

1 Phân tích luồng sự cố

Sử dụng công cụ open source hayabusa [Yamato-Security/hayabusa: Hayabusa \(隼\) is a sigma-based threat hunting and fast forensics timeline generator for Windows event logs. \(github.com\)](https://github.com/Yamato-Security/hayabusa) phân tích folder chứa winevt logs thì rule của hayabusa đưa ra rất nhiều alert

Top critical alerts:	Top high alerts:
n/a n/a n/a n/a n/a	External Remote SMB Logon from Public IP (42) User Added To Local Admin Grp (21) User Added To Global Domain Admins Grp (1) n/a n/a
Top medium alerts:	Top low alerts:
Potentially Malicious PwSh (275) Standard User In High Privileged Group (77) Uncommon New Firewall Rule Added In Windows Firewall Excepti... (37) A Rule Has Been Deleted From The Windows Firewall Exception ... (20) Certificate Private Key Acquired (20)	Logon Failure (Wrong Password) (4,312) Windows Firewall Settings Have Been Changed (38) Firewall Rule Modified In The Windows Firewall Exception Lis... (30) Local User Account Created (22) A Member Was Added to a Security-Enabled Global Group (3)
Top informational alerts:	
Task Executed (359) Kerberos Service Ticket Requested (186) Proc Exec (177) Task Updated (161) WMI Provider Started (128)	Admin Logon (104) Logoff (96) Kerberos TGT Requested (84) NTLM Auth (49) Logon (Network) (43)

Nhìn vào số lượng event Logon Failure(Wrong Passord) là 4312 cho thấy đây là dấu hiện của việc bị bruteforce .

Timestamp	RuleTitle	Level	Computer	Channel	EventID	RuleAuth
2022-05-19 01:08:07.456 +07:00	Logon Failure (Unknown)	low	WIN-090257RHSSD	Sec		4625 Zach Mat
2022-08-01 21:16:45.044 +07:00	Logon Failure (Wrong P	low	dev.cyberdefenders.org	Sec		4625 Zach Mat
2022-08-01 21:16:50.073 +07:00	Logon Failure (Unknown)	low	dev.cyberdefenders.org	Sec		4625 Zach Mat
2022-08-01 21:28:35.846 +07:00	Logon Failure (Wrong P	low	dev.cyberdefenders.org	Sec		4625 Zach Mat
2022-08-01 23:18:43.958 +07:00	Logon Failure (Wrong P	low	dev.cyberdefenders.org	Sec		4625 Zach Mat
2022-08-01 23:19:35.884 +07:00	Logon Failure (Wrong P	low	dev.cyberdefenders.org	Sec		4625 Zach Mat
2022-08-01 23:19:45.684 +07:00	Logon Failure (Wrong P	low	dev.cyberdefenders.org	Sec		4625 Zach Mat
2022-08-01 23:19:53.009 +07:00	Logon Failure (Wrong P	low	dev.cyberdefenders.org	Sec		4625 Zach Mat
2022-08-01 23:20:03.274 +07:00	Logon Failure (Wrong P	low	dev.cyberdefenders.org	Sec		4625 Zach Mat
2022-08-01 23:20:12.340 +07:00	Logon Failure (Wrong P	low	dev.cyberdefenders.org	Sec		4625 Zach Mat
2022-08-01 23:26:01.602 +07:00	Logon Failure (Wrong P	low	dev.cyberdefenders.org	Sec		4625 Zach Mat
2022-08-01 23:26:14.552 +07:00	Logon Failure (Wrong P	low	dev.cyberdefenders.org	Sec		4625 Zach Mat
2022-08-01 23:29:09.460 +07:00	Logon Failure (Wrong P	low	dev.cyberdefenders.org	Sec		4625 Zach Mat
2022-08-01 23:29:09.465 +07:00	Logon Failure (Wrong P	low	dev.cyberdefenders.org	Sec		4625 Zach Mat
2022-08-01 23:29:09.617 +07:00	Logon Failure (Wrong P	low	dev.cyberdefenders.org	Sec		4625 Zach Mat
2022-08-01 23:29:09.617 +07:00	Logon Failure (Wrong P	low	dev.cyberdefenders.org	Sec		4625 Zach Mat
2022-08-01 23:29:09.804 +07:00	Logon Failure (Wrong P	low	dev.cyberdefenders.org	Sec		4625 Zach Mat
2022-08-01 23:29:09.831 +07:00	Logon Failure (Wrong P	low	dev.cyberdefenders.org	Sec		4625 Zach Mat
2022-08-01 23:29:09.845 +07:00	Logon Failure (Wrong P	low	dev.cyberdefenders.org	Sec		4625 Zach Mat
2022-08-01 23:29:09.961 +07:00	Logon Failure (Wrong P	low	dev.cyberdefenders.org	Sec		4625 Zach Mat
2022-08-01 23:29:10.110 +07:00	Logon Failure (Wrong P	low	dev.cyberdefenders.org	Sec		4625 Zach Mat
2022-08-01 23:29:10.127 +07:00	Logon Failure (Wrong P	low	dev.cyberdefenders.org	Sec		4625 Zach Mat
2022-08-01 23:29:10.144 +07:00	Logon Failure (Wrong P	low	dev.cyberdefenders.org	Sec		4625 Zach Mat
2022-08-01 23:29:10.314 +07:00	Logon Failure (Wrong P	low	dev.cyberdefenders.org	Sec		4625 Zach Mat
2022-08-01 23:29:10.432 +07:00	Logon Failure (Wrong P	low	dev.cyberdefenders.org	Sec		4625 Zach Mat
2022-08-01 23:29:10.462 +07:00	Logon Failure (Wrong P	low	dev.cyberdefenders.org	Sec		4625 Zach Mat
2022-08-01 23:29:10.469 +07:00	Logon Failure (Wrong P	low	dev.cyberdefenders.org	Sec		4625 Zach Mat
2022-08-01 23:29:10.486 +07:00	Logon Failure (Wrong P	low	dev.cyberdefenders.org	Sec		4625 Zach Mat

