**BỘ THÔNG TIN VÀ TRUYỀN THÔNG**

**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**TIỂU LUẬN CUỐI KÌ**

**CHUYÊN ĐỀ AN TOÀN PHẦN MỀM**

Đề tài:

**CTF FORENSICS DETECTLOG4J**

Người hướng dẫn : TS. Huỳnh Trọng Thưa

Sinh viên thực hiện : Nguyễn Tuấn Kiệt

Mã số sinh viên : N18DCAT035

Lớp : D18CQAT01-N

Khóa : 2018 – 2023

Hệ : ĐẠI HỌC CHÍNH QUY

TP.HCM, tháng 11 năm 2022

* 1.What is the version of the log4j library used by the installed VMware product?

<https://communities.vmware.com/t5/VMware-vCenter-Discussions/vCenter-6-7-for-Windows-Build-19300125-Log4j/td-p/2910559>

* 2.What is the log4j library log level specified in the configuration file?

Google: log4j2 level file configuration vmware

<https://kb.vmware.com/s/article/2149228>

<https://docs.vmware.com/en/vRealize-Operations-Manager/8.1/com.vmware.vcom.config.doc/GUID-CE444BCB-6236-4778-8DB1-3796F3D71D7C.html>

* 3.The attacker used the log4shell.huntress.com payload to detect if vcenter instance is vulnerable. What is the first link of the log4huntress payload?

Search log4shell.huntress.com check thời gian

* 4.When was the first successful login to vsphere WebClient?

Google: vSphere Single-Sign On process writes

<https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-FBECACED-E9E2-4DE5-A4D2-3587D90D2420.html>

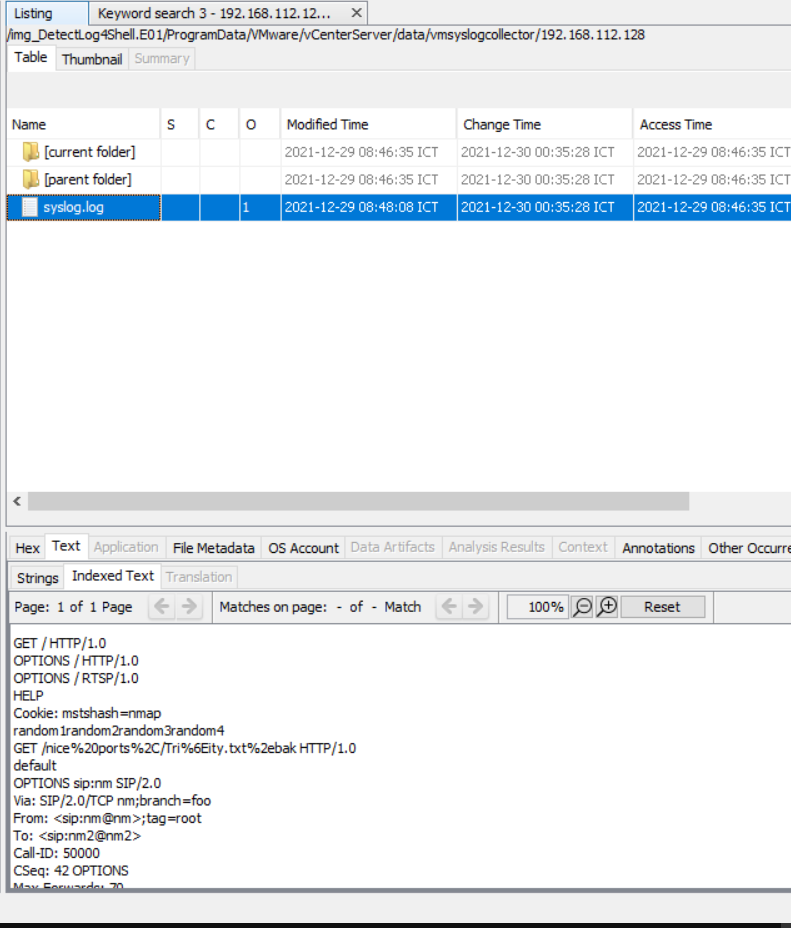
* 5.What is the attacker’s IP address?

Trong tệp Aud\_events.log, tất cả các mục nhập log4shell.huntress.com được liên kết với cùng một địa chỉ IP: 192.168.112.128

Search 192.168.112.128

Vmware syslog collector

<https://docs.vmware.com/en/VMware-vSphere/6.0/com.vmware.vsphere.vcenterhost.doc/GUID-61E7E2EA-F531-4665-9225-58BA899F55A5.html>



Một yêu cầu http

Khác so với log localhost thông thường

* 6.What is the port the attacker used to receive the cobalt strike reverse shell?

Hint: Check Microsoft-Windows-PowerShell%4Operational.evtx. Look for encoded base64 commands

ScriptBlock: $s=New-Object IO.MemoryStream(,[Convert]::FromBase64String(""));IEX (New-Object IO.StreamReader(New-Object IO.Compression.GzipStream($s,[IO.Compression.CompressionMode]::Decompress))).ReadToEnd();

Base64 và Gzip

Giải mã đoạn script

Vẫn chưa thấy port

Có 1 đoạn base64 giải mã tiếp xem có port hay k

Chỉ thấy ip hacker như vẫn chưa thấy port

Có 2 giải pháp lưu file virus .ps1 rồi chạy xem port

Trên sandbox port 1337

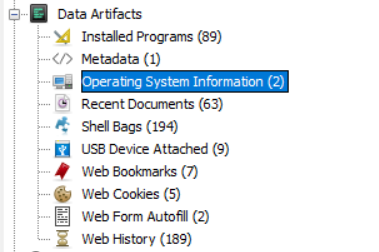
Trên máy ảo + fakenet

* 7. What is the executable used by the attacker to gain persistence??

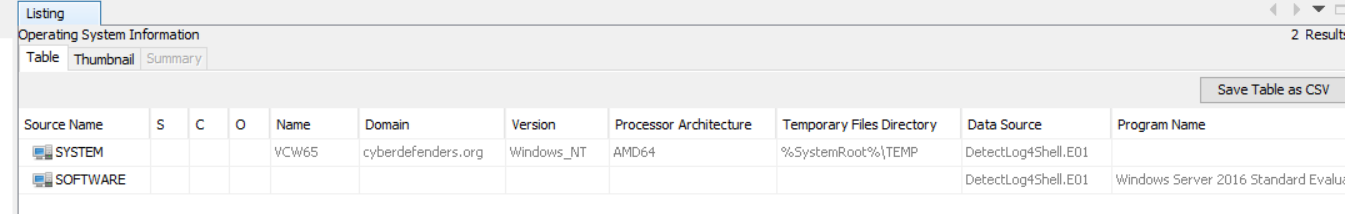
<https://www.cynet.com/attack-techniques-hands-on/the-art-of-persistence/>

#1 What is the computer hostname?

