

Campfire-1

DFIR · Very Easy

PLAY SHERLOCK ABOUT ACTIVITY RECOMMENDATIONS

Solve the Sherlock 1 of 7

OFFICIAL WRITEUP

Alonzo Spotted Weird files on his computer and informed the newly assembled SOC Team. Assessing the situation it is believed a Kerberoasting attack may have occurred in the network. It is your job to confirm the findings by analyzing the provided evidence.

You are provided with:

- 1- Security Logs from the Domain Controller
- 2- PowerShell-Operational Logs from the affected workstation
- 3- Prefetch Files from the affected workstation

Activation
Go to Site

▼ A long time ago

Domain Controller	5/21/2024 10:33 AM	File folder
Workstation	5/21/2024 10:33 AM	File folder

▼ A long time ago

SECURITY-DC	5/21/2024 8:52 AM	Event Log	1,092 KB
-------------	-------------------	-----------	----------

Powershell-Operational	5/21/2024 8:56 AM	Event Log	2,116 KB
2024-05-21T033012_triage_asset	5/21/2024 10:32 AM	File folder	

▼ A long time ago

prefetch	5/21/2024 10:32 AM	File folder
----------	--------------------	-------------

<input type="checkbox"/> SVCHOST.EXE-C25BD44A.pf	5/21/2024 9:00 AM	PF File	8 KB
<input type="checkbox"/> AUDIODG.EXE-AB22E9A6.pf	5/21/2024 8:58 AM	PF File	8 KB
<input type="checkbox"/> CONSENT.EXE-40419367.pf	5/21/2024 8:58 AM	PF File	122 KB
<input type="checkbox"/> SVCHOST.EXE-262B838E.pf	5/21/2024 8:58 AM	PF File	6 KB
<input type="checkbox"/> SVCHOST.EXE-D4A56B1A.pf	5/21/2024 8:58 AM	PF File	4 KB
<input type="checkbox"/> SVCHOST.EXE-9D041ABC.pf	5/21/2024 8:58 AM	PF File	5 KB
<input type="checkbox"/> SVCHOST.EXE-852EC587.pf	5/21/2024 8:58 AM	PF File	16 KB
<input type="checkbox"/> FILECOAUTH.EXE-88F71F64.pf	5/21/2024 8:58 AM	PF File	12 KB
<input type="checkbox"/> SMARTSCREEN.EXE-EACC1250.pf	5/21/2024 8:58 AM	PF File	15 KB
<input type="checkbox"/> DLLHOST.EXE-7D5CE0CA.pf	5/21/2024 8:58 AM	PF File	4 KB
<input type="checkbox"/> RUNDLL32.EXE-75313621.pf	5/21/2024 8:58 AM	PF File	4 KB
<input type="checkbox"/> WINRAR.EXE-BA8CDB31.pf	5/21/2024 8:58 AM	PF File	80 KB
<input type="checkbox"/> SVCHOST.EXE-F952D9A9.pf	5/21/2024 8:57 AM	PF File	9 KB
<input type="checkbox"/> TIWORKER.EXE-FBD79BD6.pf	5/21/2024 8:57 AM	PF File	15 KB
<input type="checkbox"/> TRUSTEDINSTALLER.EXE-766EFF52.pf	5/21/2024 8:57 AM	PF File	5 KB
<input type="checkbox"/> TASKHOSTW.EXE-2E5D4B75.pf	5/21/2024 8:57 AM	PF File	28 KB
<input type="checkbox"/> SEARCHFILTERHOST.EXE-44162447.pf	5/21/2024 8:57 AM	PF File	5 KB
<input type="checkbox"/> SEARCHPROTOCOLHOST.EXE-69C456C3....	5/21/2024 8:57 AM	PF File	6 KB

 QUESTION 1 

Analyzing Domain Controller Security Logs, can you confirm the UTC date & time when the kerberoasting activity occurred?

