Trademarkia Project

16.02.2023

—

Name:M.Karthikeyan
Reg No : 20BCE0145
College : Vellore Institute of technology
Course : computer science and engineering

Overview

Find faults in websites by using the well-liked penetration testing distro Kali Linux. An outline of the procedures required in using Kali Linux to detect flaws on a website like gathering information about the target website, such as its IP address, domain name, and the technologies it employs, is known as reconnaissance. Nmap, Whois, and Shodan are a few tools that may be used for this. Vulnerability scanning: After learning more about the website, you may check for vulnerabilities in the web server and web application using programmes like Nikto and OpenVAS.Exploitation: If vulnerabilities are discovered, you can access the website or the underlying server by using programmes like Metasploit and SQLmap to take advantage of them.Post-exploitation: Once you have acquired access to the server or website, you may carry out more attacks or gather more information using tools like Netcat and Wireshark.Reporting: It's crucial to keep track of your discoveries and let the right people know about them, such the website's owner or security team. This will strengthen the website's security and fend off potential threats.

Goals

1. To find bugs using kali linux mechanisms
2. Writing the document in terms of UAT guidlines.

Approach 1 : Using sqlmap

Scope of sqlmap:

An open-source programme called SQLmap is used in penetration testing to find and take advantage of SQL injection problems. The method of identifying and taking advantage of SQL injection is automated by SQLmap. Databases that use SQL can be taken over by SQL Injection attacks. They can impact any website or online application that might be connected to a SQL database, including MySQL, SQL Server, Oracle, and many more. Sensitive data including client information, personal information, trade secrets, financial information, and so on are

frequently found in these databases. It's crucial to be able to identify SQL issues and counter them. To detect these vulnerabilities, use SQLmap.

Explanation of commands used here

SQL injection using SQLmap

To update SQM map: *sudo apt install --only-upgrade sqlmap*

Basic cmds

#sqlmap -h

#sqlmap --h

Basic command structure is very simple. First you write **sqlmap** and then URL followed by specific wildcards of where you want the injection to occur.

#sqlmap -u "url"

Demo sites

https://trademarkia.com

This command will perform SQL injection on the target and report back if specified target is vulnerable or not. Assuming that target is vulnerable, all the possible SQL injection attacks will be listed for that target. In order to render out some information, first you need to get the list of available databases available at target machine.

#sqlmap -u "url" –dbs

#sqlmap -u http://testphp.vulnweb.com/ –dbs

–dbs option here will enlist all the available databases on the target machine if the target is vulnerable to SQL injection. Once you get the list of your databases, the next step is to get the list of all the tables of selected database.

#sqlmap -u "url" --tables -D database-namehere **–table** option is used to extract the list of all the tables in the selected database. -D option is used to specify the database name that you found out in the previous step. Next you need to enlist all the columns in the table.

#sqlmap -u "url" --columns -D database-name -T table-name

Now **–columns** option will tell the sqlmap to get the name of all the columns and additional -T argument is used to specify the table name from which you want to enlist all the columns.

Once you get the columns' name, either you can dump the whole columns' data into csv file from the database or you can dump the data from selected fields.

#sqlmap -u "url" --dump -D database -name -T table-name

Here this command will tell the sqlmap to dump all the data from the database-name where table table-name exists.

You can also dump the whole database by using following command

#sqlmap -u "url" --dump -D database-name

Check if current user is a database administrator

To see if the current user has root access to the database management system, issue the following command.

#sqlmap -u "url" -o -b --current-user --is-dba

If current user turns out be a root user you can extract the password for that user and all the other users. Use the following command.

#sqlmap -u "url" -v1 --current-user --password

SQLmap on multiple target list.

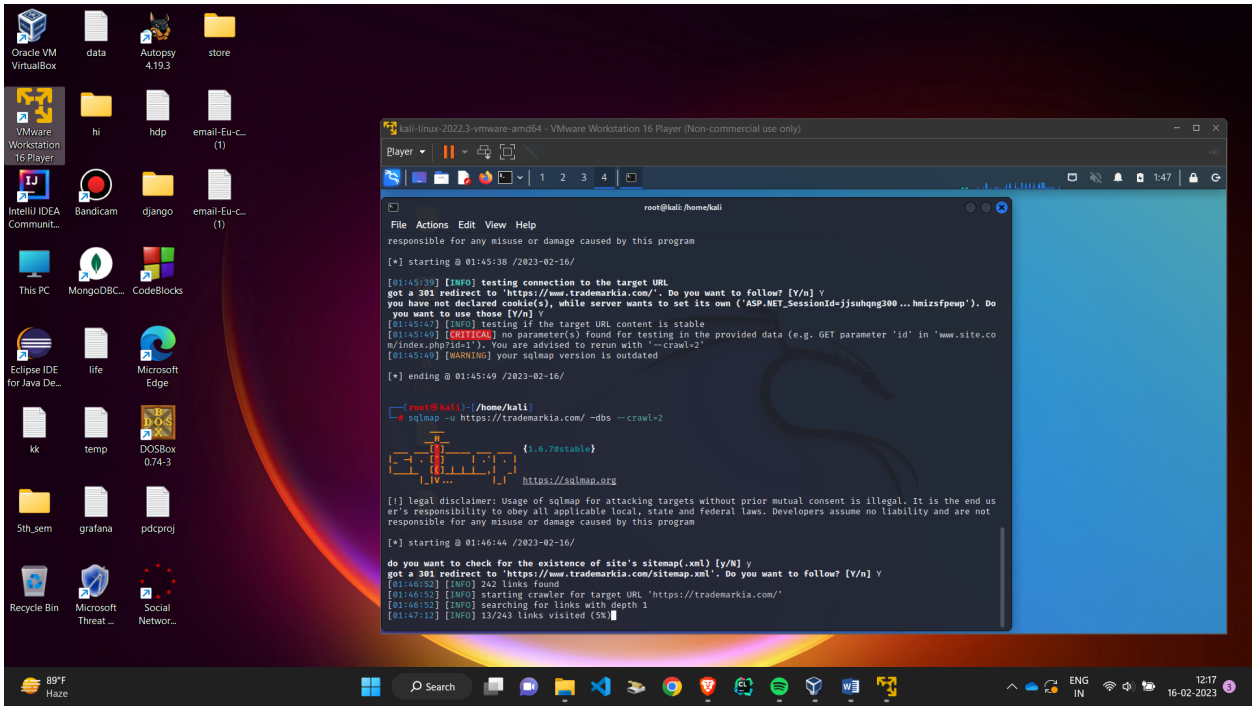
sqlmap is a very flexible tool. You can give it any number of target in a text file and it will test all the targets on time.

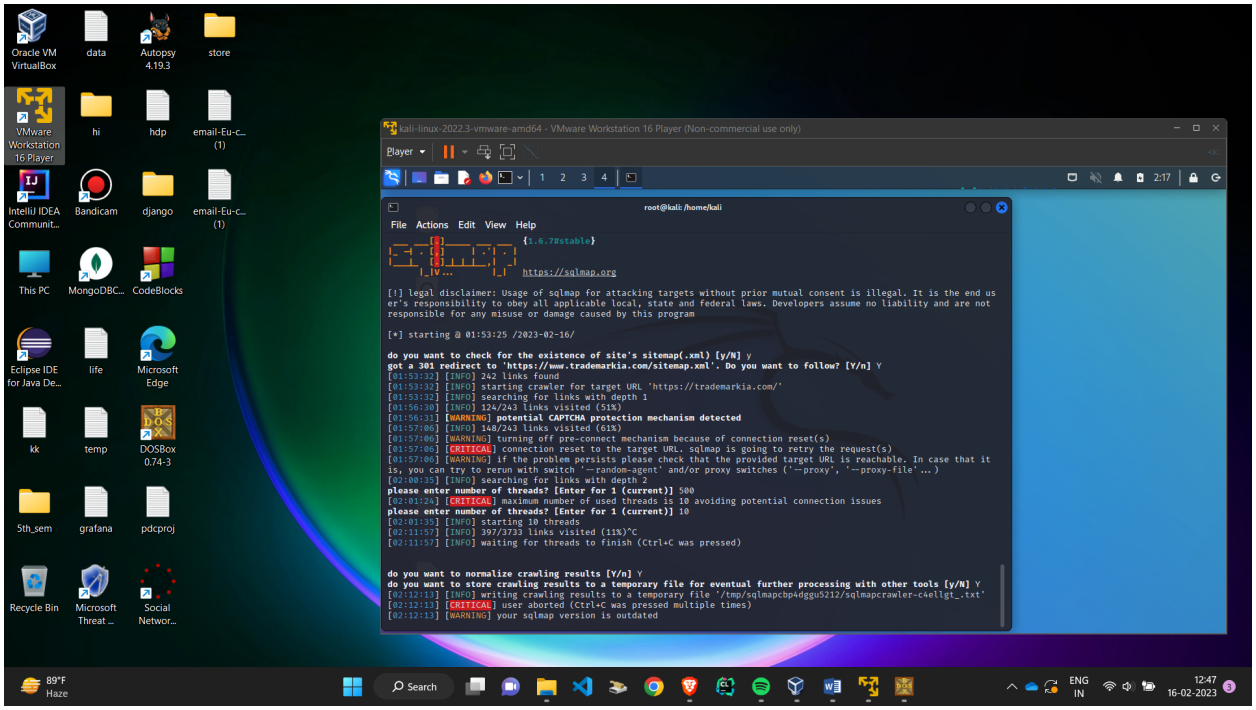
#sqlmap -m "path-to-file" --batch

here –batch option will process all the target with default options.

SQLmap also has password cracking capability. It can perform dictionary attack on the found hashes. Hash cracking process will take time according to your CPU power.

Methodology





Bug detected : database can be got if provided with multiple threads say 500 threads running at once on sqlmap leading to acquiring of database but as local machine machine supports only 10 threads and with ample internet speed we get possibilities of chances to acquire database and use above commands to become dba user

Environemnt used : sqlmap and kalilinux

Test cases : demo website here trademarkia.com

Criteria :

User input validation: SQL injection is frequently a problem for web programmes that do not adequately check user input. The application's input validation and susceptibility to SQL injection may both be tested using SQLMap.