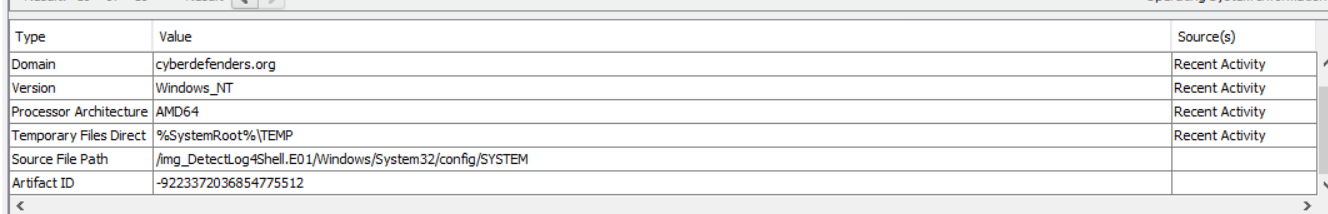
B1:



B2:



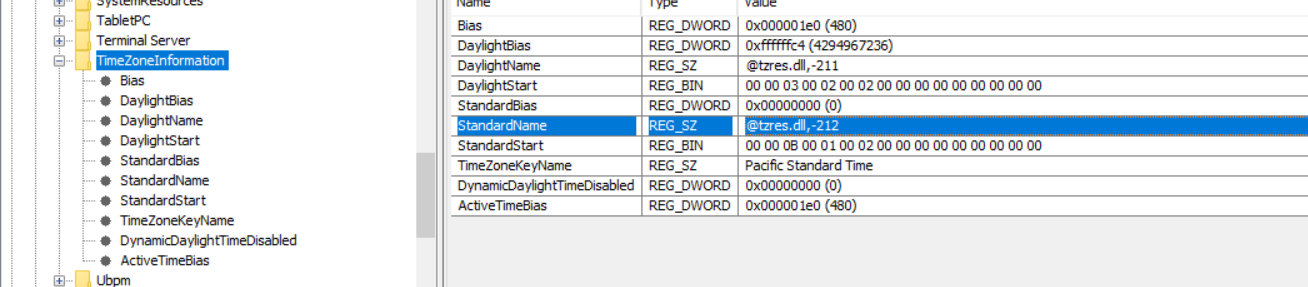
B3:



#2 What is the Timezone of the compromised machine?

**Windows\System32\config**

click System, controlset001, control , timezoneinformation

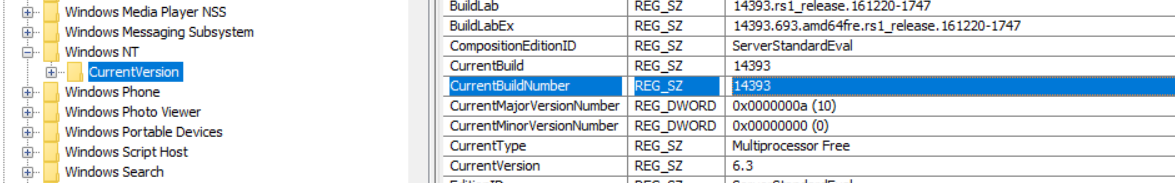


#3 What is the current build number on the system?

**Windows\System32\config**

click software , **Microsoft > Windows NT**

current version : 14393

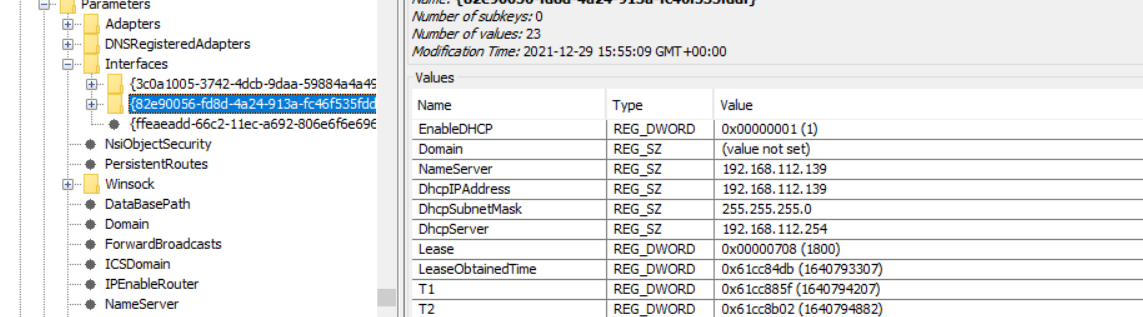


#4 What is the computer IP?

**Windows\System32\config**

click system

**ControlSet001 > Services > Tcpip**



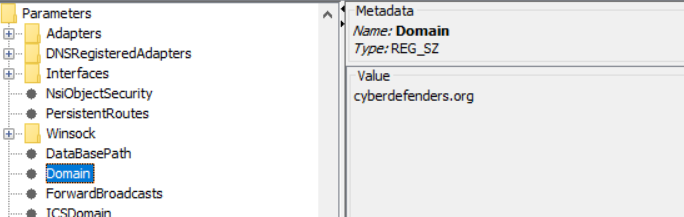
#5 What is the domain computer was assigned to?