2024-05-21 03:18:09 

Sol:

SECURITY-DC Number of events: 293											
Level	Date and Time	Source	Event ID	Task Category							
(i) Information	5/21/2024 8:48:52 AM	Micros...	4699	Other Object Access Events							
(i) Information	5/21/2024 8:48:52 AM	Micros...	5379	User Account Management							
(i) Information	5/21/2024 8:48:52 AM	Micros...	5379	User Account Management							
(i) Information	5/21/2024 8:48:52 AM	Micros...	5379	User Account Management							
(i) Information	5/21/2024 8:48:52 AM	Micros...	4799	Security Group Management							
(i) Information	5/21/2024 8:48:51 AM	Micros...	4769	Kerberos Service Ticket Operati...							
(i) Information	5/21/2024 8:48:51 AM	Micros...	4768	Kerberos Authentication Service							
(i) Information	5/21/2024 8:48:09 AM	Micros...	4769	Kerberos Service Ticket Operati...							
(i) Information	5/21/2024 8:47:31 AM	Micros...	4771	Kerberos Authentication Service							
(i) Information	5/21/2024 8:47:31 AM	Micros...	4771	Kerberos Authentication Service							
(i) Information	5/21/2024 8:47:31 AM	Micros...	4771	Kerberos Authentication Service							
(i) Information	5/21/2024 8:47:30 AM	Micros...	4771	Kerberos Authentication Service							
(i) Information	5/21/2024 8:47:30 AM	Micros...	4771	Kerberos Authentication Service							
(i) Information	5/21/2024 8:47:30 AM	Micros...	4771	Kerberos Authentication Service							
(i) Information	5/21/2024 8:47:30 AM	Micros...	4771	Kerberos Authentication Service							
(i) Information	5/21/2024 8:47:30 AM	Micros...	4771	Kerberos Authentication Service							
(i) Information	5/21/2024 8:47:30 AM	Micros...	4771	Kerberos Authentication Service							
Event 4769, Microsoft Windows security auditing.											
General Details <table border="1"> <tr> <td>Account Name:</td><td>alonzo.spire@FORELA.LOCAL</td> </tr> <tr> <td>Account Domain:</td><td>FORELA.LOCAL</td> </tr> <tr> <td>Logon GUID:</td><td>{59f3b9b1-65ed-a449-5ac0-8ea1f68478ee}</td> </tr> </table>						Account Name:	alonzo.spire@FORELA.LOCAL	Account Domain:	FORELA.LOCAL	Logon GUID:	{59f3b9b1-65ed-a449-5ac0-8ea1f68478ee}
Account Name:	alonzo.spire@FORELA.LOCAL										
Account Domain:	FORELA.LOCAL										
Logon GUID:	{59f3b9b1-65ed-a449-5ac0-8ea1f68478ee}										
Log Name:	Security										
Source:	Microsoft Windows security	Logged:	5/21/2024 8:48:09 AM								
Event ID:	4769	Task Category:	Kerberos Service Ticket Operations								

QUESTION 2

What is the Service Name that was targeted?

SUBMIT

Sol:
MSSQLService

Event 4769, Microsoft Windows security auditing.

	Information	Date	User	Process ID	Category
1	Information	5/21/2024 8:48:09 AM	Micros...	4769	Kerberos Service Ticket Operati...
2	Information	5/21/2024 8:47:31 AM	Micros...	4771	Kerberos Authentication Service
3	Information	5/21/2024 8:47:31 AM	Micros...	4771	Kerberos Authentication Service
4	Information	5/21/2024 8:47:31 AM	Micros...	4771	Kerberos Authentication Service
5	Information	5/21/2024 8:47:30 AM	Micros...	4771	Kerberos Authentication Service
6	Information	5/21/2024 8:47:30 AM	Micros...	4771	Kerberos Authentication Service
7	Information	5/21/2024 8:47:30 AM	Micros...	4771	Kerberos Authentication Service
8	Information	5/21/2024 8:47:30 AM	Micros...	4771	Kerberos Authentication Service
9	Information	5/21/2024 8:47:30 AM	Micros...	4771	Kerberos Authentication Service
10	Information	5/21/2024 8:47:30 AM	Micros...	4771	Kerberos Authentication Service

General Details

Service Information:
Service Name: MSSQLService
Service ID: S-1-5-21-3239415629-1862073780-2394361899-1105

Log Name: Security
Source: Microsoft Windows security Logged: 5/21/2024 8:48:09 AM
Event ID: 4769 Task Category: Kerberos Service Ticket Operations

QUESTION 3

It is really important to identify the Workstation from which this activity occurred. What is the IP Address of the workstation?