Web applications may be vulnerable to SQL injection if they generate extensive error messages that include SQL syntax or other information that might be utilised to exploit SQL injection vulnerabilities.

HTTP response codes: SQLMap can determine whether a web application is providing particular HTTP response codes, such a 500 Internal Server Error, that point to SQL injection vulnerabilities.

Reports : Once database hacked it can be overcome using proxy firewalls by compromising only the intermediateires

Responsiblities : As a QA analyst for Sqlmap, your duties would include making sure the tool functions as intended by testing its functionalities, testing it from the perspective of the user to ensure that it meets their needs, testing its compatibility with various environments, testing its security features, reporting and tracking any issues found during testing, documenting the testing process and findings, and offering training and support to users who require it. The tool must function successfully, satisfy user demands, and not bring any new problems or vulnerabilities. This is your key job.

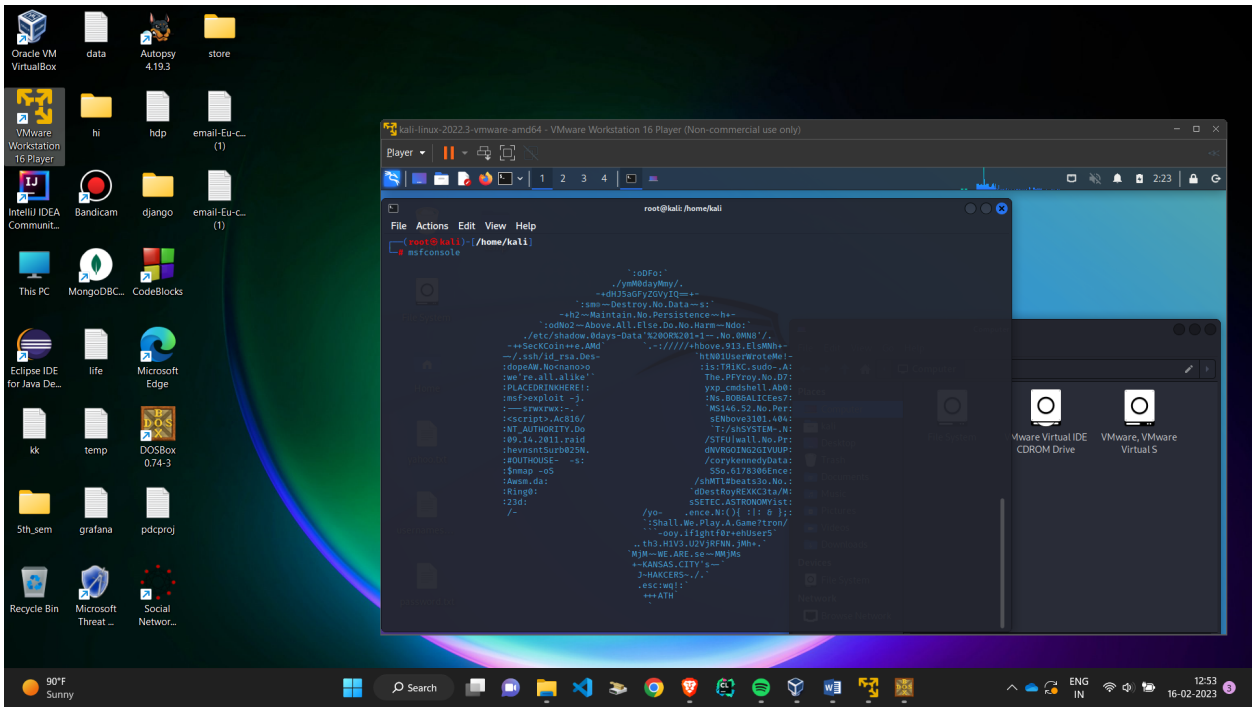
Approach 2 : with help of metasploit and payloads

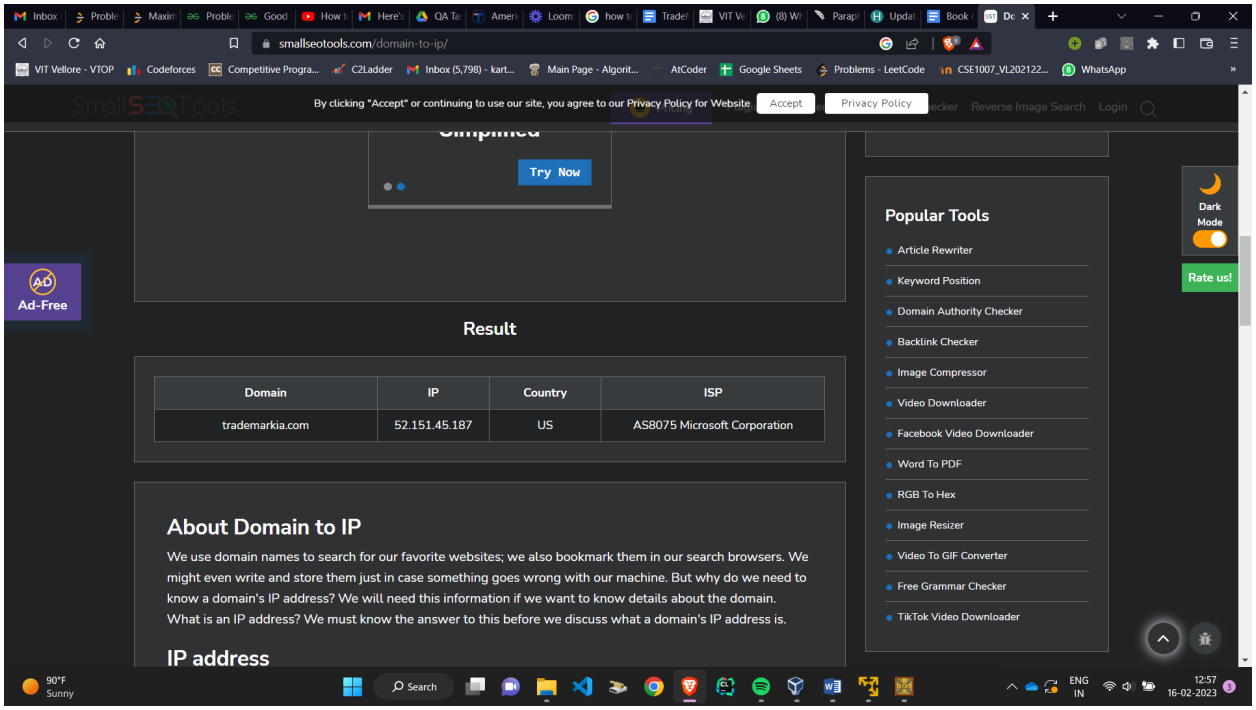
Scope :

Cybercriminals and ethical hackers may both utilise the sophisticated Metasploit framework to scan servers and networks for systemic weaknesses. It may be used with most operating systems and is highly customizable because it is an open-source framework.

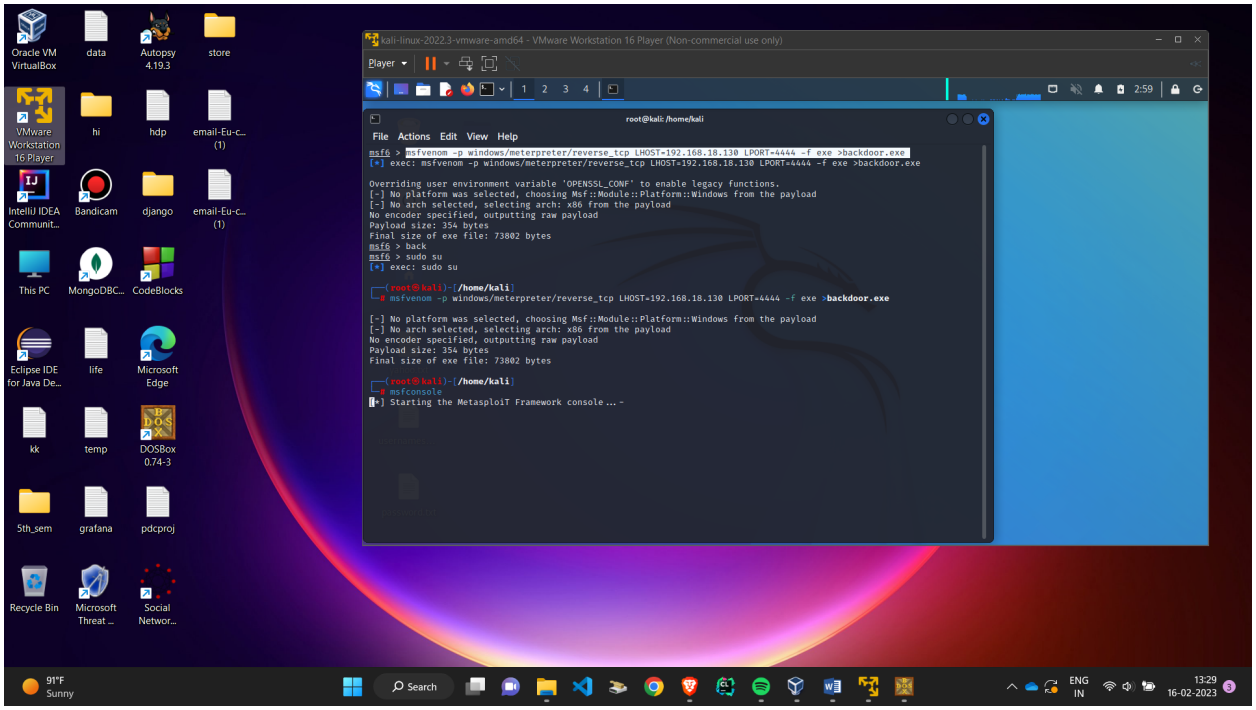
The pen testing team may employ ready-made or bespoke code with Metasploit to introduce it into a network and probe for vulnerabilities. Once faults are discovered and recorded, a different variation of threat hunting may be used to prioritise fixes and address systemic issues.

