Vulnerable Machine using Snapshots (WIP)

• Go through everything

• **Aim**:

To build a vulnerable virtual machine in the format of snapshots to educate students in the field of professional penetration testing. This would be similar to the cybersecurity capture the flag (CTF) standard. The aim of the snapshots is to teach skills and tools to break the final snapshot.

**Scope:**

* Snapshot 1 will be based around web exploitation. Ports 80/tcp and 443/tcp will be open. Web page with company details (think de-ice). Flag 1 is on a page on the site. Flag 2 is hidden in the source. Flag 3 is on the https website.
* Snapshot 2 is FTP exploitation. Port open will be 21. Flag 1 is anonymous login. Flag 2 is using Metasploit to exploit a version of ftp. Flag 3 is brute forcing ftp password.
* Snapshot 3 is SSH exploitation. Port open is 22. Flag 1 is in the banner. Flag 2 is Metasploit version attack. Flag 3 is bruteforce.
* 4 is Networking, based around the use of two tools (Burp & Wireshark). Port 80 is open. Flag 1 is using Burp. Flag 2 is wireshark.
* 5 is UDP scanning. There’ll be a hidden udp port open. Flag 1 is finding the ssh password (ssh is set to a random udp port). Flag 2 is in the machine somewhere.
* 6 is vuln scanners. OpenVAS is intended scanner, to find vulnerabilities. Misleading folders and files. Flags 1-4 are very similar (slight change to try and trick attacker that he may have the same flag). Flag 5 is hint for the next snapshot.
* 7 is hash breaking. Hashcat is intended tool. FTP and SSH are open, passwords are in rockyou. This links with snapshot 1’s website (it has names). Intended method is to break into user1 to get root’s username, and break into user3 to get root’s password. Flag 1 is in /root folder. Flag 2 is in user1 home folder. It is ciphered. Flag 3 is the same as flag 2, just that it is ciphered multiple times using different ciphers.

* 8 is reverse shell. Use Metasploit to open meterpreter shell on target. The flags are hidden all over machine. Each flag is a section of the complete flag.
* 9 is getting past the firewall (firewall exploitation). Chain is set to drop. 1st 1024 ports are closed (to throw off a nmap scan). Random high port is open. 4 flags are hidden all over machine.
* 10 is nightmare mode. Has all previous snapshots with no hints. Idea is to use knowledge gained from previous sections to break final machine. Flags are hidden all over.