XX.X.X

SUBMIT

Event 4769, Microsoft Windows security auditing.

	Information	Date	User	Process ID	Category
1	Information	5/21/2024 8:48:09 AM	Micros...	4769	Kerberos Service Ticket Operati...
2	Information	5/21/2024 8:47:31 AM	Micros...	4771	Kerberos Authentication Service
3	Information	5/21/2024 8:47:31 AM	Micros...	4771	Kerberos Authentication Service
4	Information	5/21/2024 8:47:31 AM	Micros...	4771	Kerberos Authentication Service
5	Information	5/21/2024 8:47:30 AM	Micros...	4771	Kerberos Authentication Service

General Details

Service ID: S-1-5-21-3239415629-1862073780-2394361899-1105

Network Information:
Client Address: ::ffff:172.17.79.129
Client Port: 58107

Additional Information:
Ticket Options: 0x40800000
Ticket Encryption Type: 0x17
Failure Code: 0x0

Now that we have identified the workstation, a triage including PowerShell logs and Prefetch files are provided to you for some deeper insights so we can understand how this activity occurred on the endpoint. What is the name of the file used to Enumerate Active directory objects and possibly find Kerberoastable accounts in the network?

powerview.ps1



Warning	5/21/2024 8:47:25 AM	PowerShell (Microsoft-Windows-PowerShell)	4104 Execute a Remote Command
Warning	5/21/2024 8:47:25 AM	PowerShell (Microsoft-Windows-PowerShell)	4104 Execute a Remote Command
Warning	5/21/2024 8:47:23 AM	PowerShell (Microsoft-Windows-PowerShell)	4104 Execute a Remote Command
Warning	5/21/2024 8:47:23 AM	PowerShell (Microsoft-Windows-PowerShell)	4104 Execute a Remote Command
Warning	5/21/2024 8:47:23 AM	PowerShell (Microsoft-Windows-PowerShell)	4104 Execute a Remote Command
Warning	5/21/2024 8:46:32 AM	PowerShell (Microsoft-Windows-PowerShell)	4104 Execute a Remote Command
Warning	5/21/2024 8:46:32 AM	PowerShell (Microsoft-Windows-PowerShell)	4104 Execute a Remote Command
Warning	5/21/2024 8:46:32 AM	PowerShell (Microsoft-Windows-PowerShell)	4104 Execute a Remote Command
Warning	5/21/2024 8:46:32 AM	PowerShell (Microsoft-Windows-PowerShell)	4104 Execute a Remote Command

Event 4104, PowerShell (Microsoft-Windows-PowerShell)

General Details

```
elseif($Properties[$_.count -eq 1] {  
    $ObjectProperties[$_] = $Properties[$_] [0]  
}  
else {  
    $ObjectProperties[$_] = $Properties[$_]  
}  
}
```

ScriptBlock ID: a6fb3be0-d713-45d0-a227-e94dea7b9928
[Path: C:\Users\alonzo.spire\Downloads\powerview.ps1]

Log Name: Microsoft-Windows-PowerShell/Operational
Source: PowerShell (Microsoft-Windows-PowerShell) Logged: 5/21/2024 8:47:25 AM
Event ID: 4104 Task Category: Execute a Remote Command
Level: Warning Keywords: None
User: S-1-5-21-3239415629-186207 Computer: Forela-Wkstn001.forela.local
OpCode: On create calls

What is the full path of the tool used to perform the actual kerberoasting attack?