Methodology

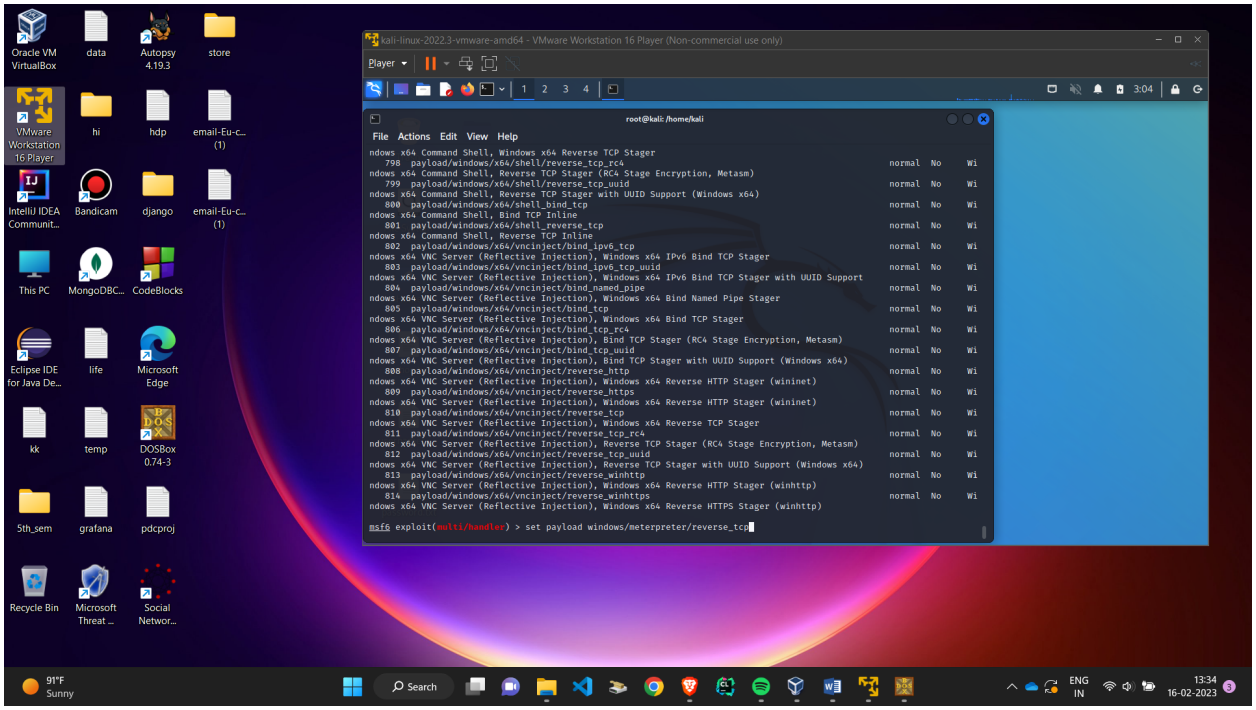


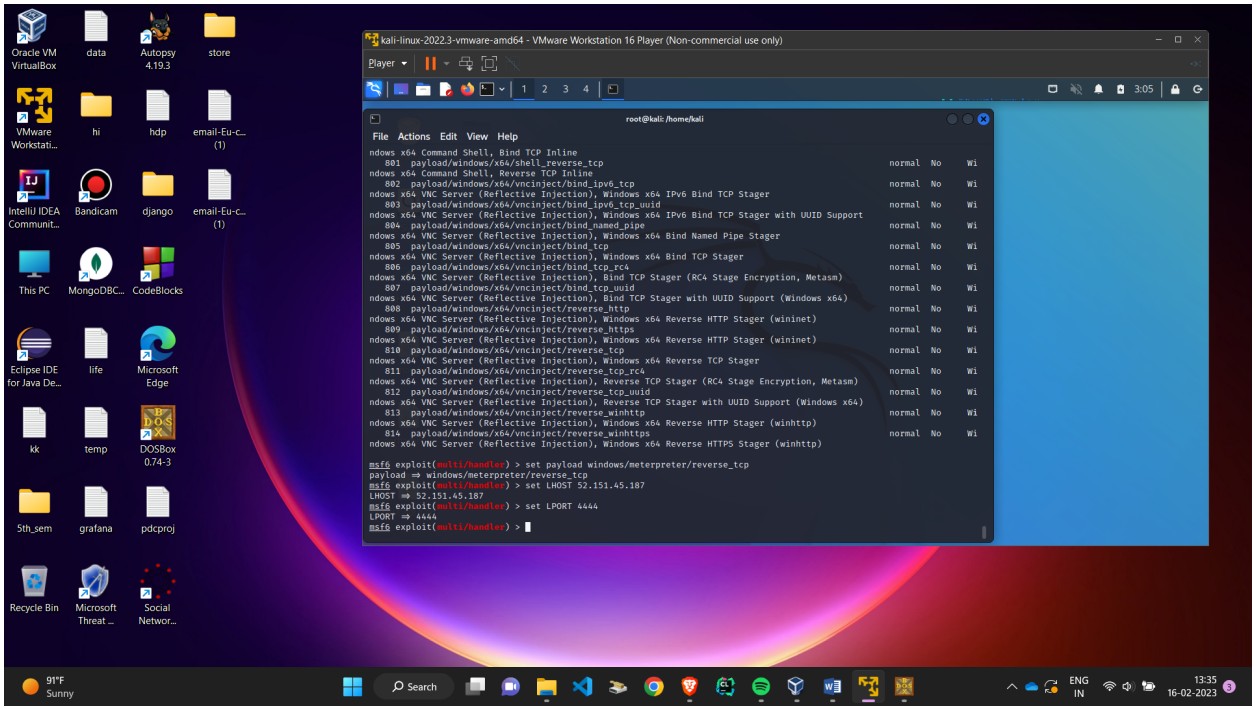


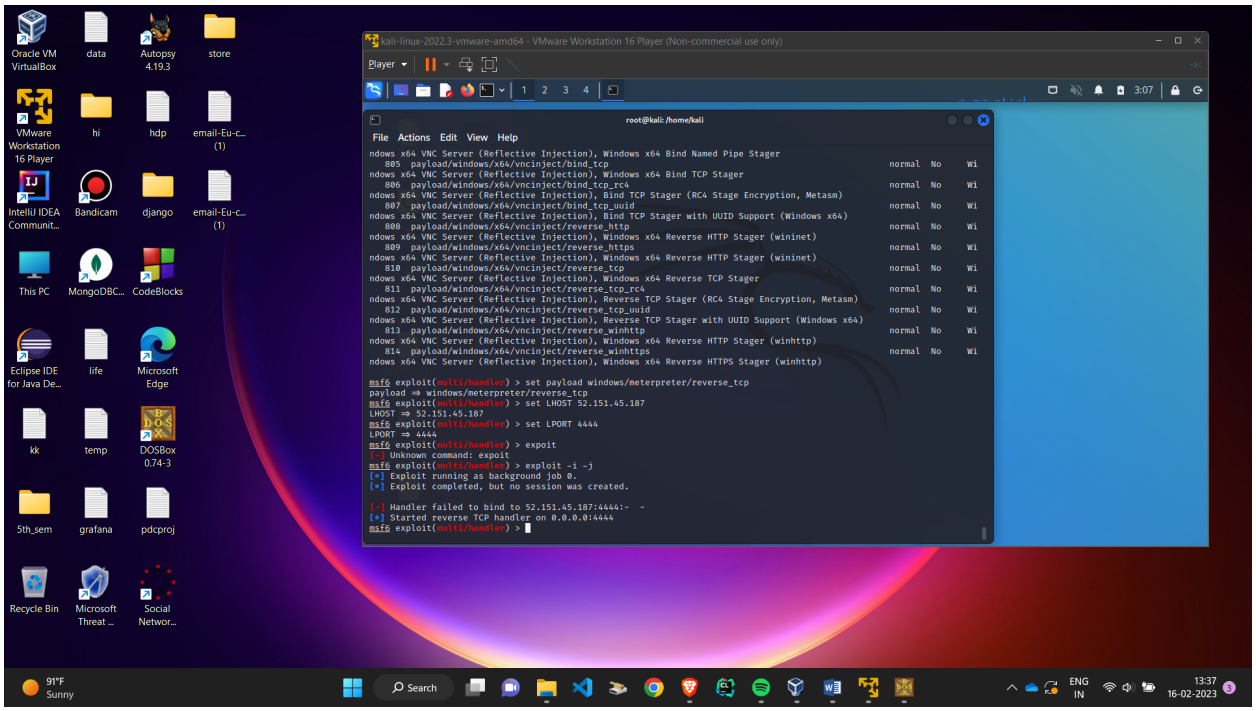
Domain ip : 52.151.45.187



Use the above ip as RHOSTS with backdoor functionality in msfconsole







Though no session was created because it is secure but of tried for 50 different payloads with keyword meterpreter a possibility of getting a open session is possible.

Environemnt used : metaspoit and some known payloads and handlers

Test cases : demo website here trademarkia.com

Criteria : To be vulnerable and to be able to retrieve meterpreter by exploiting vulnerabilities Payload creation is the process of developing a payload that is used to attack a target system's vulnerability. It is crucial to check if the produced payload is multi-handler compliant and has the ability to connect to the handler.

Delivery of the payload: There are a number of ways to send the payload to the target machine, including social engineering, email, and vulnerability exploitation. It is crucial to verify that the payload is properly delivered to the target system and establishes a connection with the multi-handler.

Connection stability: For the target system to remain under control, the link between the payload and multi-handler must be stable. Testing the connection's stability is crucial.

Reports : Once meterpreter request given from unknown source it can be overcome using ADG and using stateful protocol analysis it can be overcome

Responsiblities : As a QA analyst for payload based attacks , your duties would include making sure the tool functions as intended by testing its functionalities, testing it from the perspective of the user to ensure that it meets their needs, testing its compatibility with various environments, testing its security features, reporting and tracking any issues found during testing, documenting the testing process and findings, and offering training and support to users who require it. The tool must function successfully, satisfy user demands, and not bring any new problems or vulnerabilities. This is your key job.

