

CyberDefenders QRadar 101



Sharing my thought process as I work through Cyberdefenders Qradar101 Threat Hunting lab. I've yet to experiment with Qradar, so this will be a learning experience for me.

Lab Link: <https://cyberdefenders.org/blueteam-ctf-challenges/qradar101/>

Category: Threat Hunting

Tactics: Execution, Persistence, Privilege Escalation, Defense Evasion, Discovery, Lateral Movement, Collection, Command and Control, Exfiltration

Scenario Overview

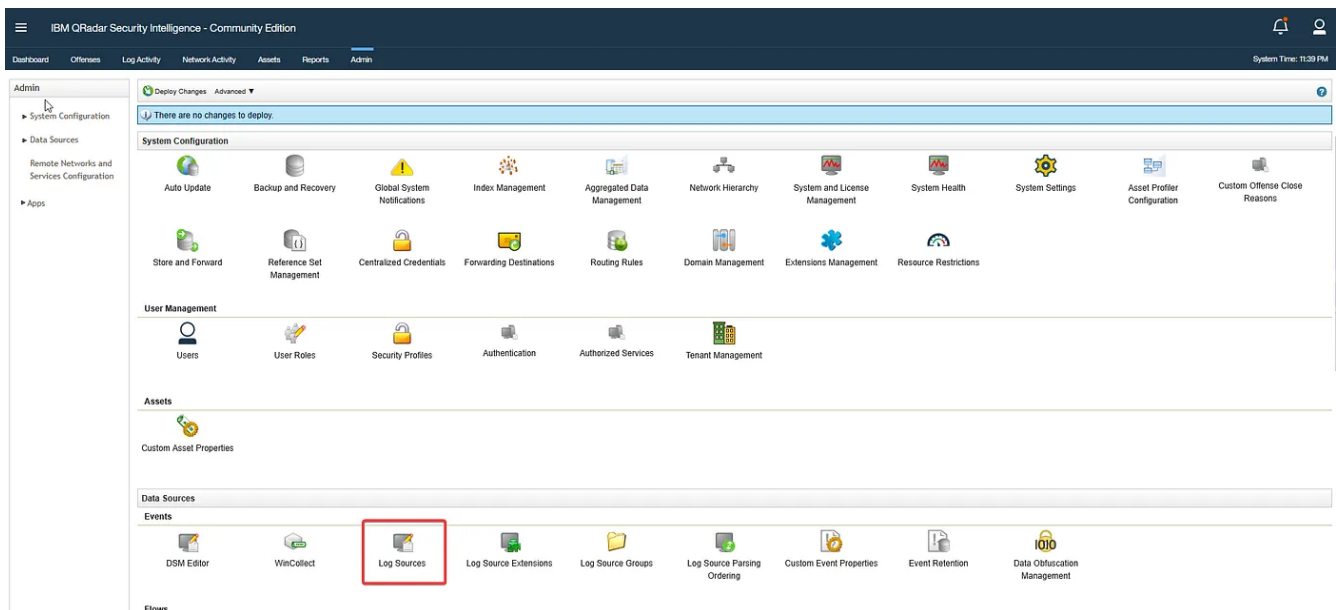
A financial company was compromised, and they are looking for a security analyst to help them investigate the incident. The company suspects that an insider helped the attacker get into the network, but they have no evidence.

The initial analysis performed by the company's team showed that many systems were compromised. Also, alerts indicate the use of well known malicious tools in the network. As a SOC analyst, you are assigned to investigate the incident using QRadar SIEM and reconstruct the events carried out by the attacker.

Threat Hunting Questions

Q1: How many log sources are available?

Navigating to the admin console, under Data Sources I obtained a list of all log sources:



192.168.20.21/console/do/core/genericsearchlist?appName=eventviewer&pageld=SensorDeviceList

Warning: This interface will be unavailable in future versions of QRadar. Download the new QRadar Log Source Management App from the IBM App Exchange.
[Don't Show Me Again](#) [Remind Me Later](#)

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		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
ptSense-Firewall	Netgate ptSense	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

Displaying 1 to 15 of 15 items (Elapsed time: 0:00:00.093)

Q2: What is the IDS software used to monitor the network?

Within log sources module, the IDS software of Suricata is listed.