C:\full\path\to\file.ext

SUBMIT

There are several tools that can be used to perform kerberoasting like [impacket](#), [Rubeus](#), [PowerSploit \(Invoke-Kerberoast\)](#) but when we are given with prefetch mean its 90% Rubeus since impacket was written in C#.

in python and PowerSploit is powershell script and to confirm this we will use `PECmd.exe -d prefetch --csv . --csvf prefetch.csv` to parse prefetch files, process them and output it in csv format

```
Processing C:\Users\dexter14\Downloads\campfire_1\Triage\Workstation\2024-05-21T033012_triage_asset\C\Windows\prefetch\WWAHOST.EXE

Created on: 2024-05-21 05:02:37
Modified on: 2023-05-02 14:28:13
Last accessed on: 2024-05-21 05:02:37

Executable name: WWAHOST.EXE
Hash: 2CFA09D4
File size (bytes): 315,342
Version: Windows 10 or Windows 11

Run count: 3
Last run: 2023-05-02 14:28:08
Other run times: 2023-03-08 11:17:24, 2023-03-08 09:52:06

Volume information:

#0: Name: \VOLUME{01d951602330db46-52233816} Serial: 52233816 Created: 2023-03-08 01:48:53 Directories: 64 File references: 944

Directories referenced: 64

#0: \VOLUME{01d951602330db46-52233816}\PROGRAMDATA
#1: \VOLUME{01d951602330db46-52233816}\PROGRAMDATA\MICROSOFT
#2: \VOLUME{01d951602330db46-52233816}\PROGRAMDATA\MICROSOFT\WINDOWS
#3: \VOLUME{01d951602330db46-52233816}\PROGRAMDATA\MICROSOFT\WINDOWS\APPREPOSITORY
#4: \VOLUME{01d951602330db46-52233816}\PROGRAMDATA\MICROSOFT\WINDOWS\APPREPOSITORY\PACKAGES
#5: \VOLUME{01d951602330db46-52233816}\PROGRAMDATA\MICROSOFT\WINDOWS\APPREPOSITORY\PACKAGES\MICROSOFT.WINDOWS.CLOUDEXPERIENCEHOST_2TXYEWY
#6: \VOLUME{01d951602330db46-52233816}\PROGRAMDATA\MICROSOFT\WINDOWS\APPREPOSITORY\PACKAGES\MICROSOFTWINDOWS.UNDOCKEDDEVKIT_10.0.19
```

```
C:\> Tools > PECmd > prefetch.csv
```

Note	SourceFilename	SourceCreated	SourceModified	SourceAccessed	ExecutableName	Hash	Size	Version	RunCount
1	J:\Users\dexter14\Downloads\campfire_1\Triage\Workstation\2024-05-21T033012_triage_asset\	C:\Windows\prefet							
2	J:\Users\dexter14\Downloads\campfire_1\Triage\Workstation\2024-05-21T033012_triage_asset\	C:\Windows\prefet							
3	J:\Users\dexter14\Downloads\campfire_1\Triage\Workstation\2024-05-21T033012_triage_asset\	C:\Windows\prefet							
4	J:\Users\dexter14\Downloads\campfire_1\Triage\Workstation\2024-05-21T033012_triage_asset\	C:\Windows\prefet							
5	J:\Users\dexter14\Downloads\campfire_1\Triage\Workstation\2024-05-21T033012_triage_asset\	C:\Windows\prefet							
6	J:\Users\dexter14\Downloads\campfire_1\Triage\Workstation\2024-05-21T033012_triage_asset\	C:\Windows\prefet							
7	J:\Users\dexter14\Downloads\campfire_1\Triage\Workstation\2024-05-21T033012_triage_asset\	C:\Windows\prefet							
8	J:\Users\dexter14\Downloads\campfire_1\Triage\Workstation\2024-05-21T033012_triage_asset\	C:\Windows\prefet							
9	J:\Users\dexter14\Downloads\campfire_1\Triage\Workstation\2024-05-21T033012_triage_asset\	C:\Windows\prefet							
10	J:\Users\dexter14\Downloads\campfire_1\Triage\Workstation\2024-05-21T033012_triage_asset\	C:\Windows\prefet							
11	J:\Users\dexter14\Downloads\campfire_1\Triage\Workstation\2024-05-21T033012_triage_asset\	C:\Windows\prefet							
12	J:\Users\dexter14\Downloads\campfire_1\Triage\Workstation\2024-05-21T033012_triage_asset\	C:\Windows\prefet							
13	J:\Users\dexter14\Downloads\campfire_1\Triage\Workstation\2024-05-21T033012_triage_asset\	C:\Windows\prefet							
14	J:\Users\dexter14\Downloads\campfire_1\Triage\Workstation\2024-05-21T033012_triage_asset\	C:\Windows\prefet							
15	J:\Users\dexter14\Downloads\campfire_1\Triage\Workstation\2024-05-21T033012_triage_asset\	C:\Windows\prefet							
16	J:\Users\dexter14\Downloads\campfire_1\Triage\Workstation\2024-05-21T033012_triage_asset\	C:\Windows\prefet							
17	J:\Users\dexter14\Downloads\campfire_1\Triage\Workstation\2024-05-21T033012_triage_asset\	C:\Windows\prefet							
18	J:\Users\dexter14\Downloads\campfire_1\Triage\Workstation\2024-05-21T033012_triage_asset\	C:\Windows\prefet							
19	J:\Users\dexter14\Downloads\campfire_1\Triage\Workstation\2024-05-21T033012_triage_asset\	C:\Windows\prefet							
20	J:\Users\dexter14\Downloads\campfire_1\Triage\Workstation\2024-05-21T033012_triage_asset\	C:\Windows\prefet							
21	J:\Users\dexter14\Downloads\campfire_1\Triage\Workstation\2024-05-21T033012_triage_asset\	C:\Windows\prefet							
22	J:\Users\dexter14\Downloads\campfire_1\Triage\Workstation\2024-05-21T033012_triage_asset\	C:\Windows\prefet							