cyberdefenders.org

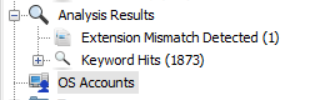
**Windows\System32\config**

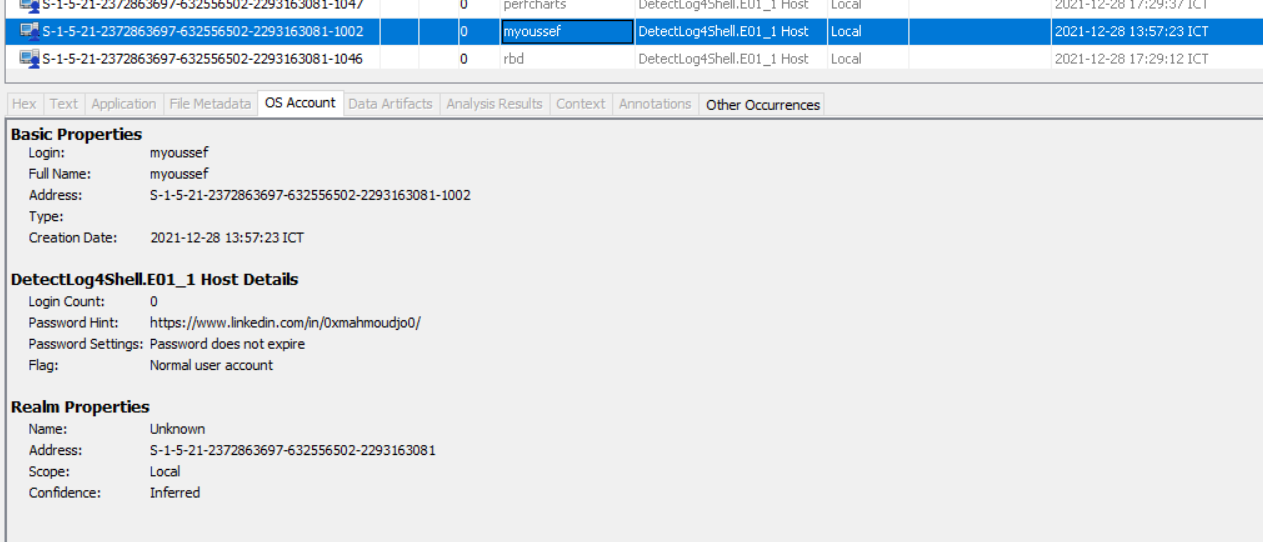
System

**ControlSet001 > Services > Tcpip> Winsock**

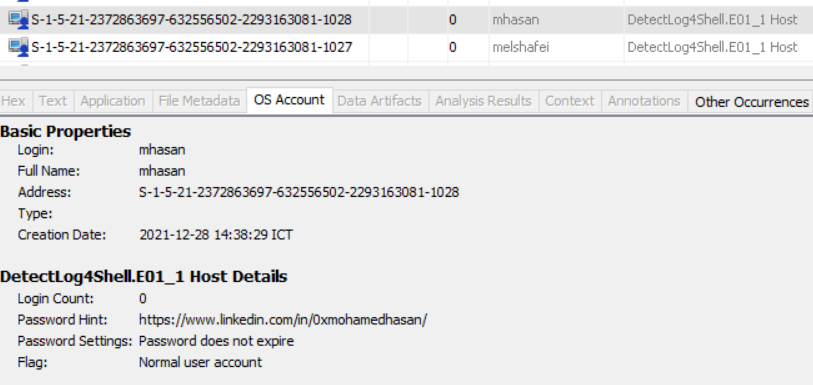


#6 When was myoussef user created?





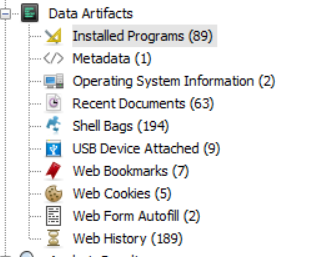
#7 What is the user mhasan password hint?

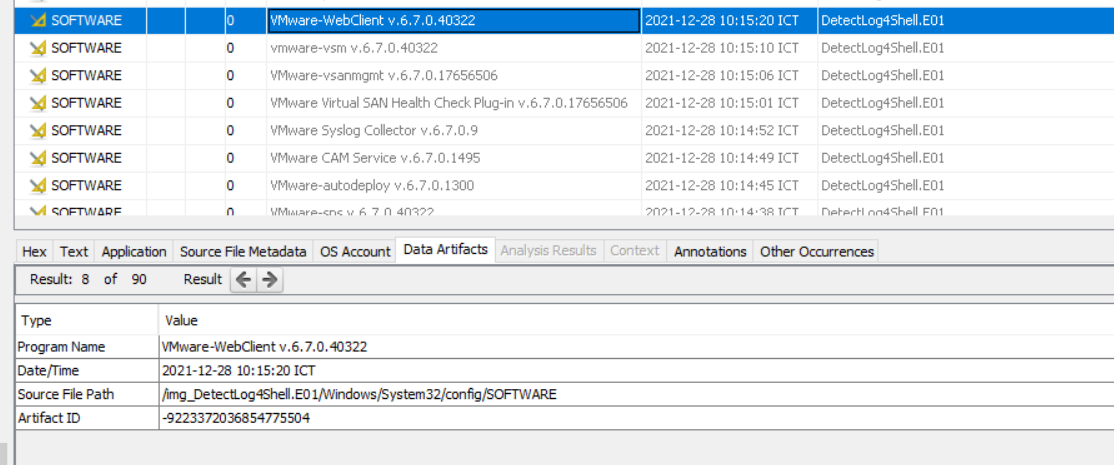


#8 What is the version of the VMware product installed on the machine?

**Data Artifacts > Installed Programs**

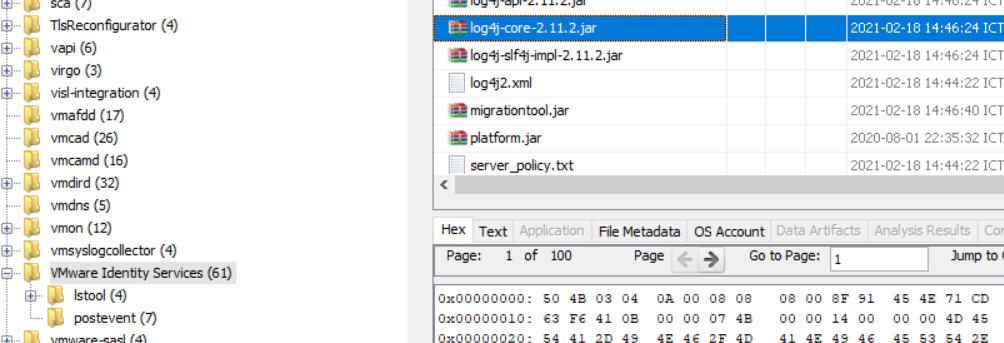
search for VMware product , version is 6.7.0.40322



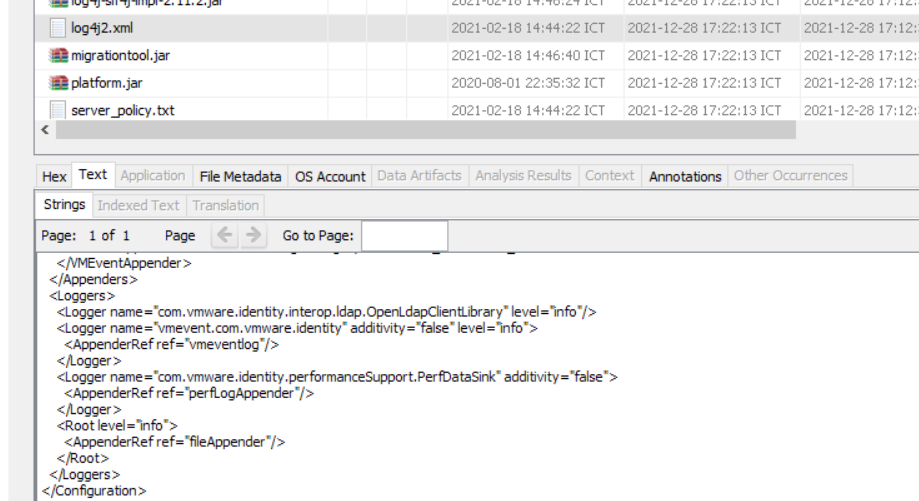


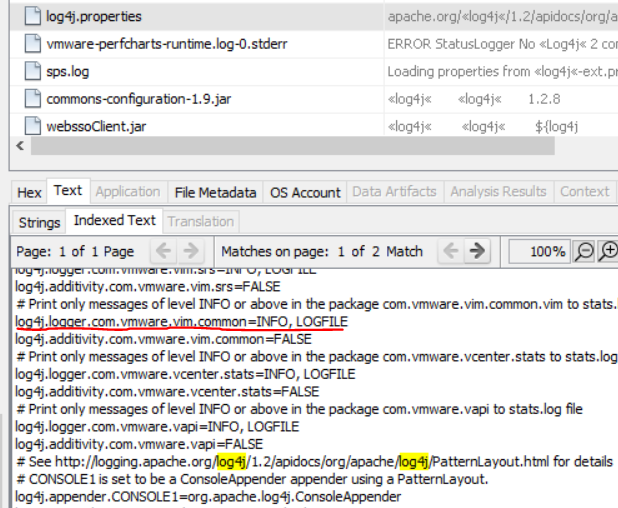
#9 What is the version of the log4j library used by the installed VMware product?

