.0/24`	Discovers IP, MAC Address and MAC vendor on the subnet from ARP, helpful for confirming you’re on the right VLAN at $client site

SMB Enumeration

Enumerate Windows shares / Samba shares.

COMMAND	DESCRIPTION

COMMAND	DESCRIPTION
`nbtscan 192.168.1.0/24`	Discover Windows / Samba servers on subnet, finds Windows MAC addresses, netbios name and discover client workgroup / domain
`enum4linux -a target-ip`	Do Everything, runs all options (find windows client domain / workgroup) apart from dictionary based share name guessing

Python Local Web Server

Python local web server command, handy for serving up shells and exploits on an attacking machine.

COMMAND	DESCRIPTION
`python -m SimpleHTTPServer 80`	Run a basic http server, great for serving up shells etc

Mounting File Shares

How to mount NFS / CIFS, Windows and Linux file shares.

COMMAND	DESCRIPTION
`mount 192.168.1.1:/vol/share /mnt/nfs`	Mount NFS share to `/mnt/nfs`
`mount -t cifs -o username=user,password=pass,domain=blah //192.168.1.X/share-name /mnt/cifs`	Mount Windows CIFS / SMB share on Linux at `/mnt/cifs` if you remove password it will prompt on the CLI (more secure as it wont end up in bash_history)
`net use Z: \\win-server\share password /user:domain\janedoe /savecred /p:no`	Mount a Windows share on Windows from the command line
`apt-get install smb4k -y`	Install smb4k on Kali, useful Linux GUI for browsing SMB shares

Basic Finger Printing

Manual finger printing / banner grabbing.

COMMAND	DESCRIPTION
`nc -v 192.168.1.1 25` `telnet 192.168.1.1 25`	Basic versioning / finger printing via displayed banner

SNMP Enumeration

COMMAND	DESCRIPTION

`snmpcheck -t 192.168.1.X -c public`
`snmpwalk -c public -v1 192.168.1.X 1| grep hrSWRunName|cut -d* * -f`
`snmpenum -t 192.168.1.X`
`onesixtyone -c names -i hosts`
	SNMP enumeration

DNS Zone Transfers

COMMAND	DESCRIPTION
`nslookup -> set type=any -> ls -d blah.com`	Windows DNS zone transfer
`dig axfr blah.com @ns1.blah.com`	Linux DNS zone transfer

DNSRecon

DNS Enumeration Kali – DNSRecon

root:~# dnsrecon -d TARGET -D /usr/share/wordlists/dnsmap.txt -t std –xml ouput.xml

HTTP / HTTPS Webserver Enumeration

COMMAND	DESCRIPTION
`nikto -h 192.168.1.1`	Perform a nikto scan against target
`dirbuster`	Configure via GUI, CLI input doesn't work most of the time

Packet Inspection

COMMAND	DESCRIPTION
`tcpdump tcp port 80 -w output.pcap -i eth0`	tcpdump for port 80 on interface eth0, outputs to output.pcap

Username Enumeration

Some techniques used to remotely enumerate users on a target system.

SMB User Enumeration

COMMAND	DESCRIPTION
`python /usr/share/doc/python-impacket-doc/examples /samrdump.py 192.168.XXX.XXX`	Enumerate users from SMB
`ridenum.py 192.168.XXX.XXX 500 50000 dict.txt`	RID cycle SMB / enumerate users from SMB

SNMP User Enumeration

COMMAND	DESCRIPTION
`snmpwalk public -v1 192.168.X.XXX 1 |grep 77.1.2.25 |cut -d" " -f4`	Enmerate users from SNMP
`python /usr/share/doc/python-impacket-doc/examples/ samrdump.py SNMP 192.168.X.XXX`	Enmerate users from SNMP

COMMAND	DESCRIPTION
`nmap -sT -p 161 192.168.X.XXX/254 -oG snmp_results.txt (then grep)`	Search for SNMP servers with nmap, grepable output

Passwords

Wordlists

COMMAND	DESCRIPTION
`/usr/share/wordlists`	Kali word lists

Brute Forcing Services

Hydra FTP Brute Force

COMMAND	DESCRIPTION
`hydra -l USERNAME -P /usr/share/wordlistsnmap.lst -f 192.168.X.XXX ftp -V`	Hydra FTP brute force

Hydra POP3 Brute Force

COMMAND	DESCRIPTION
`hydra -l USERNAME -P /usr/share/wordlistsnmap.lst -f 192.168.X.XXX pop3 -V`	Hydra POP3 brute force

Hydra SMTP Brute Force

COMMAND	DESCRIPTION
`hydra -P /usr/share/wordlistsnmap.lst 192.168.X.XXX smtp -V`	Hydra SMTP brute force

Use `-t` to limit concurrent connections, example: `-t 15`

Password Cracking

John The Ripper – JTR

COMMAND	DESCRIPTION
`john --wordlist=/usr/share/wordlists/rockyou.txt hashes`	JTR password cracking
`john --format=descrypt --wordlist /usr/share/wordlists/rockyou.txt hash.txt`	JTR forced descrypt cracking with wordlist
`john --format=descrypt hash --show`	JTR forced descrypt brute force cracking

From → Brute Force Hacking, DNS, Hacking, KALI, Man in the Middle Attack, Uncategorized

Leave a Comment