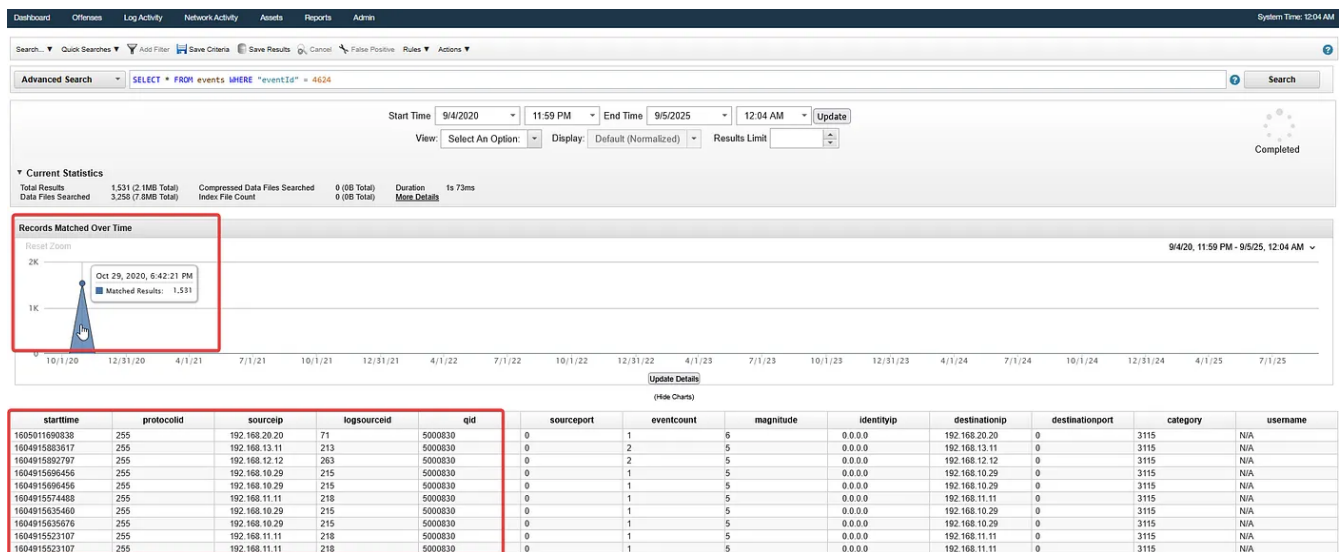
Q3: What is the domain name used in the network?

Researching the query language for Qradar, I was able to understand that Qradar utilizes [AQL](#), which seemed similar to SQL to me.

Since we are searching for the domain name, this information should be present in logins, so I ran a query to display all successful logins within the date range of 9/4/2020 through 9/4/2025 since the specific date range of the attack was not specified.

```
SELECT * FROM events WHERE "eventId" = 4624
```

The query returned 1,531 results of successful logins all occurring on October 29th, 2020.



Analyzing the first present log, I was able to inspect the payload information, in which the account domain of "HACKDEFEND.local" was present.

Payload Information

```
utf hex base64
Wrap Text
[13]Nov 18 04:34:45 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=4624
EventIDCode=4624 EventType=9 EventCategory=12544 RecordNumber=1389399 TimeGenerated=1609011682 TimeWritten=1609011682 Level=Log Always Keyword=Audit Success Task=SE_ADT_LOCAL_LOGIN OpcodeInfo MessageAn account was
successfully logged on. Subject: Security ID: NT AUTHORITY\SYSTEM Account Name: DCS Account Domain: Login ID: 8x3E7 Logon Type: 5 Impersonation Level: Impersonation New Logon: Security ID: NT AUTHORITY\SYSTEM Account Name:
SYSTEM Account Domain: NT AUTHORITY Logon ID: 8x3E7 Logon GUID: (00000000-0000-0000-0000-000000000000) Process Information: Process ID: 0x20c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network
Address: - Source Port: - Detailed Authentication Information:
```

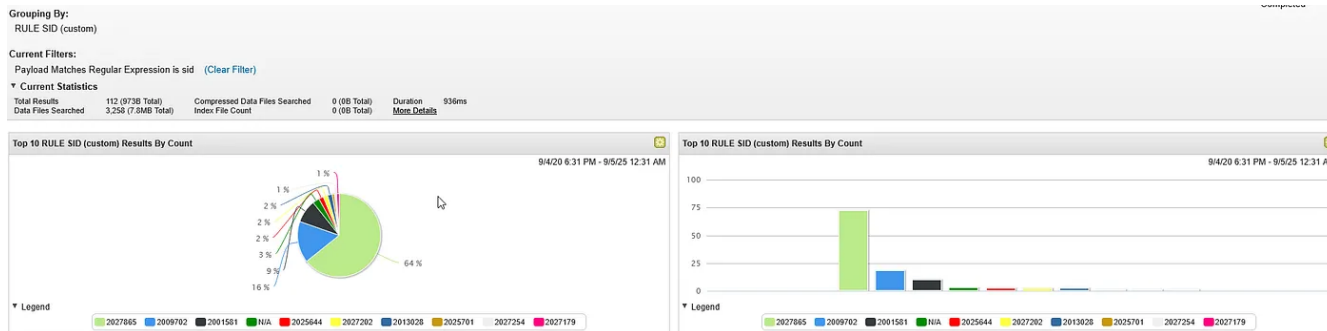
Q4: Multiple IPs were communicating with the malicious server. One of them ends with "20". Provide the full IP.