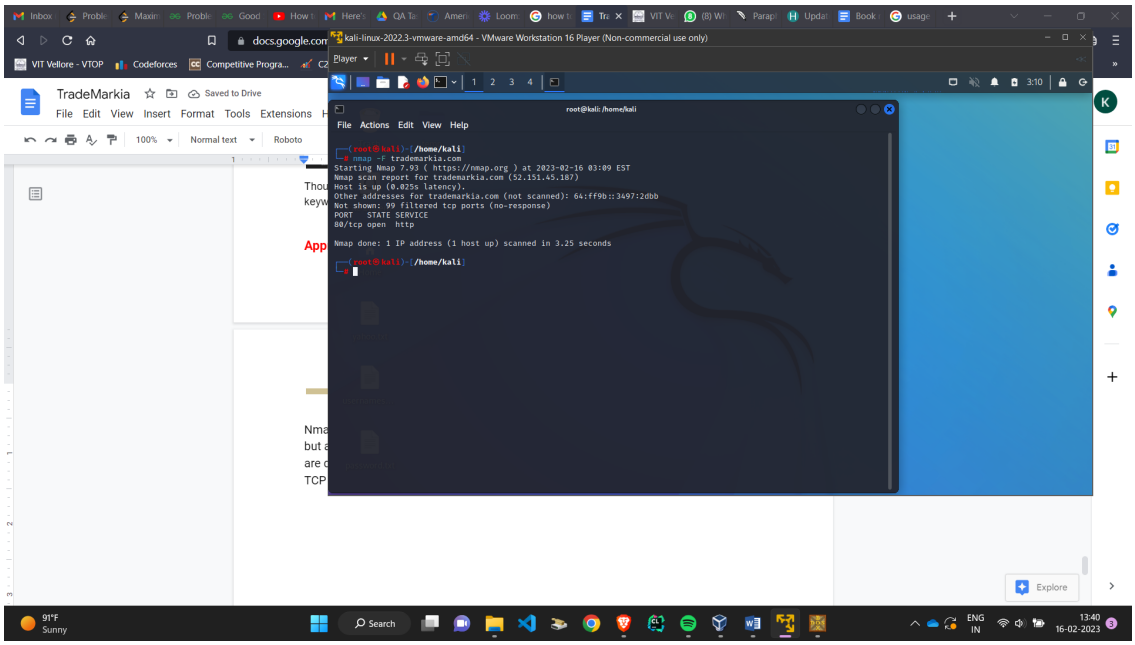
Approach 3 : Using nmap

Scope:

Nmap enables you to scan your network and find out not only what is connected to it but also a range of details such as what services each host is running, how many hosts are connected, and so on. Numerous scanning methods are supported, including UDP, TCP connect, TCP SYN (half-open), and FTP.

From nmap one of the port 80 is open and to be resolved to tackle the open port to attack the server

Methodology



From above 80/tcp is open with that some possible vulnerabilties can be exploited

Environemnt used : metasploit and some known nmap code

Test cases : demo website here trademarkia.com

Criteria :

Functionality: To make sure Nmap performs as intended, you must test its functionality as a QA analyst. This entails testing Nmap's numerous scanning options as well as making sure it can recognise and report on open ports, operating systems, and other network data.

Test Nmap's compatibility with various operating systems, network setups, and other software tools that are often employed in the sector.

Accuracy: For evaluating network security, Nmap's accuracy is essential. You must evaluate Nmap's capacity to spot vulnerabilities, correctly identify hosts and services, and deliver helpful details for patching.

Speed: In many network security scenarios, Nmap's speed is crucial. You must evaluate Nmap's capacity to swiftly and thoroughly scan networks while reducing false positives and false negatives.

Security: Security testing may be done using Nmap itself, but it's also crucial to evaluate Nmap's security features. You must evaluate Nmap's capacity to scan networks without endangering the network or its connected devices, as well as its defence against illegal access.

Training and documentation: Just as with any tool, it's crucial to give users training and documentation. You must make sure that users can understand how to use Nmap and validate the documentation's clarity and thoroughness.

Reports : Nmap is basic and wont affect the organization much as its a very entry level attack that can be auto configured and be ready with team and backup data

Responsiblities : As a QA analyst for Nmap, your duties would include making sure the tool functions as intended by testing its functionalities, testing it from the perspective of the user to ensure that it meets their needs, testing its compatibility with various environments, testing its security features, reporting and tracking any issues found during testing, documenting the testing process and findings, and offering training and support to users who require it. The tool must function successfully, satisfy user demands, and not bring any new problems or vulnerabilities. This is your key job.

Approach 4 : Legion

Scope

NMAP, whataweb, nikto, Vulners, Hydra, SMBenum, dirbuster, sslyzer, webslayer, and more automatic recon and scanning tools (with almost 100 auto-scheduled scripts)

Pentesters may easily locate and exploit attack vectors on hosts thanks to an intuitive graphical user interface with rich context menus and panels.

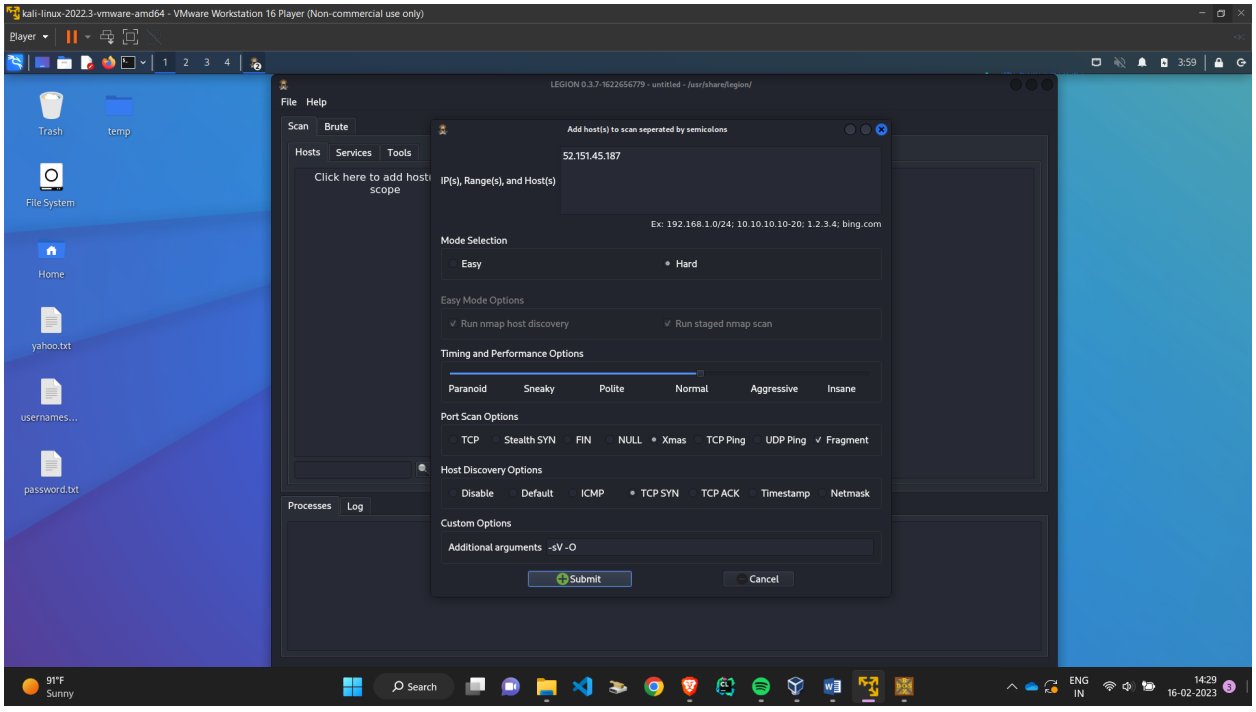
Legion's modular architecture enables users to quickly configure it and automatically invoke their own tools and scripts.

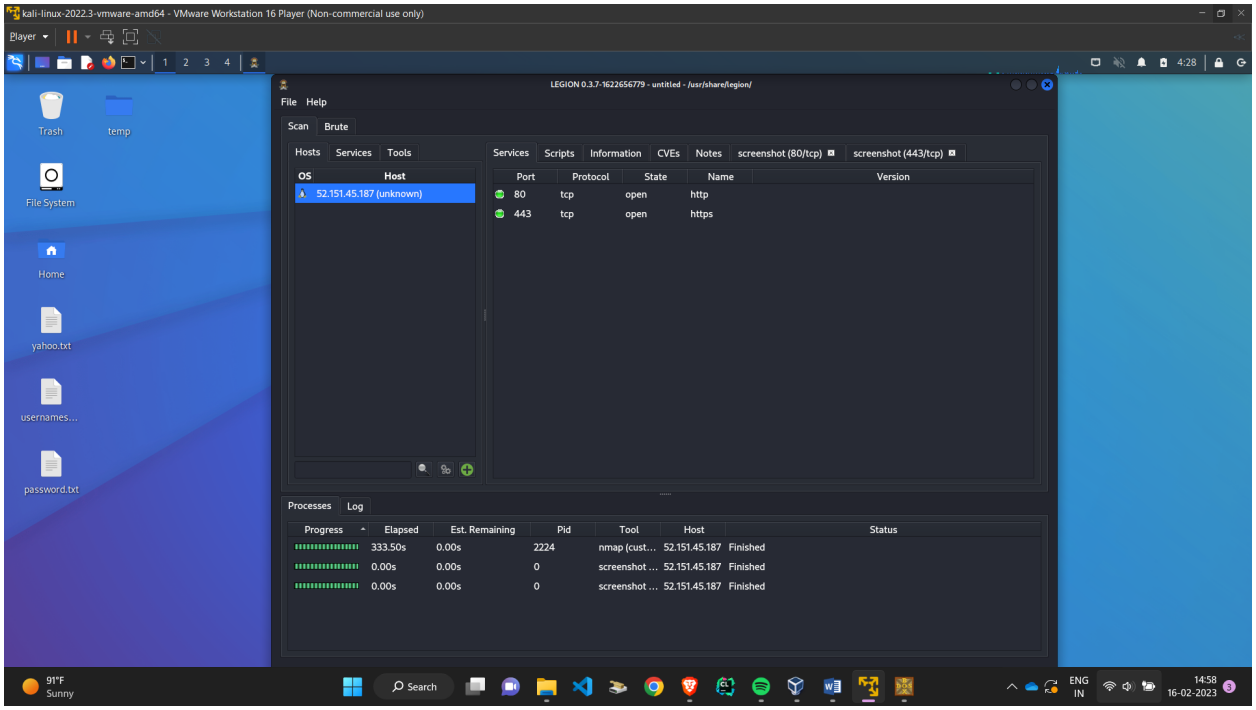
Extremely adjustable stage scanning for IPS evasion with ninja-like skills