Go to **Program Files\VMWare\vCenter Server\VMware Identity Services**



#10 What is the log4j library log level specified in the configuration file?





#11 The attacker exploited log4shell through an HTTP login request. What is the HTTP header used to inject payload?

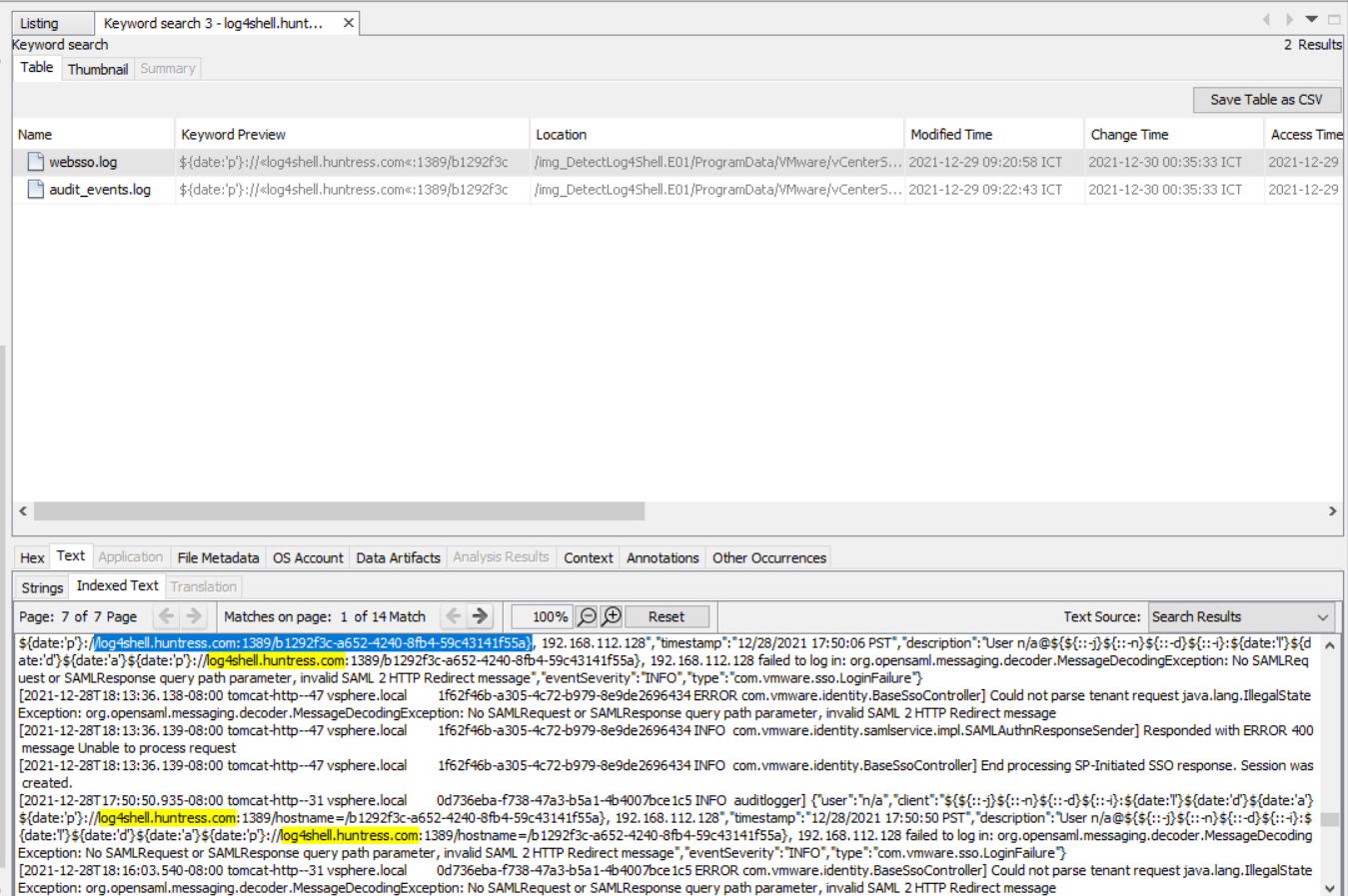
Google “vcenter log4j exploit”

“The vulnerability is in the X-Forwarded-For header on the vCenter SSO login page…” , so HTTP header should be X-Forwarded-For

#12 The attacker used the log4shell.huntress.com payload to detect if vcenter instance is vulnerable. What is the first link of the log4huntress payload?

/

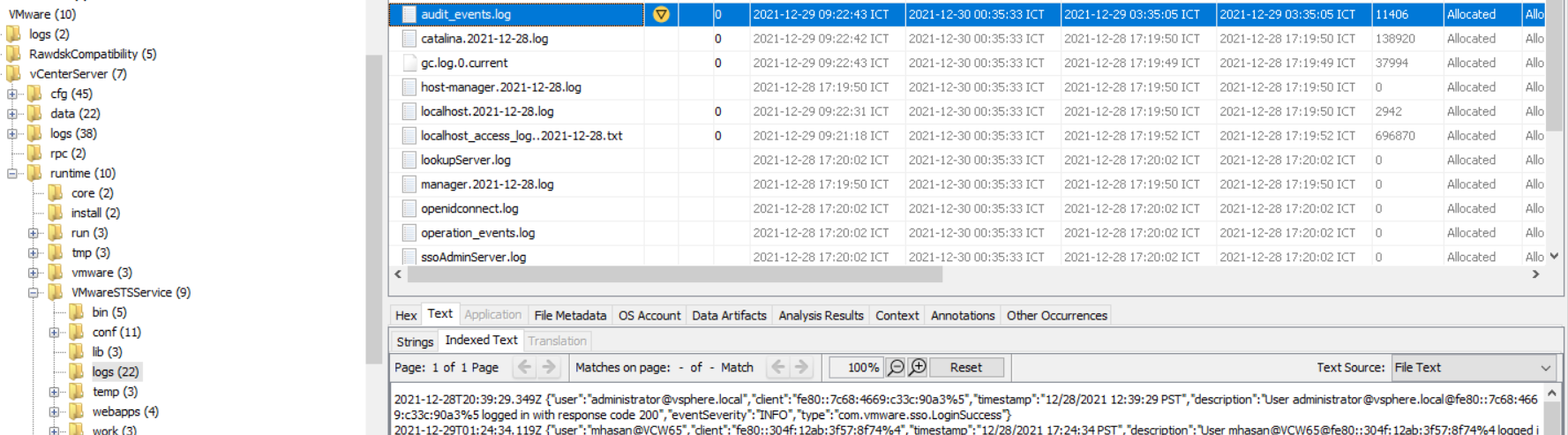
log4shell.huntress.com:1389/b1292f3c-a652-4240-8fb4-59c43141f55a}



#13 When was the first successful login to vsphere WebClient?