Ironically, I noticed the first IP that was given in my successful logon query ended in .20, which solved my answer.

Q5: What is the SID of the most frequent alert rule in the dataset?

As im still getting familiar with Qradar, I was unsure on how to group by a column, after doing some research, I was able to find the SID of the most frequent alert by Log Activity > Search > Edit Search > Column or Select From List.

The screenshot displays the IBM QRadar Security Intelligence - Community Edition interface. The top navigation bar includes links for Dashboard, Offenses, Log Activity, Network Activity, Assets, Reports, and Admin. Below this, the 'Manage Search Results' and 'Manage Custom Properties' tabs are visible. The main section is titled 'Advanced View Definition' and contains a 'Type Column or Select from List' input field with the text 'sid'. To the left, under 'Available Columns', the 'RULE SID (custom)' column is listed. On the right, the 'Group By' section is highlighted with a red box and contains 'RULE SID (custom)'. Below this, the 'Columns' section lists 'Event Name', 'Log Source', 'Event Count (Sum)', 'Start Time (Minimum)', 'Category', and 'Source IP'. The 'Order By' section shows 'Count' and 'Desc' selected. At the bottom, the 'Results Limit' is set to '1,000'.



By filtering on SID column, the search returns a pie chart explicitly giving me the amount of alerts with the SID associated.

The most frequent PID was associated with DNS queries to .cloud domains, flagging them as potentially bad traffic.

Q6: What is the attacker's IP address?

By reviewing the Offenses tab in Qradar, we can identify a specific offense related to excessive firewall denies between hosts. This offense tells us the source IP address that is causing these excessive firewall denies resulting in this offense.

IBM QRadar Security Intelligence - Community Edition

Dashboard **Offenses** Log Activity Network Activity Assets Reports Admin

System Time: 2:53 PM

Offenses

My Offenses

All Offenses

By Category

By Source IP

By Destination IP

By Network

Rules

Search... Save Criteria Actions Print

Last Refresh: 00:00:30

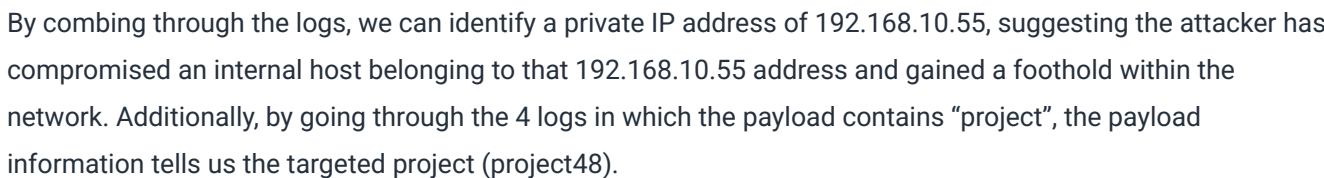
Current Search Parameters: All Offenses View Offenses with: Select An Option:

Id	Description	Offense Type	Offense Source	Magnitude	Source IPs	Destination IPs
13	Exploit Followed by Suspicious Host Activity - Chained containing Success Audit: Successful login with administrative or special privileges	Source IP	192.168.20.20	High	192.168.20.20	Multiple
18	Exploit Followed by Suspicious Host Activity - Chained containing Module Logging Command Invocation	Source IP	192.168.20.20	High	192.168.20.20	Multiple
21	Exploit Followed by Suspicious Host Activity - Chained containing Module Logging Command Invocation	Source IP	192.168.20.20	High	192.168.20.20	Multiple
2	Exploit Followed by Suspicious Host Activity - Chained containing The Group Policy settings for the user were processed successfully	Source IP	192.168.10.11	High	192.168.10.11	Multiple
6	Exploit Followed by Suspicious Host Activity - Chained containing Success Audit: Successful login with administrative or special privileges	Source IP	192.168.12.11	High	192.168.12.11	Multiple
8	Exploit Followed by Suspicious Host Activity - Chained containing Success Audit: Successful login with administrative or special privileges	Source IP	192.168.10.15	High	192.168.10.15	Multiple
11	Exploit Followed by Suspicious Host Activity - Chained containing Success Audit: Successful login with administrative or special privileges	Source IP	192.168.11.13	High	192.168.11.13	Multiple
12	Exploit Followed by Suspicious Host Activity - Chained containing Success Audit: Successful login with administrative or special privileges	Source IP	192.168.10.15	High	192.168.10.15	Multiple
14	Exploit Followed by Suspicious Host Activity - Chained containing Success Audit: Successful login with administrative or special privileges	Source IP	192.168.11.11	High	192.168.11.11	Multiple
16	Exploit Followed by Suspicious Host Activity - Chained containing Success Audit: Successful login with administrative or special privileges	Source IP	192.168.10.15	High	192.168.10.15	Multiple
19	Exploit Followed by Suspicious Host Activity - Chained containing Success Audit: Successful login with administrative or special privileges	Source IP	192.168.12.11	High	192.168.12.11	Multiple
22	Exploit Followed by Suspicious Host Activity - Chained containing Success Audit: Successful login with administrative or special privileges	Source IP	192.168.12.12	High	192.168.12.12	Multiple
23	Exploit Followed by Suspicious Host Activity - Chained containing Success Audit: Successful login with administrative or special privileges	Source IP	192.168.10.29	High	192.168.10.29	Multiple
24	Exploit Followed by Suspicious Host Activity - Chained containing Success Audit: Successful login with administrative or special privileges	Source IP	192.168.13.12	High	192.168.13.12	Multiple
25	Exploit Followed by Suspicious Host Activity - Chained containing Success Audit: Successful login with administrative or special privileges	Source IP	192.168.10.15	High	192.168.10.15	Multiple
26	Exploit Followed by Suspicious Host Activity - Chained containing Success Audit: Successful login with administrative or special privileges	Source IP	192.168.11.11	High	192.168.11.11	Multiple
3	Excessive Firewall Denies Between Hosts containing Firewall - Deny	Source IP	192.168.12.12	High	192.168.12.12	Local (250)
7	Exploit Followed by Suspicious Host Activity - Chained containing Success Audit: Successful login with administrative or special privileges	Source IP	192.168.12.12	High	192.168.12.12	Local (250)
20	Exploit Followed by Suspicious Host Activity - Chained containing Success Audit: Successful login with administrative or special privileges	Source IP	192.168.11.11	High	192.168.11.11	Local (250)
5	Multiple Login Failures for the Same User containing Failure Audit: An account failed to log on	Username	Guest	Low	192.168.10.19	Guest
9	Login Failures Followed By Success from the same Username preceded by Multiple Login Failures for the Same User containing Failure Audit: An account failed to log on	Username	gradarc collector	Low	Multiple (5)	Local (6)
17	Login Failures Followed By Success from the same Username preceded by Multiple Login Failures for the Same User containing Failure Audit: An account failed to log on	Username	gradarc collector	Low	Multiple (6)	Local (6)
10	General Authentication Successful and Admin Login Successful and User Login Failure and User Login Success	Username	gradarc collector	Low	Multiple (4)	Local (4)
15	Multiple Login Failures for the Same User containing Failure Audit: An account failed to log on	Username	Guest	Low	192.168.11.11	Guest
1	Flow Source/Interface Stopped Sending Flows	Rule	Flow Source Stopped...	Low	192.168.20.21	9.9.9.9

Displaying 1 to 26 of 26 Items (Elapsed time: 0:00:00.112)

Q7: The attacker was searching for data belonging to one of the company's projects, can you find the name of the project?

I stopped filtering by the original attacker IP address of 192.20.80.25, and decided to filter on the payload. Using a specific payload contains regular expression filter on "project" .



From the payload information and log information pertaining to the source IP, we identified the compromised host IP address of 192.168.10.15, filtering logs between May 1st, 2020, and December 30th, 2025, on the compromised host IP address and event ID 4624 for a successful logon. Through the logs, we are able to identify the compromised user “nour”.