Automated CPE (Common Platform Enumeration) and Vulnerability detection (Common Vulnerabilities and Exposures)

Real-time automatic task and project outcome storing

Methodology





Environemnt used : legion with hard mode and XMS attack

Test cases : demo website here trademarkia.com

Criteria : To be vulnerable and to be able to retrieve available open ports for exploiting open ports

Reports : As it sends request for open ports unmatched id requests can be router configured to a dead end which retrieves NULL or garbage address

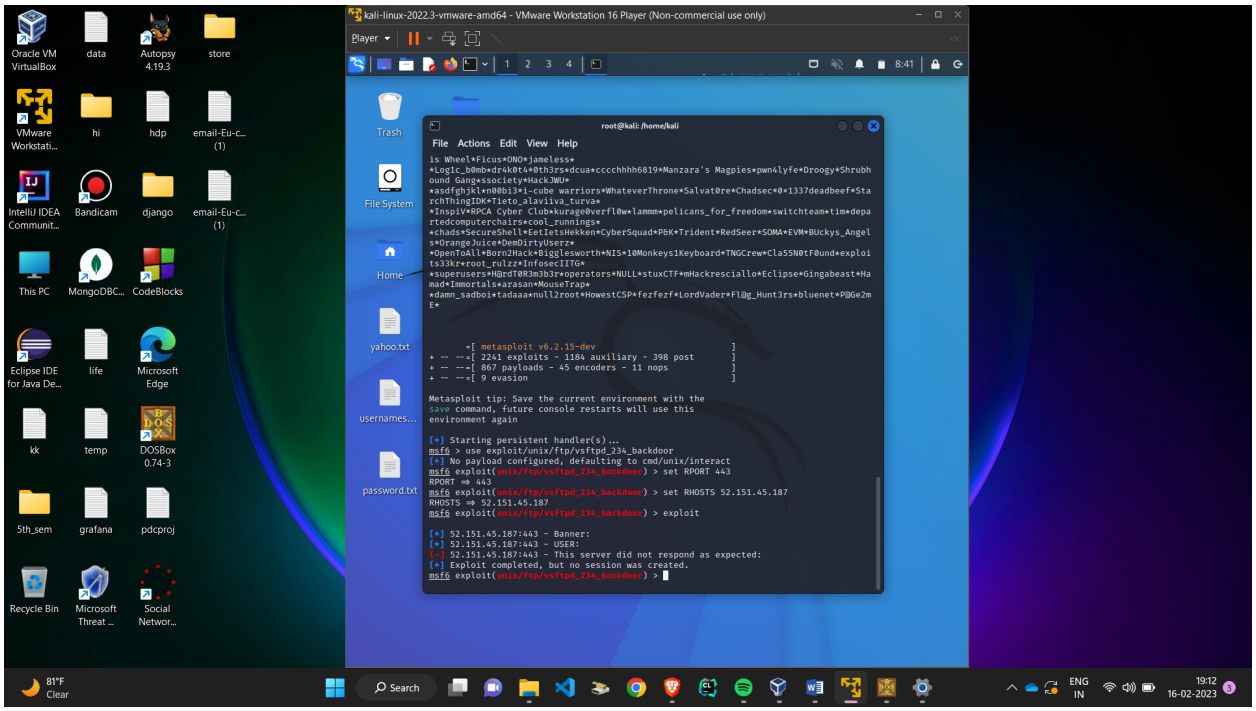
Responsiblities : As a QA analyst for Legion, your duties would include making sure the tool functions as intended by testing its functionalities, testing it from the perspective of the user to ensure that it meets their needs, testing its compatibility with various environments, testing its security features, reporting and tracking any issues found during testing, documenting the testing process and findings, and offering training and support to users who require it. The tool must function successfully, satisfy user demands, and not bring any new problems or vulnerabilities. This is your key job.

Approach 5 : backdoor vsftpd

Now with open ports by setting 80 and 443 as RPORTS we can try to find bugs and vulnerabilities using exploitable backdoor commands but it may not give open shell if the site trademarkia.com is very secure

For this we will be using vsftpd backdoor exploit command

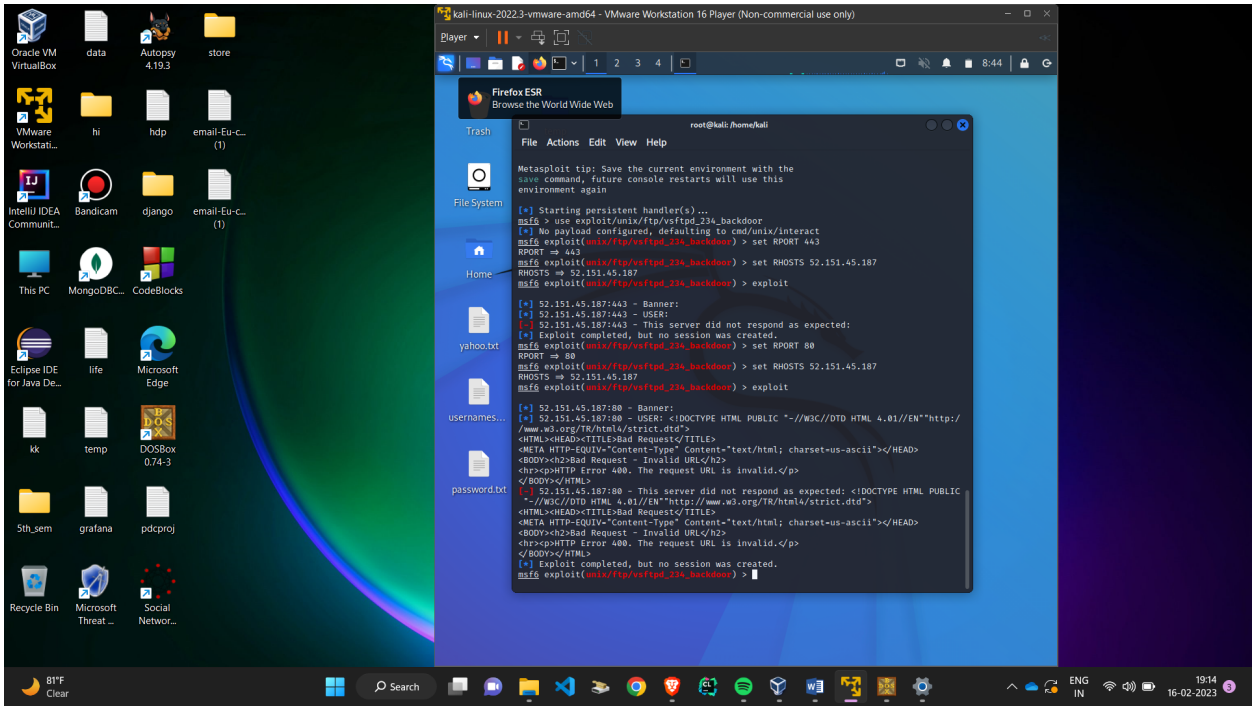
Trying for port 443:



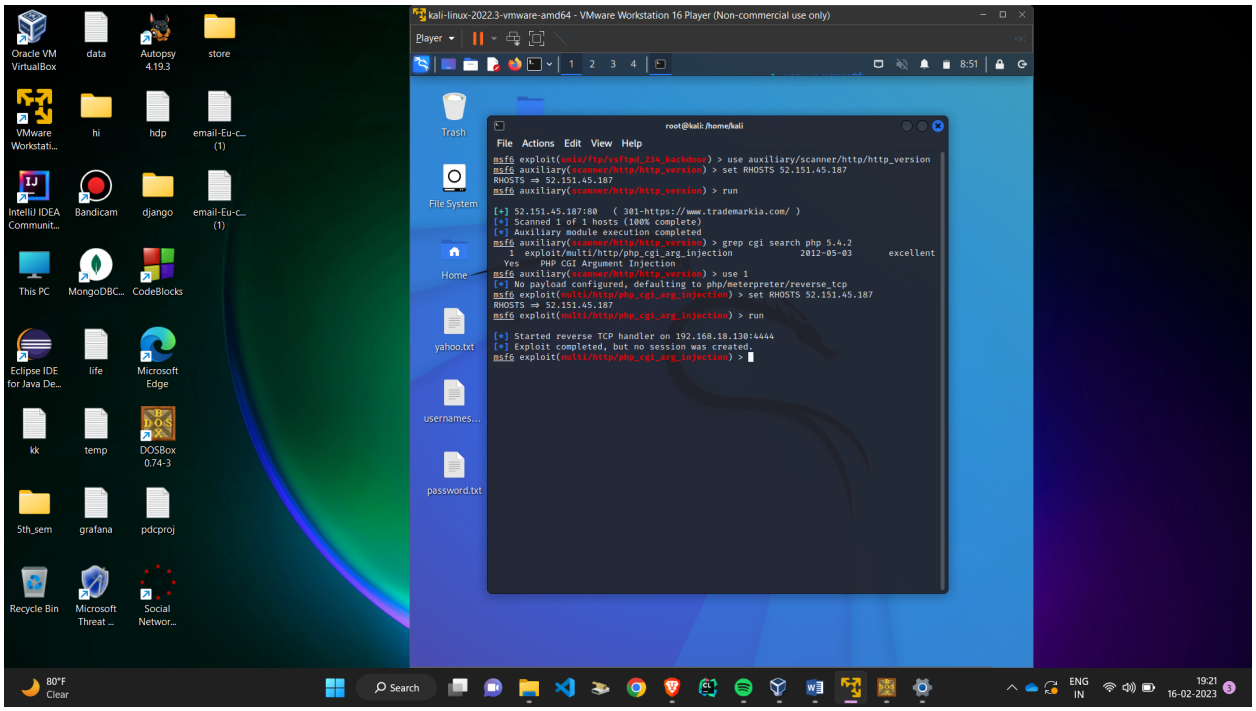
As the firewall is good its not possible to create a session in 443

Now trying in port 80:

As the site overcomes XSS attacks it it quite secure



Using another handler too gave no session as seems to be secure too



Environemnt used : metasploit and vsftpd attack handler to do ftp attack and http attack with different ports which are open

Test cases : demo website here trademarkia.com

Criteria : To be vulnerable and to be able to retrieve available open ports for exploiting open ports and can create a vulnerable session and open a shell within the domain giving access as an admin

Reports :

Update vsftpd: Ensure that vsftpd is running at the most recent version. All security flaws that are currently known may be fixed using this.