**ProgramData\VMWare\vCenterServer\runtime\VMWareSTSService\logs**

click audit\_events.log



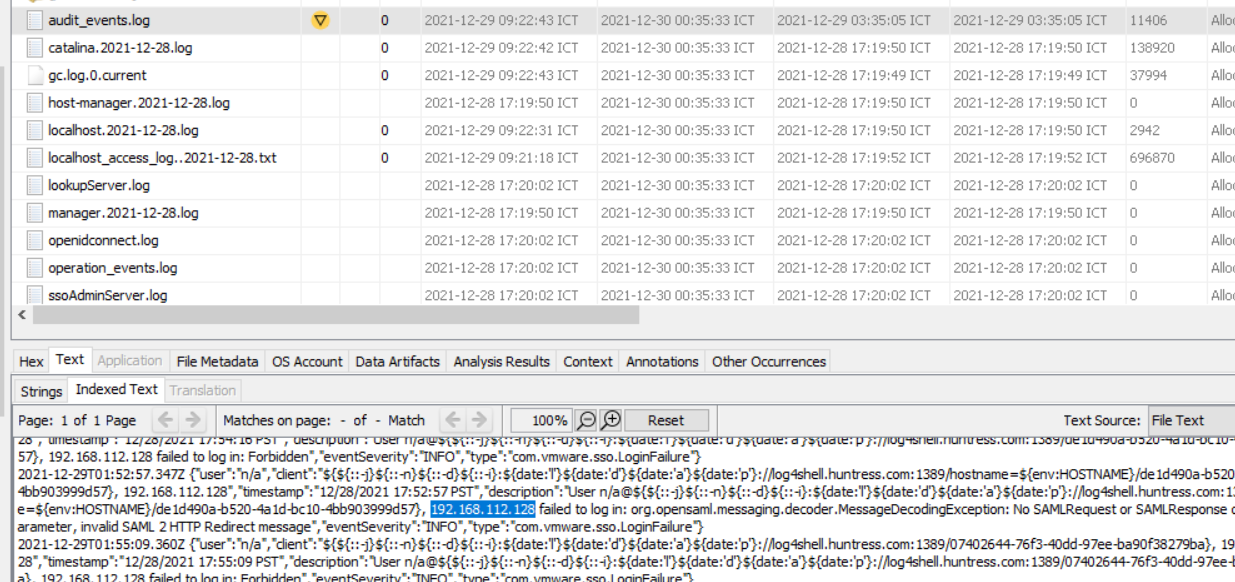
first sucess login : 12/28/2021 12:39:29 PST

submitted with UTC format 28/12/2021 20:39:29 UTC

#14 What is the attacker’s IP address?

look for attacker’s IP in audit\_events.log

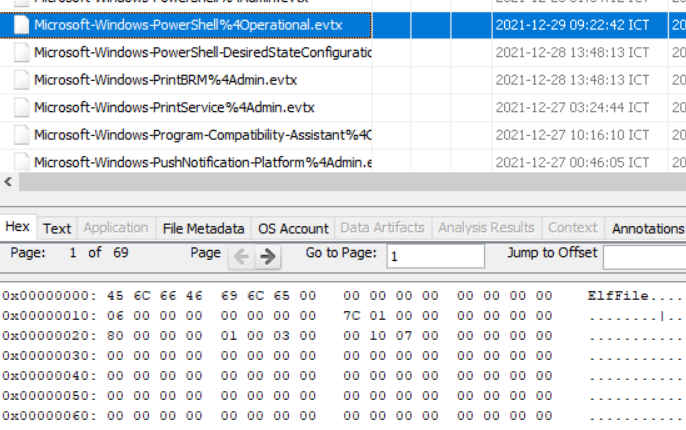
**192.168.112.128**



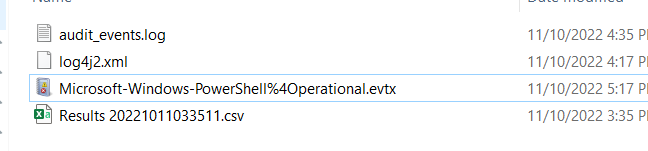
#15 What is the port the attacker used to receive the cobalt strike reverse shell?