IBM QRadar Security Intelligence - Community Edition

Dashboard Overview Log Activity Network Activity Assets Reports Admin

Search... Quick Searches Add Filter Save Entries Save Results Cancel False Positive Rules Actions

Start Time: 5/1/2020 3:43 PM End Time: 12/30/2020 3:43 PM Update

View: Select An Option Display: Default (Normalized) Results Limit

Current Filters: Source or Destination IP is 192.168.10.15 (Clear Filter) EventID (custom) is any of 4624 (Clear Filter)

Current Statistics: Total Results 109 (155KB Total) Subsearch (No Data Files) Compressed Data Files Searched Index File Count Subsearch (No Compressed Data Files) Subsearch (No Index Files) Duration 235ms

Event Name	Log Source	Event Count	Time	Low Level Category	Source IP	Source Port	Destination IP	Destination Port	Username	Magnitude
Success Audit: An account was successfully logged on	HD-FIN-03	2	Nov 8, 2020, 11:20:27 PM	User Login Success	192.168.10.15	0	192.168.10.15	0	N/A	
Success Audit: An account was successfully logged on	HD-FIN-03	2	Nov 8, 2020, 11:19:24 PM	User Login Success	192.168.10.15	0	192.168.10.15	0	N/A	
Success Audit: An account was successfully logged on	DC	1	Nov 8, 2020, 11:14:08 PM	User Login Success	192.168.10.15	50149	192.168.20.20	0	nour	
Success Audit: An account was successfully logged on	DC	1	Nov 8, 2020, 11:13:47 PM	User Login Success	192.168.10.15	50147	192.168.20.20	0	N/A	
Success Audit: An account was successfully logged on	HD-FIN-03	2	Nov 8, 2020, 11:10:06 PM	User Login Success	192.168.10.15	0	192.168.10.15	0	N/A	
Success Audit: An account was successfully logged on	HD-FIN-03	2	Nov 8, 2020, 11:05:38 PM	User Login Success	192.168.10.15	0	192.168.10.15	0	N/A	
Success Audit: An account was successfully logged on	HD-FIN-03	2	Nov 8, 2020, 11:05:35 PM	User Login Success	192.168.10.15	0	192.168.10.15	0	N/A	
Success Audit: An account was successfully logged on	DC	1	Nov 8, 2020, 10:58:42 PM	User Login Success	192.168.10.15	50113	192.168.20.20	0	N/A	
Success Audit: An account was successfully logged on	HD-FIN-03	2	Nov 8, 2020, 10:57:23 PM	User Login Success	192.168.10.15	0	192.168.10.15	0	N/A	
Success Audit: An account was successfully logged on	DC	1	Nov 8, 2020, 10:56:47 PM	User Login Success	192.168.10.15	50106	192.168.20.20	0	nour	
Success Audit: An account was successfully logged on	HD-FIN-03	2	Nov 8, 2020, 10:48:47 PM	User Login Success	192.168.10.15	0	192.168.10.15	0	N/A	
Success Audit: An account was successfully logged on	HD-FIN-03	2	Nov 8, 2020, 10:47:55 PM	User Login Success	192.168.10.15	0	192.168.10.15	0	N/A	
Success Audit: An account was successfully logged on	DC	1	Nov 8, 2020, 10:43:39 PM	User Login Success	192.168.10.15	50089	192.168.20.20	0	N/A	
Success Audit: An account was successfully logged on	HD-FIN-03	2	Nov 8, 2020, 10:42:49 PM	User Login Success	192.168.10.15	0	192.168.10.15	0	N/A	
Success Audit: An account was successfully logged on	HD-FIN-03	1	Nov 8, 2020, 10:41:35 PM	User Login Success	192.168.10.15	0	192.168.10.15	0	N/A	
Success Audit: An account was successfully logged on	HD-FIN-03	1	Nov 8, 2020, 10:36:00 PM	User Login Success	192.168.10.15	0	192.168.10.15	0	N/A	
Success Audit: An account was successfully logged on	HD-FIN-03	1	Nov 8, 2020, 10:35:48 PM	User Login Success	192.168.10.15	0	192.168.10.15	0	N/A	
Success Audit: An account was successfully logged on	DC	1	Nov 8, 2020, 10:30:15 PM	User Login Success	192.168.10.15	50024	192.168.20.20	0	nour	
Success Audit: An account was successfully logged on	DC	1	Nov 8, 2020, 10:28:39 PM	User Login Success	192.168.10.15	49967	192.168.20.20	0	N/A	
Success Audit: An account was successfully logged on	HD-FIN-03	2	Nov 8, 2020, 10:27:15 PM	User Login Success	192.168.10.15	0	192.168.10.15	0	N/A	
Success Audit: An account was successfully logged on	DC	2	Nov 8, 2020, 10:25:29 PM	User Login Success	192.168.10.15	0	192.168.10.15	0	N/A	
Success Audit: An account was successfully logged on	DC	6	Nov 8, 2020, 10:25:21 PM	User Login Success	192.168.10.15	49913	192.168.20.20	0	nour	
Success Audit: An account was successfully logged on	DC	2	Nov 8, 2020, 10:24:59 PM	User Login Success	192.168.10.15	49881	192.168.20.20	0	nour	
Success Audit: An account was successfully logged on	DC	1	Nov 8, 2020, 10:24:49 PM	User Login Success	192.168.10.15	49877	192.168.20.20	0	nour	
Success Audit: An account was successfully logged on	DC	1	Nov 8, 2020, 10:24:49 PM	User Login Success	192.168.10.15	49872	192.168.20.20	0	nour	
Success Audit: An account was successfully logged on	DC	1	Nov 8, 2020, 10:24:49 PM	User Login Success	192.168.10.15	49871	192.168.20.20	0	nour	
Success Audit: An account was successfully logged on	DC	2	Nov 8, 2020, 10:24:49 PM	User Login Success	192.168.10.15	49879	192.168.20.20	0	nour	
Success Audit: An account was successfully logged on	HD-FIN-03	8	Nov 8, 2020, 10:24:47 PM	User Login Success	192.168.10.15	0	192.168.10.15	0	N/A	
Success Audit: An account was successfully logged on	HD-FIN-03	1	Nov 8, 2020, 10:21:30 PM	User Login Success	192.168.10.15	0	192.168.10.15	0	N/A	