Alter the default port: Make a non-standard port the default for vsftpd. By doing this, automated assaults that target the default port may be less likely to succeed.

Firewall enable: To limit access to vsftpd to to trustworthy sources, enable a firewall on your Linux server.

Turn off anonymous login: Turn off anonymous login to stop hackers from using the system without being verified.

Use strong passwords: For all user accounts on the Linux server, including vsftpd accounts, use strong passwords.

Install SSL/TLS: To protect data transfers between the FTP server and clients, implement SSL/TLS encryption.

Keep an eye on logs: Keep an eye on the vsftpd logs for any improbable or attempted

Responsiblities : As a QA analyst for backdoor based attacks, your duties would include making sure the tool functions as intended by testing its functionalities, testing it from the perspective of the user to ensure that it meets their needs, testing its compatibility with various environments, testing its security features, reporting and tracking any issues found during testing, documenting the testing process and findings, and offering training and support to users who require it. The tool must function successfully, satisfy user demands, and not bring any new problems or vulnerabilities. This is your key job.

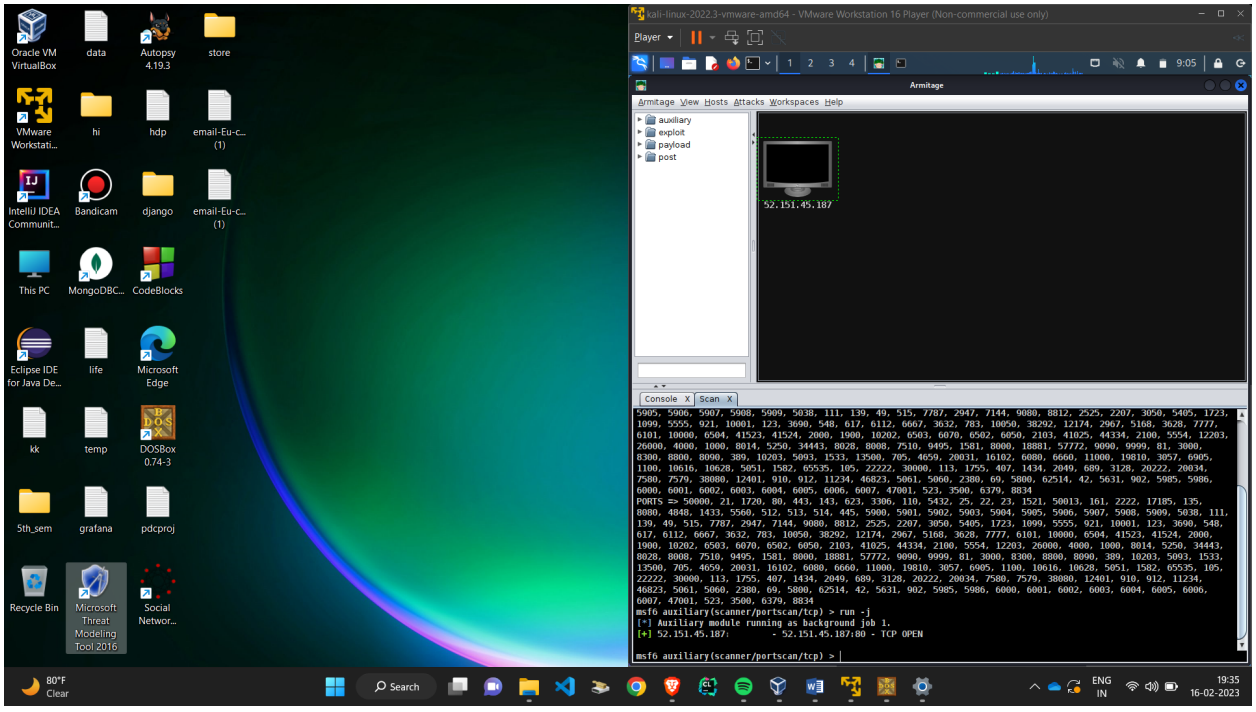
Approach 6 : Armitage

Scope :

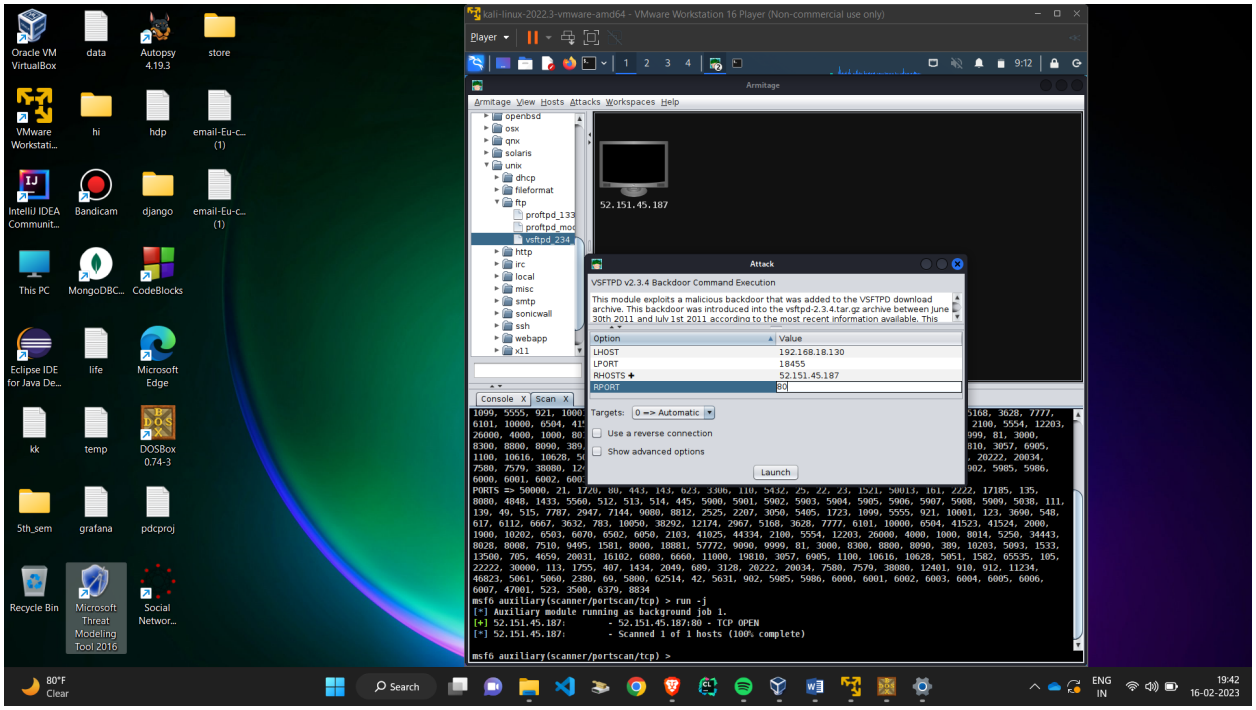
A famous Linux distribution used for penetration testing and ethical hacking, Kali Linux, includes Armitage, a graphical interface for managing cyber attacks. It offers a user-friendly interface for starting and administering attacks, and it's intended to make finding and exploiting holes in target systems easier.In addition to automating numerous penetration test tasks, Armitage enables users to observe and interact with network topologies, attack pathways, and attack payloads.

Methodology

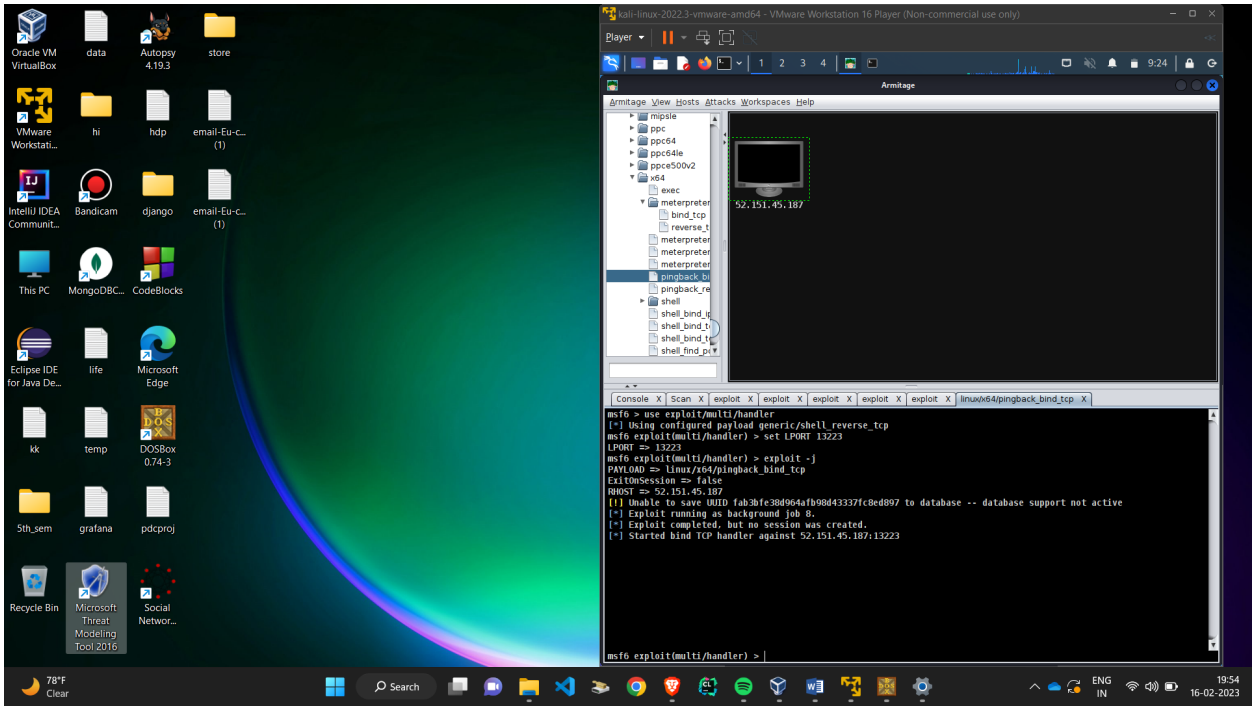
Scanning



Setting exploits



Did 10 different attacks on host with multiple handlers with main vulnerable host as port 80 but still not open session were available



Environemnt used : metasploit and armitage software

Test cases : demo website here trademarkia.com

Criteria : Installation of Kali Linux: Kali Linux comes with Armitage by default. To use Armitage, you must have Kali Linux installed on a physical or virtual system.