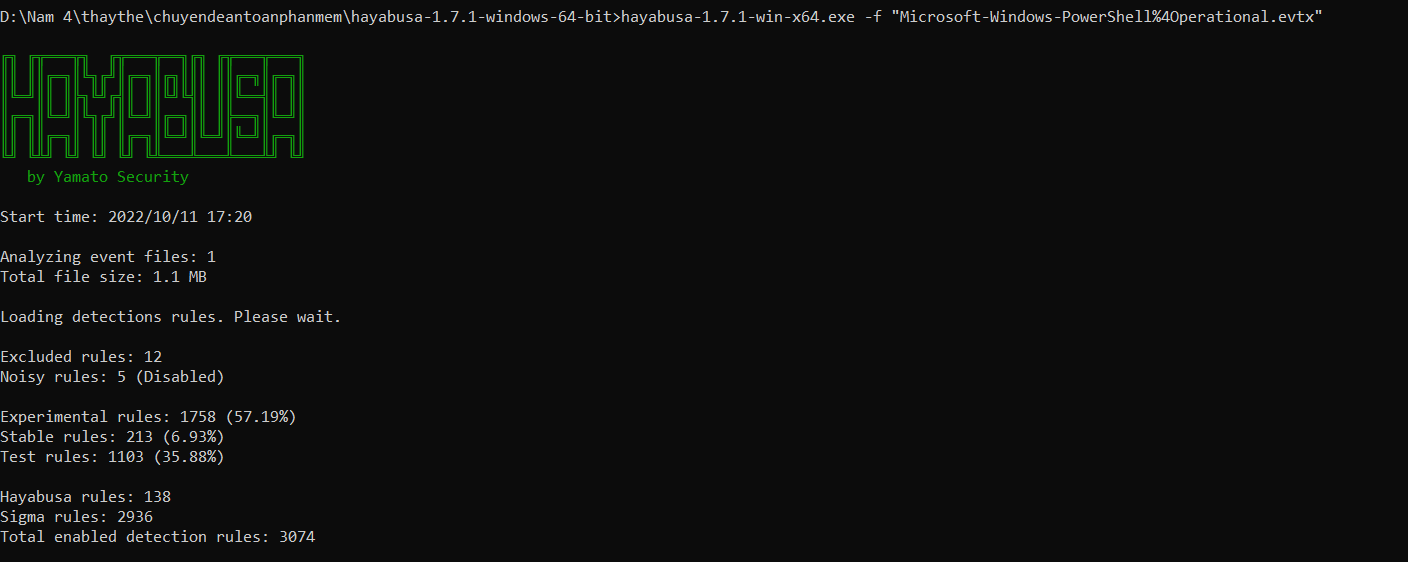
**Windows\System32\winevt\Logs**

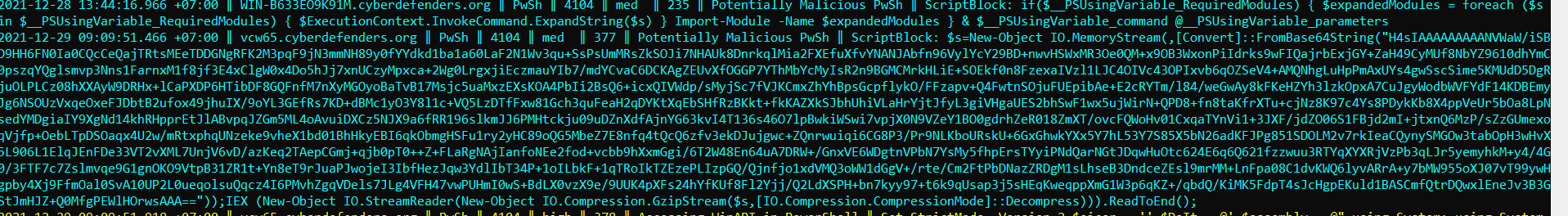
**Microsft-Windows-PowerShell%4Operational.evtx**