Displaying 81 to 109 of 109 items (Elapsed time: 0.00:00.073)

Page: 3 → < 1 2 3 >

Q10: Hackers do not like logging, what logging was the attacker checking to see if enabled?

To try and find this information, I originally tried filtering on the username “nour” and event IDs 4719 and 1102. Unfortunately, this returned unsuccessful, so I tried a different approach of filtering on events of process creation (4688). This also was unsuccessful. Instead, I focused on any logs related to the username “nour”. Looking at the first chronological logs related to nour, I found several logon/off, and a powershell console started.

Start Time: 5/1/2020 3:43 PM End Time: 12/30/2020 3:43 PM Update

View: Select An Option Display: Default (Normalized) Results Limit

Current Filters: Username is any of nour (Clear Filter)

Current Statistics: Total Results 139 (183.7KB Total) Subsearch (No Data Files) Compressed Data Files Searched Index File Count Subsearch (No Compressed Data Files) Subsearch (No Index Files) Duration 93ms

Event Name	Log Source	Event Count	Time	Low Level Category	Source IP	Source Port	Destination IP	Destination Port	Username	Magnitude
PowerShell Console Ready	HD-FIN-03	1	Nov 8, 2020, 10:38:25 PM	Information	192.168.10.15	0	192.168.10.15	0	nour	
PowerShell Console Started	HD-FIN-03	1	Nov 8, 2020, 10:38:15 PM	Information	192.168.10.15	0	192.168.10.15	0	nour	
Success Audit: An account was successfully logged on	DC	1	Nov 8, 2020, 10:30:15 PM	User Login Success	192.168.10.15	50024	192.168.20.20	0	nour	
Success Audit: An account was logged off	DC	1	Nov 8, 2020, 10:30:13 PM	Host Logout	192.168.20.20	0	192.168.20.20	0	nour	
Success Audit: An account was logged off	DC	1	Nov 8, 2020, 10:26:13 PM	Host Logout	192.168.20.20	0	192.168.20.20	0	nour	
Success Audit: An account was logged off	DC	1	Nov 8, 2020, 10:26:03 PM	Host Logout	192.168.20.20	0	192.168.20.20	0	nour	
Success Audit: An account was successfully logged on	DC	6	Nov 8, 2020, 10:25:21 PM	User Login Success	192.168.10.15	49913	192.168.20.20	0	nour	
Success Audit: An account was logged off	DC	2	Nov 8, 2020, 10:24:59 PM	Host Logout	192.168.20.20	0	192.168.20.20	0	nour	
Success Audit: An account was successfully logged on	DC	2	Nov 8, 2020, 10:24:59 PM	User Login Success	192.168.10.15	49881	192.168.20.20	0	nour	
Success Audit: An account was logged off	DC	1	Nov 8, 2020, 10:24:49 PM	Host Logout	192.168.20.20	0	192.168.20.20	0	nour	
Success Audit: An account was successfully logged on	DC	1	Nov 8, 2020, 10:24:49 PM	User Login Success	192.168.10.15	49877	192.168.20.20	0	nour	
Success Audit: A Kerberos service ticket was granted	DC	1	Nov 8, 2020, 10:24:49 PM	Kerberos Session Opened	192.168.10.15	49874	192.168.20.20	0	nour	
Success Audit: An account was successfully logged on	DC	1	Nov 8, 2020, 10:24:49 PM	User Login Success	192.168.10.15	49872	192.168.20.20	0	nour	
Success Audit: An account was logged off	DC	1	Nov 8, 2020, 10:24:49 PM	Host Logout	192.168.20.20	0	192.168.20.20	0	nour	
Success Audit: An account was successfully logged on	DC	1	Nov 8, 2020, 10:24:49 PM	User Login Success	192.168.10.15	49871	192.168.20.20	0	nour	
Success Audit: An account was successfully logged on	DC	2	Nov 8, 2020, 10:24:49 PM	User Login Success	192.168.10.15	49879	192.168.20.20	0	nour	