Armitage needs network connectivity in order to look for hosts and vulnerabilities as well as to initiate attacks against targets. To utilise Armitage, you must be physically or digitally linked to a network.

Armitage is developed on top of the well-known open-source Metasploit Framework, a penetration testing platform. To utilise Armitage on your Kali Linux system, Metasploit Framework must be installed.

Armitage was created using the Java programming language, thus your computer must have the Java Runtime Environment (JRE) installed.

Reports :

Access restrictions: Provide only trustworthy users with a genuine need for access to the system that runs Armitage.

Update software: Verify that Armitage and any other installed programmes are current with all security patches and updates.

Employ strong passwords: For all user accounts, including the one used to access Armitage, use strong passwords.

Watch logs: Keep an eye out for any strange behaviour that would point to an Armitage assault.

Restrict privileges: To stop attackers from getting administrative access to the system, restrict the rights of the user account used to access Armitage.

Firewall enablement: To limit access to Armitage to reputable sources only, enable a firewall on the Linux machine.

Secure data exchanges between Armitage and by using encryption

Bug reporting and tracking: You would be responsible for identifying and reporting any bugs, defects, or issues that you find during testing, and tracking their resolution through the testing and development process.

Documentation and training: You would be responsible for documenting your testing process, findings, and results, and providing training and support to users who may need assistance with using the tool.

Responsiblities :

Testing the Armitage tool's many functionality is your responsibility in order to make sure it functions as planned. To make sure they function as intended, several functionalities including attack launch, port scanning, vulnerability scanning, and session management are tested.You would be in charge of testing Armitage from the viewpoint of the user to make sure it satisfies their needs and expectations. To make that the tool is user-friendly and fits the user's needs, this involves testing the user interface, user experience, and ease of use.

Testing for compatibility: To make sure Armitage operates correctly across a range of scenarios, you would need to test it for compatibility with various operating systems, hardware setups, and network settings.

Approach 7 : Using mozilla observatory

Scope:

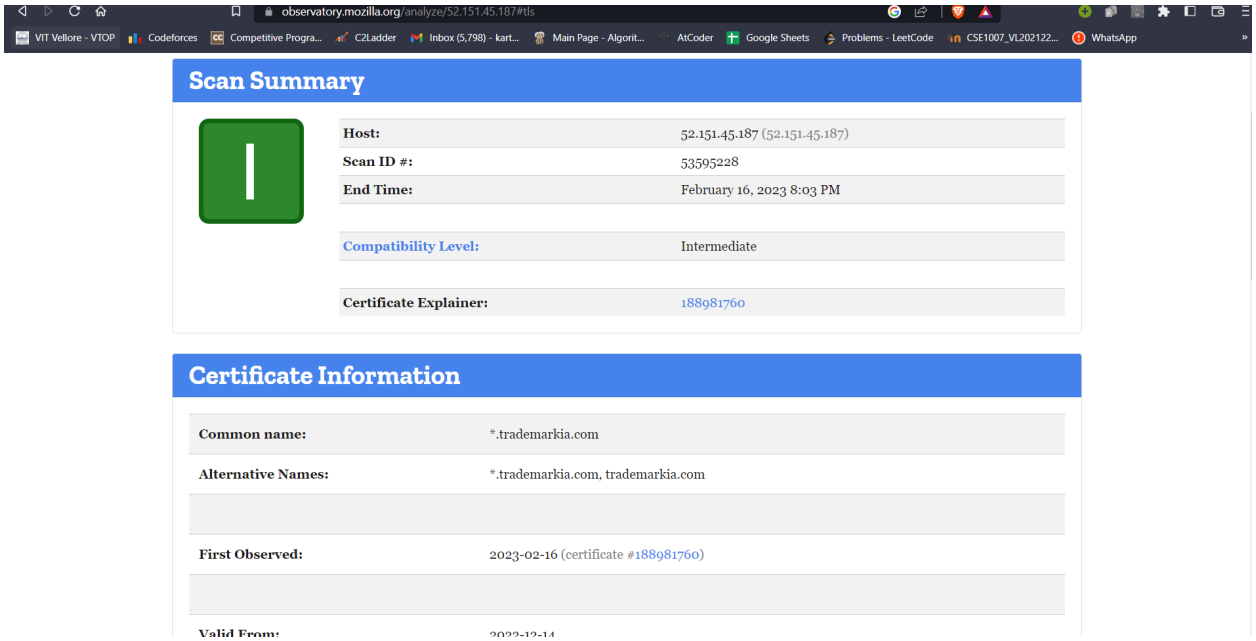
Security headers are HTTP response headers that can help shield a website from many sorts of attacks, including cross-site scripting (XSS), cross-site request forgery (CSRF), and clickjacking. Mozilla Observatory examines a website for security headers. Each header receives a score from the tool based on how successfully it is used.

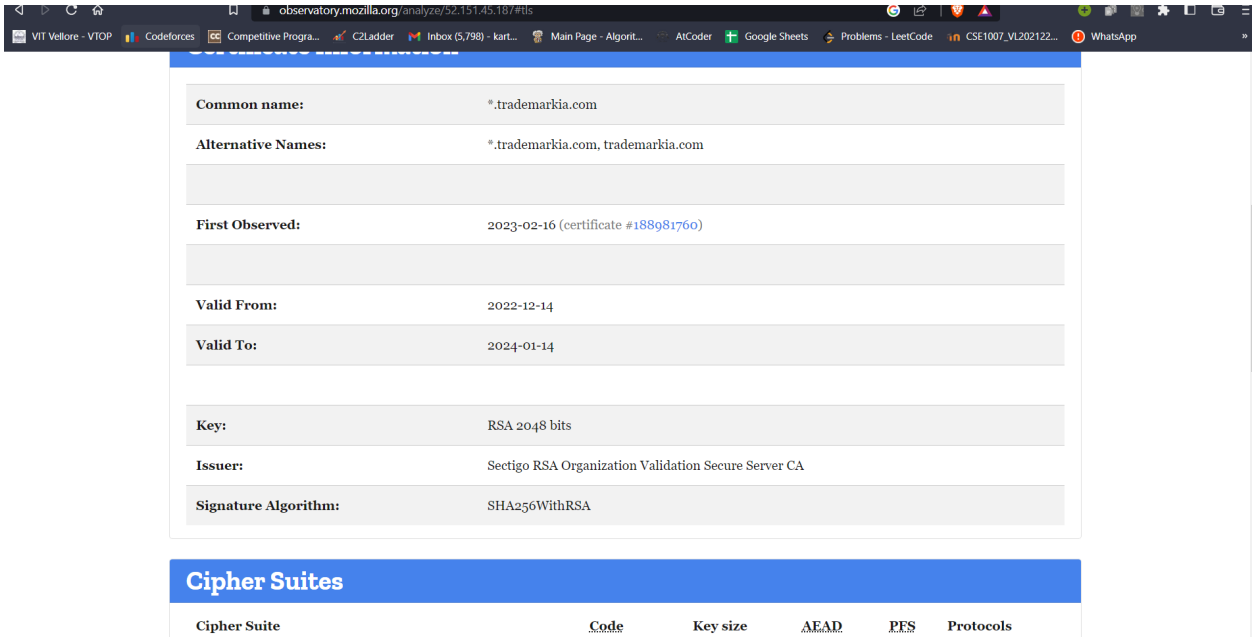
The SSL/TLS setup of the website, which is used to encrypt data transferred between the website and the user's browser, is tested by Mozilla Observatory. It looks for problems like old protocols, brittle cyphers, and expired certificates.

Cookies: The website's usage of cookies, which are used to store user information on the client-side, is tested by Mozilla Observatory. It checks

for problems including the usage of unsafe cookies and missing or inaccurate flags.

Methodology



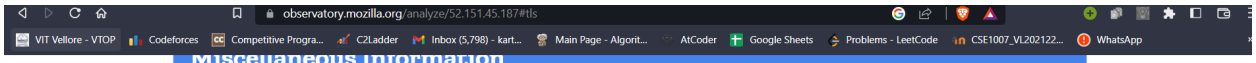


Cipher Suites

Cipher Suite	Code	Key size	AEAD	PFS	Protocols
ECDHE-RSA-AES256-GCM-SHA384	0x0C 0x30	2048 bits	✓	✓	TLS 1.2
ECDHE-RSA-AES128-GCM-SHA256	0x0C 0x2F	2048 bits	✓	✓	TLS 1.2
ECDHE-RSA-AES256-SHA384	0x0C 0x28	2048 bits	✗	✓	TLS 1.2
ECDHE-RSA-AES128-SHA256	0x0C 0x27	2048 bits	✗	✓	TLS 1.2
ECDHE-RSA-AES256-SHA	0x0C 0x14	2048 bits	✗	✓	TLS 1.2
ECDHE-RSA-AES128-SHA	0x0C 0x13	2048 bits	✗	✓	TLS 1.2

Miscellaneous Information

CAA Record:	No
Cipher Preference:	Server selects preferred cipher
Compatible Clients:	Android 4.4.2, Apple ATS 9, BingPreview Jan 2015, Chrome 30, Edge 12, Firefox 31.3.0 ESR, Googlebot Feb 2015, IE 11, Java 8b132, OpenSSL 1.0.1h, Opera 17, Safari 5, Yahoo Slurp Jun 2014, YandexBot Sep 2014



Miscellaneous Information

CAA Record:	No
Cipher Preference:	Server selects preferred cipher
Compatible Clients:	Android 4.4.2, Apple ATS 9, BingPreview Jan 2015, Chrome 30, Edge 12, Firefox 31.3.0 ESR, Googlebot Feb 2015, IE 11, Java 8b132, OpenSSL 1.0.1h, Opera 17, Safari 5, Yahoo Slurp Jun 2014, YandexBot Sep 2014
OCSP Stapling:	Yes

Suggestions

Looking for improved security and have a user base of only modern clients?