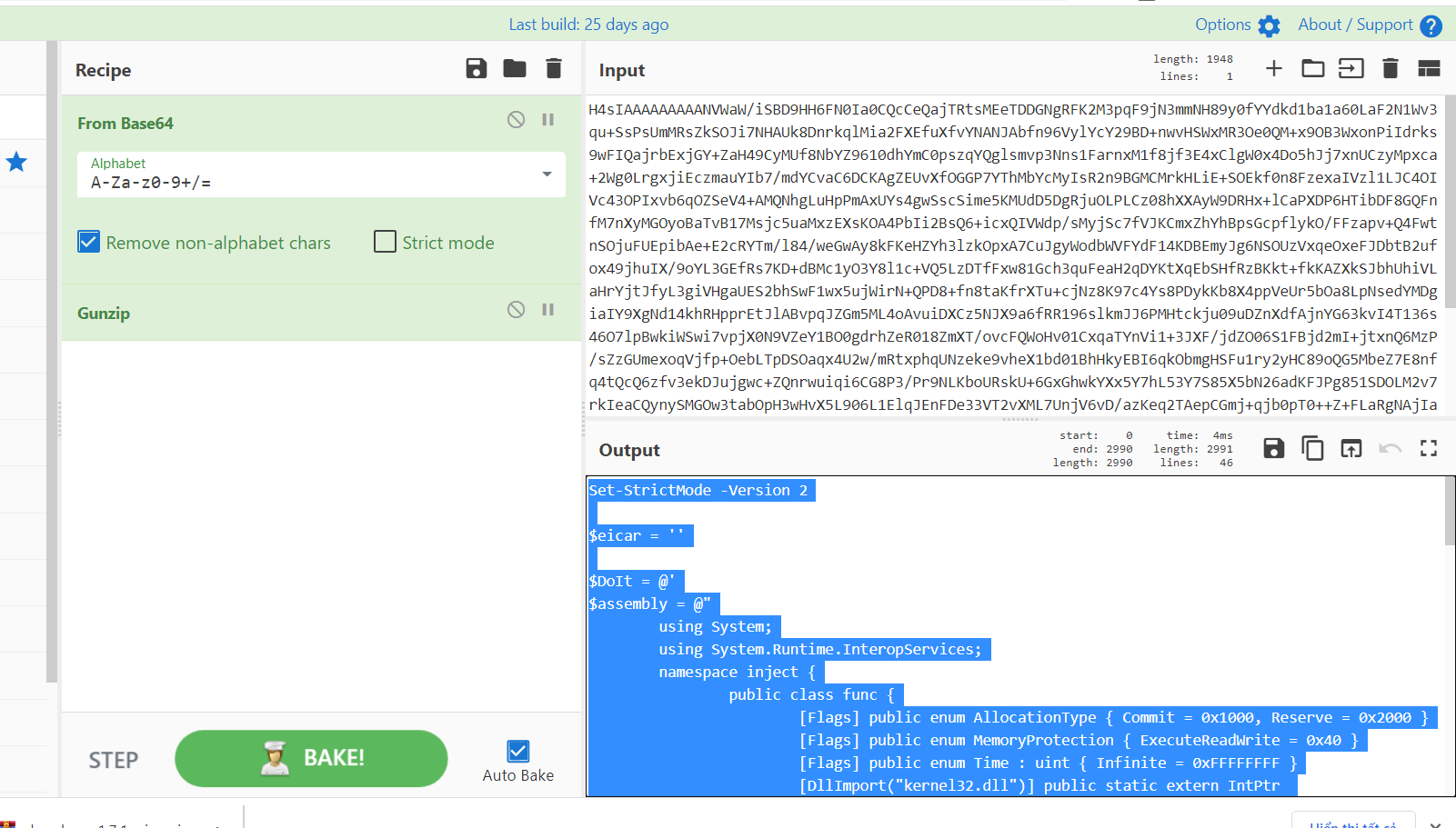


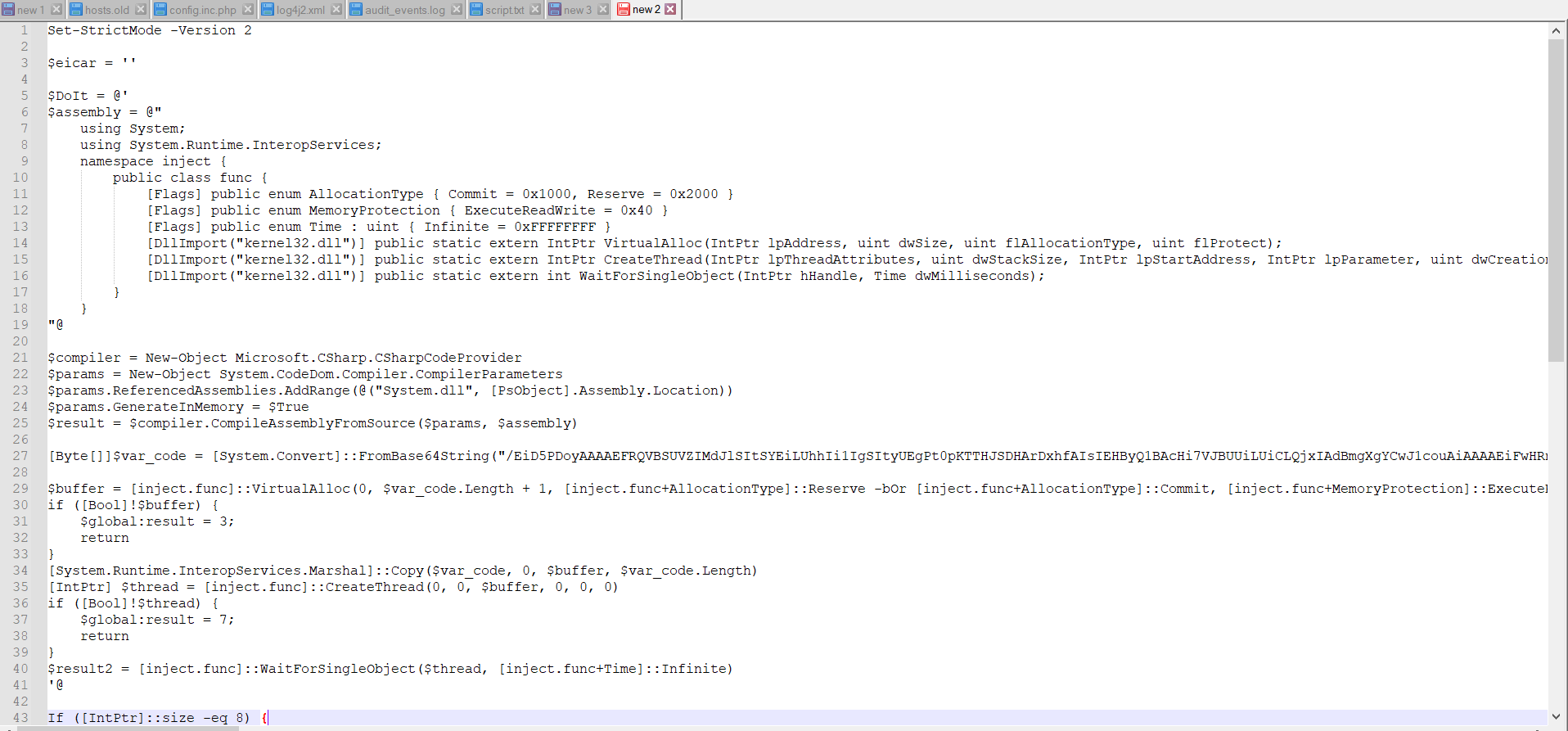
Export

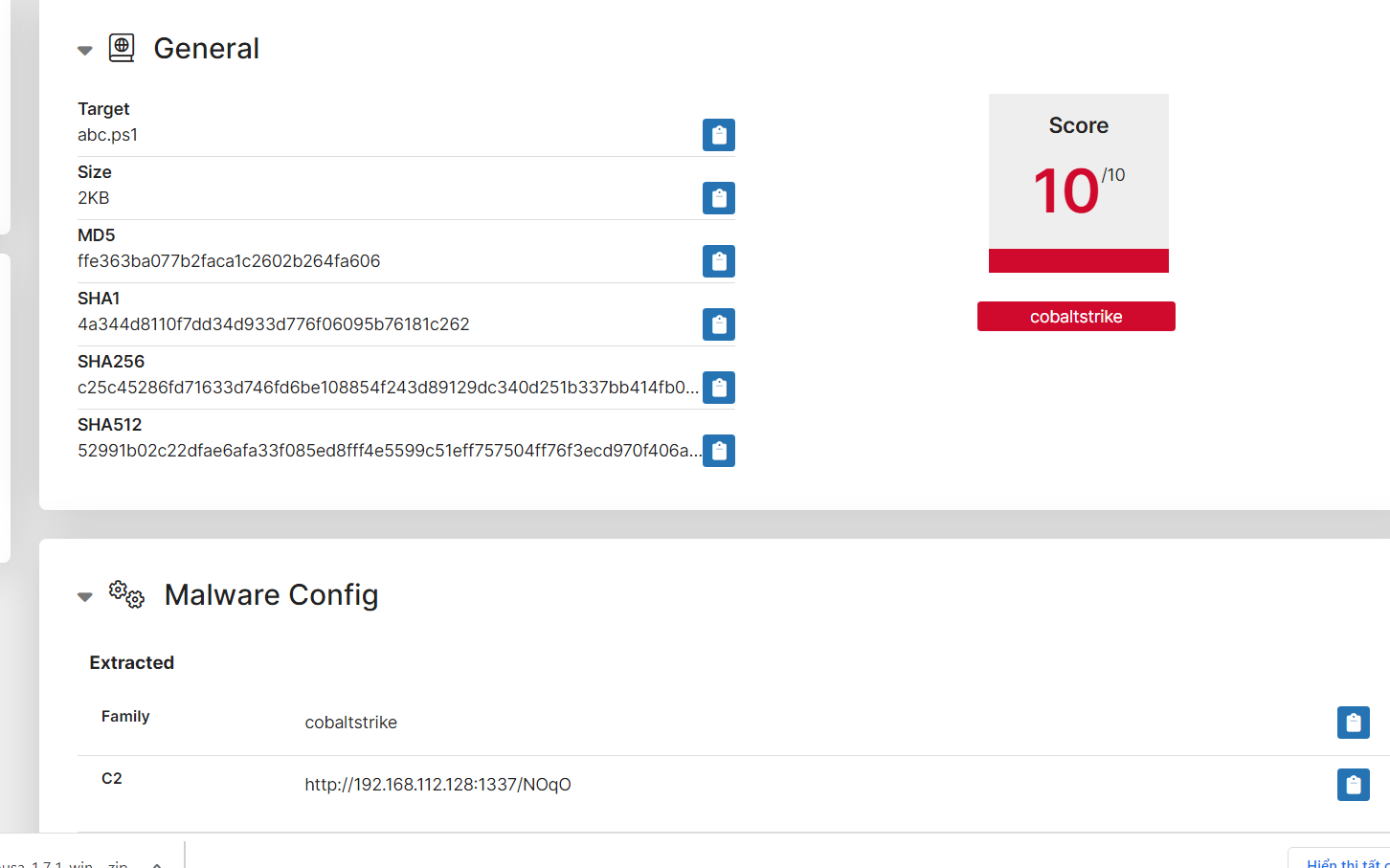


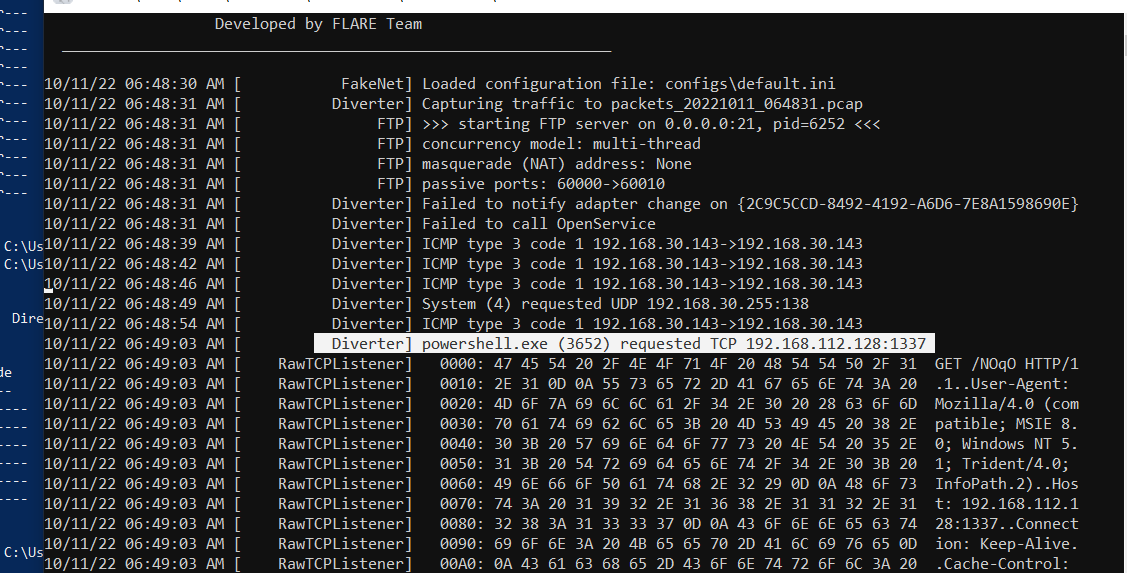








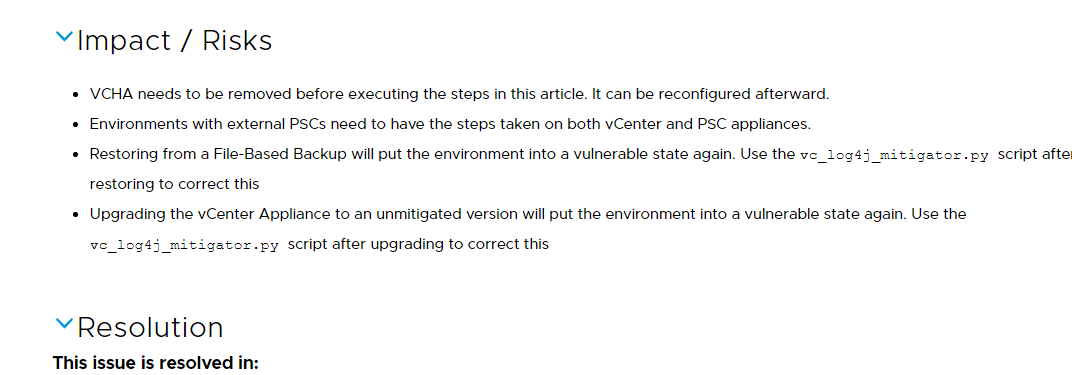




#16 What is the script name published by VMware to mitigate log4shell vulnerability?

<https://kb.vmware.com/s/article/87081>

vc\_log4j\_mitigator.py



* 1.What is the version of the log4j library used by the installed VMware product?

<https://communities.vmware.com/t5/VMware-vCenter-Discussions/vCenter-6-7-for-Windows-Build-19300125-Log4j/td-p/2910559>

* 2.What is the log4j library log level specified in the configuration file?

Google: log4j2 level file configuration vmware

<https://kb.vmware.com/s/article/2149228>

<https://docs.vmware.com/en/vRealize-Operations-Manager/8.1/com.vmware.vcom.config.doc/GUID-CE444BCB-6236-4778-8DB1-3796F3D71D7C.html>

* 3.The attacker used the log4shell.huntress.com payload to detect if vcenter instance is vulnerable. What is the first link of the log4huntress payload?

Search log4shell.huntress.com check thời gian

* 4.When was the first successful login to vsphere WebClient?

Google: vSphere Single-Sign On process writes

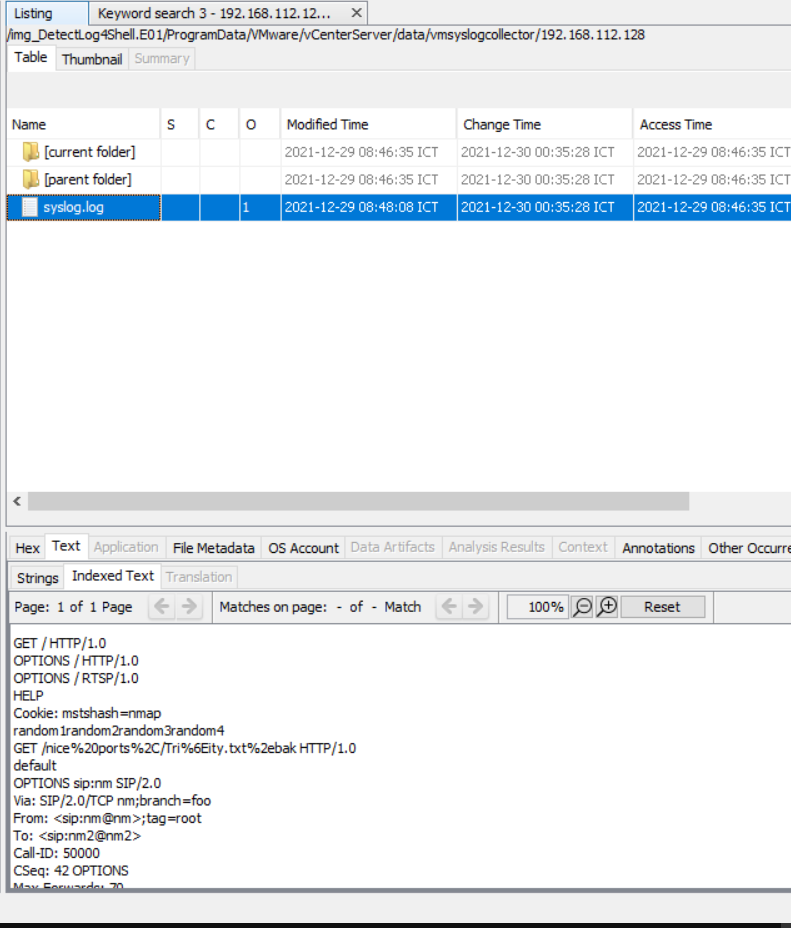