Following the powershell console, a ton of module logging command invocation came after, outlining the attackers use of PowerShell to possibly get more information about the environment.

Q11: Name of the second system the attacker targeted to cover up the employee?

To find information on this, we know the attacker is using PowerShell cmdlets to gain information on the

environment. To find information on the second system the attacker targeted to cover up the employee, we can filter on “Process CommandLine” containing “del”. 4 logs return, and combing through these logs, we can find a suspicious cmd command.

```
cmd.exe /Q /c del sami.xlsx 1> \\127.0.0.1\ADMIN$_1604917981.0572538 2>&1
```

IBM QRadar Security Intelligence - Community Edition

Dashboard Offenses Log Activity Network Activity Assets Reports Admin

System Time: 4:26 PM

Return to Event List Offense Map Event False Positive Extract Property Previous Next Print Obfuscation

Command (custom)	
ParentCommandLine (custom)	N/A
ParentImage (custom)	N/A
ParentImageName (custom)	N/A
Process CommandLine (custom)	cmd.exe /Q /c del sami.xlsx 1> \\127.0.0.1\ADMIN\$_1604917981.0572538 2>&1
Process Guid (custom)	N/A
Realm (custom)	N/A
Scope (custom)	N/A
Source Workstation (custom)	N/A
Domain	Default Domain

deleting files/possibly evidence, and redirecting output to ADMIN\$ would suggest attacker has gained elevated permissions

Source and Destination Information			
Source IP	192.168.13.11	Destination IP	192.168.13.11
Source Asset Name	N/A	Destination Asset Name	N/A
Source Port	0	Destination Port	0
Pre NAT Source IP		Pre NAT Destination IP	
Pre NAT Source Port	0	Pre NAT Destination Port	0
Post NAT Source IP		Post NAT Destination IP	

Examining the command that run, /Q turns on quiet mode, and /c is used to delete the file “sami.xlsx”, which could be deleting important files maybe related to project48 or possibly evidence of some sort. The output is then redirected to localhost/ADMIN\$ which requires elevated permission to succesfully run, which indicates the attacker has gained elevated permissions.

Q12: When was the first malicious connection to the domain controller (log start time – hh:mm:ss)?

Examining the first connections made to the DC we can filter on events of “Network Connection Detected”.

Q18: What is the name of the new account added by the attacker?

[illegible]

10 / 14

Q19: What is the PID of the process that performed injection?

By filtering on our infected host (192.168.10.15), and on Process Creation events, this returns 48 events. By going through the logs, we can see in the payload information the compromised user “nour” runs a suspicious file from the path “C:\Users\nour.HACKDEFEND\FSETPBEUslek.exe” responsible for the injection. PID located in the payload information.

Q20: What is the name of the tool used for lateral movement?

I struggled with identifying the answer for this, but from what I’ve researched, the cmd process that was ran earlier that showed us the attacker had gained elevated permissions by writing to >ADMIN\$, this is a common template used by wmiexec. According to Nischal Khadgi, “wmiexec allows a threat actor to execute commands on a remote system and/or establish a semi-interactive shell on a remote host. A detailed analysis along with the hunting guide is provided below”.