What is the full path of the tool used to perform the actual kerberoasting attack?

C:\Users\Alonzo.Spire\Downloads\RUBEUS.EXE



```
ampfire_1\Triage\Workstation\2024-05-21T033012_triage_asset\Windows\prefetch\RUBEUS.E  
ampfire_1\Triage\Workstation\2024-05-21T033012_triage_asset\Windows\prefetch\RUNDLL32  
ampfire_1\Triage\Workstation\2024-05-21T033012_triage_asset\Windows\prefetch\RUNDLL32  
ampfire_1\Triage\Workstation\2024-05-21T033012_triage_asset\Windows\prefetch\RUNDLL32  
ampfire_1\Triage\Workstation\2024-05-21T033012_triage_asset\Windows\prefetch\RUNDLL32
```

QUESTION 7

When was the tool executed to dump credentials? (UTC)

2024-05-21 03:18:08



RUBEUS.EXE-5873E24B.pf

Key Learning:

🔑 Key Learnings – Campfire-1 (Kerberoasting Investigation)

1 Prefetch is critical for proving execution

Domain Controller Security logs (Event ID 4769) indicate Kerberos service ticket activity, but they do not prove which tool was executed on the endpoint. Prefetch artifacts provide definitive evidence of **actual binary execution**, including execution timestamps and run count.

2 Correlation of multiple artifacts is essential

Kerberoasting detection requires correlating **DC Kerberos logs**, **PowerShell operational logs**, and **endpoint Prefetch artifacts**. No single log source provides the full picture on its own.

3 Single execution is enough to leave evidence

Even a **single execution** of an attacker tool (e.g., Rubeus.exe) generates a Prefetch file, making Prefetch a reliable artifact for detecting one-time post-exploitation activity.

4 Prefetch timestamps help confirm attack timing

Prefetch last-execution timestamps can be aligned with Kerberos TGS request spikes to accurately determine **when Kerberoasting occurred**, even if command-line arguments are not available.

5 Command-line arguments are not always recoverable

Prefetch artifacts do not store full command-line arguments. Analysts must infer attacker intent through **behavioral correlation** rather than relying solely on direct command reconstruction.

⑥ Security logs show impact, not cause

Windows Security logs show the **effect** of Kerberoasting (ticket requests), while Prefetch artifacts reveal the **cause** (tool execution), reinforcing the need for endpoint-level forensic analysis.