<https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-FBECACED-E9E2-4DE5-A4D2-3587D90D2420.html>

* 5.What is the attacker’s IP address?

Trong tệp Aud\_events.log, tất cả các mục nhập log4shell.huntress.com được liên kết với cùng một địa chỉ IP: 192.168.112.128

Vmware syslog collector

<https://docs.vmware.com/en/VMware-vSphere/6.0/com.vmware.vsphere.vcenterhost.doc/GUID-61E7E2EA-F531-4665-9225-58BA899F55A5.html>



Một yêu cầu http

Khác so với log localhost thông thường

* 6.What is the port the attacker used to receive the cobalt strike reverse shell?

Hint: Check Microsoft-Windows-PowerShell%4Operational.evtx. Look for encoded base64 commands

ScriptBlock: $s=New-Object IO.MemoryStream(,[Convert]::FromBase64String(""));IEX (New-Object IO.StreamReader(New-Object IO.Compression.GzipStream($s,[IO.Compression.CompressionMode]::Decompress))).ReadToEnd();

Base64 và Gzip

Giải mã đoạn script

Vẫn chưa thấy port

Có 1 đoạn base64 giải mã tiếp xem có port hay k

Chỉ thấy ip hacker như vẫn chưa thấy port

Có 2 giải pháp lưu file virus .ps1 rồi chạy xem port

Trên sandbox port 1337

Trên máy ảo + fakenet

* 7. What is the executable used by the attacker to gain persistence??

<https://www.cynet.com/attack-techniques-hands-on/the-art-of-persistence/>