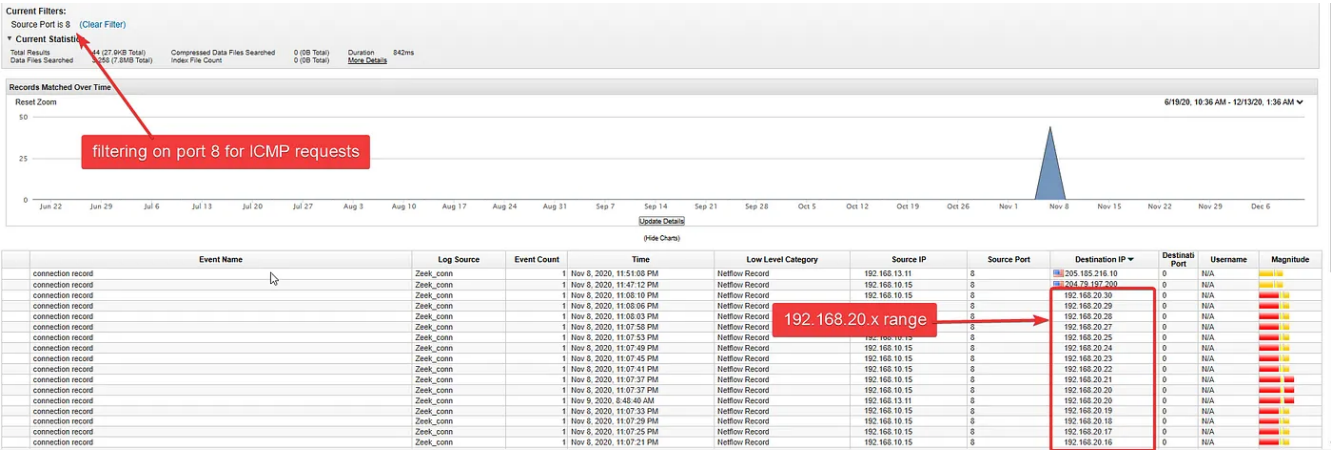
According to [Hunting for Impacket](#), wmiexec allows a threat actor to execute commands on a remote system and/or establish a semi-interactive shell on a remote host.

Source and Destination Information			
Source IP	192.168.13.11	Destination IP	192.168.13.11
Source Asset Name	N/A	Destination Asset Name	N/A
Source Port	0	Destination Port	0
Pre NAT Source IP		Pre NAT Destination IP	
Pre NAT Source Port	0	Pre NAT Destination Port	0
Post NAT Source IP		Post NAT Destination IP	

Q21: Attacker exfiltrated one file, what is the name of the tool used for exfiltration?

Knowing common ways for attackers to exfiltrate files may be through the use of curl, wget, or python servers, we can filter on these to see if any process creations are logged related to these events.

To find information on the network the threat actor scanned from the host IP 1 to 30, we can filter on port 8 for ICMP requests, and reviewing the destination IPs. Based off the logs, we can conclude from the second compromised host at 192.168.10.15, the threat actor is scanning the destination IP range from 192.168.20.X



Q24: What is the name of the employee who hired the attacker?

Going back to the suspicious .xlsx file that was exfiltrated, although we do not know the contents, we do know the file name was "sami.xlsx", which was uploaded through wmiexec.py. We can infer that sami is a name, and potentially the file came from an employee named sami, which was confirmed by the answer.

Overview

From what I observed, the attacker gained initial access through a malicious document (important_instructions.docx), which executed a payload (FSETPBEUslek.exe) on the host 192.168.10.55 under the user "nour". Using PowerShell and wmiexec.py, the attacker escalated privileges, created a new account, and moved laterally to another host (192.168.10.15). They performed host discovery using ICMP scans (possibly through the use of nmap), searched for sensitive project data related to "project48", and ultimately exfiltrated the file sami.xlsx to their external server on 192.20.80.25:8000 using curl. Finally, they attempted to cover their tracks by deleting evidence and checking logging configurations. The threat actor demonstrated thorough persistence techniques, privilege escalation, lateral movement, and data exfiltration.

Key Takeaways

- QRadar provides powerful log analysis capabilities for incident response
- Understanding AQL (Ariel Query Language) is essential for effective SIEM analysis
- Event correlation helps identify complex attack chains
- Proper log parsing and filtering is crucial for threat hunting
- Attackers often use common tools like PowerShell, wmiexec, and curl for lateral movement and exfiltration

References

- [CyberDefenders QRadar 101 Challenge](#)
- [IBM QRadar AQL Documentation](#)
- [Hunting for Impacket - WMIExec Analysis](#)



hunts.dev

Originally published on hunts.dev

<https://hunts.dev/blog/qradar101/>