Take a look at the Mozilla "Modern" TLS configuration! It provides an extremely high level of security and performance and is compatible with all clients released in the last couple years. It is not recommended for general purpose websites that may need to service older clients such as Android 4.x, Internet Explorer 10, or Java 6.x.

Want the detailed technical nitty-gritty?

Please note that these suggestions may not be appropriate for your particular usage requirements! If they do sound like something you'd like assistance with, then hop on board:

Teleport me to Mozilla's configuration generator!

Environemnt used : Using mozilla observatory

Test cases : demo website here trademarkia.com

Criteria : It is crucial to examine security headers, SSL/TLS configuration, cookies, the Content Security Policy (CSP), referrer policy, and third-party resources while using Mozilla Observatory to test a domain for flaws. These tests can aid in locating potential security holes in the domain and offer advice on how to strengthen its defences.

Reports : A survey of the tool used to higher officials and the result based on it are sent back with bugs and vulnerabilities being detected from web malware available

Responsiblities : As a QA analyst for mozilla observatory, your duties would include making sure the tool functions as intended by testing its functionalities, testing it from the perspective of the user to ensure that it meets their needs, testing its compatibility with various environments, testing its security features, reporting and tracking any issues found during testing, documenting the testing process and findings, and offering training and support to users who require it. The tool must function successfully, satisfy user demands, and not bring any new problems or vulnerabilities. This is your key job.

Approach 8 : Using nikto evaluator

Scope:

Web server scanning: Nikto has the ability to check web servers for vulnerabilities, such as out-of-date software, improperly configured services, and well-known flaws.Cross-site scripting (XSS), SQL injection, and file inclusion vulnerabilities are among the vulnerabilities that Nikto may check for in online applications.Nikto can check SSL/TLS certificates and settings to look for any problems that can endanger the server.Testing of authentication procedures: Nikto can check the security of a web application's authentication procedures.Nikto may also be used to conduct brute-force attacks against web servers or apps to check for the presence of weak passwords or other forms of authentication.

Methodology

Examine a web server to find potential problems and security vulnerabilities, including:

- Server and software misconfigurations
- Default files and programs
- Insecure files and programs
- Outdated servers and programs

The scanning requires time (up to some hours). Please wait for a while.

Examples:

- http://relax-nk.ru
- https://zalinux.ru/

```
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          52.151.45.187
+ Target Hostname:    52.151.45.187
+ Target Port:        80
+ Proxy:              localhost:8118
+ Start Time:         2023-02-16 20:10:54 (GMT3)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a differ
fashion to the MIME type
+ Root page / redirects to: https://www.trademarkia.com/
+ Server banner has changed from '' to 'Microsoft-IIS/10.0' which may suggest a WAF, load balancer or proxy is in place
+ Cookie ICart created without the httponly flag
+ No CGI Directories found (use '-C all' to force check all possible dirs)
```

Environemnt used : Using nikto evaluator

Test cases : demo website here trademarkia.com

Criteria : Version of the web server being used may be determined by Nikto, who can then compare it to a database of known vulnerabilities.Web application: Nikto can inspect the web application that is hosted on the web server and find any configuration errors or known vulnerabilities.Nikto can determine if the web server is configured incorrectly, which might result in possible security problems.Versions of running software that are out of date and possibly vulnerable to known attacks are detected by Nikto. Examples include PHP and Apache.Configuration for SSL/TLS: Nikto can check SSL/TLS certificates and settings to find any problems that might endanger the server.Authentication procedures: Nikto may evaluate a web application's authentication procedures to see whether it is secure

.

Reports : A survey of the tool used to higher officials and the result based on it are sent back with bugs and vulnerabilities being detected from web malware available

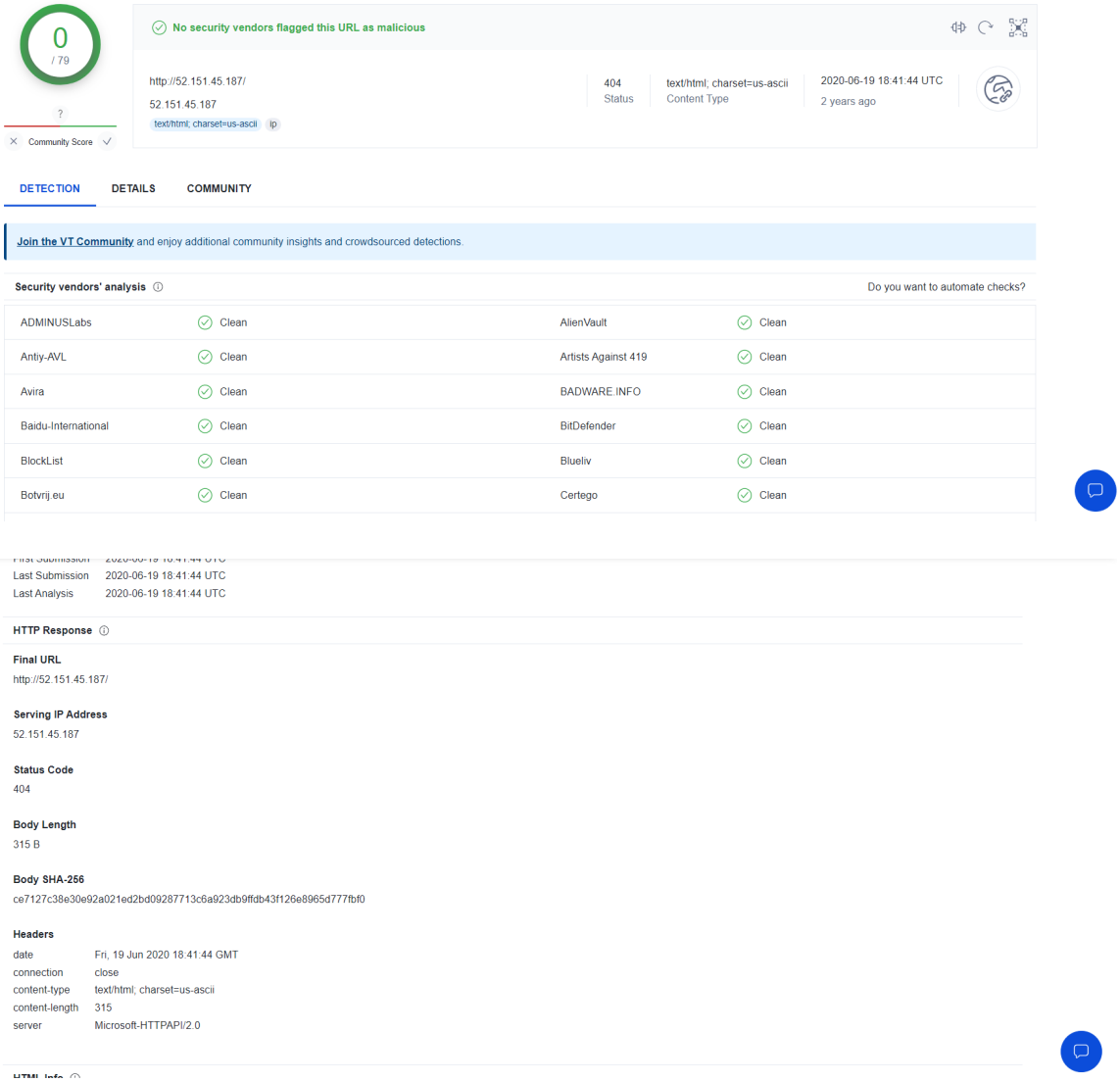
Responsiblities : As a QA analyst for mozilla observatory, your duties would include making sure the tool functions as intended by testing its functionalities, testing it from the perspective of the user to ensure that it meets their needs, testing its compatibility with various environments, testing its security features, reporting and tracking any issues found during testing, documenting the testing process and findings, and offering training and support to users who require it. The tool must function successfully, satisfy user demands, and not bring any new problems or vulnerabilities. This is your key job.

Approach 9 : VirusTotal scanner

Scope:

Users may check files, URLs, and IP addresses using the free internet service VirusTotal for malware and other forms of dangerous behaviour. To find possible dangers, the service examines uploaded information using a variety of antivirus engines and other security technologies. VirusTotal provides a thorough view of the analysis findings for a specific file, including any antivirus engine detections as well as extra metadata, such as the file's digital signature and other characteristics.

Methodology



Environemnt used : Using Virus total scanner

Test cases : demo website here trademarkia.com

Criteria : To have web identifiable bugs that have been pre determined and can be detected by virus total defender and report generated witht the available bugs in the input domain

Reports :

Reports on antivirus software: This report gives the findings of any antivirus engines that have scanned the file, URL, or IP address for malware. It displays which antivirus engines labelled the sample as safe and which ones recognised it as harmful.

Report on behavioural analysis: This report offers details on how the file, URL, or IP address behaved. If the file has attempted to communicate with any other systems, if it has produced any processes or files on the system, and what kind of network activity has been seen can all be included in this.

VirusTotal's community has seen the file, URL, or IP address a certain number of times, according to this study on crowd-sourced threat intelligence. Moreover, it provides information on the regions that are most

Affected by threat

Responsiblities : As a QA analyst for mozilla observatory, your duties would include making sure the tool functions as intended by testing its functionalities, testing it from the perspective of the user to ensure that it meets their needs, testing its compatibility with various environments, testing its security features, reporting and tracking any issues found during testing, documenting the testing process and findings, and offering training and support to users who require it. The tool must function successfully, satisfy user demands, and not bring any new problems or vulnerabilities. This is your key job

Result:

Thus we have finally found some bugs from trademarkia.com official website using frameworks and techniques and written them as UAT guidelines format.

Loom video :
https://www.loom.com/share/62872b82e33b4125854dace82ccb37bb