Nhìn vào timestamp liên tiếp nhau trong 1 thời gian ngắn càng khẳng định là computer này đã bị bruteforce

Level	Date and Time	Source	Event ID	Task Category
Information	8/1/2022 11:32:33 PM	Microsoft Windows security a...	4625	Logon
Information	8/1/2022 11:32:33 PM	Microsoft Windows security a...	4625	Logon
Information	8/1/2022 11:32:33 PM	Microsoft Windows security a...	4625	Logon
Information	8/1/2022 11:32:33 PM	Microsoft Windows security a...	4776	Credential Validation
Information	8/1/2022 11:32:33 PM	Microsoft Windows security a...	4672	Special Logon
Information	8/1/2022 11:32:33 PM	Microsoft Windows security a...	4624	Logon
Information	8/1/2022 11:32:33 PM	Microsoft Windows security a...	4625	Logon

Event 4624, Microsoft Windows security auditing.

General Details

Logon GUID: {00000000-0000-0000-0000-000000000000}

Process Information:

Process ID: 0x0

Process Name: -

Network Information:

Workstation Name: kali

Source Network Address: 192.168.1.60

Source Port: 0

Detailed Authentication Information:

Logon Process: NtLmSsp

Authentication Package: NTLM

Transited Services: -

Package Name (NTLM only): NTLM V2

Key Length: 128

Log Name: Security

Source: Microsoft Windows security ; Logged: 8/1/2022 11:32:33 PM

Event ID: 4624 Task Category: Logon

Level: Information Keywords: Audit Success

User: N/A Computer: dev.cyberdefenders.org

OpCode: Info

Chúng ta có thể thấy ip của attacker là 192.168.1.60

Timestamp	RuleTitle	Level	Computer	Channel	EventID	RuleAuthor	RuleMci	Status	Record	Details	ExtraFie	MitreTactics
2022-08-01 23:32:34.140 +07:00	RDS Logon	info	dev.cyberdefenders.org	RDS-RCM	1149	Zach Mathis	#####	stable	2639	User: squadronwar	◆◆	LatMov
2022-08-01 23:32:44.081 +07:00	RDS Logon	info	dev.cyberdefenders.org	RDS-RCM	1149	Zach Mathis	#####	stable	2761	User: interjectaerobics	-	LatMov
2022-08-01 23:32:53.768 +07:00	RDS Logon	info	dev.cyberdefenders.org	RDS-RCM	1149	Zach Mathis	#####	stable	2880	User: infestedmerchant	-	LatMov
2022-08-01 23:33:03.592 +07:00	RDS Logon	info	dev.cyberdefenders.org	RDS-RCM	1149	Zach Mathis	#####	stable	3001	User: turtledovercall	◆	LatMov
2022-08-01 23:33:13.409 +07:00	RDS Logon	info	dev.cyberdefenders.org	RDS-RCM	1149	Zach Mathis	#####	stable	3119	User: harrashusky	◆◆	LatMov
2022-08-01 23:34:57.526 +07:00	RDS Logon	info	dev.cyberdefenders.org	RDS-RCM	1149	Zach Mathis	#####	stable	4413	User: administrator	◆◆	LatMov
2022-08-01 23:46:10.910 +07:00	RDS Logon	info	dev.cyberdefenders.org	RDS-RCM	1149	Zach Mathis	#####	stable	4416	User: administrator	◆◆	LatMov

Có vẻ như nó đã dùng RDP để bruteforce chúng ta có thể thấy hayabusa đưa ra alert là có những user này đã login thành công trong thời gian máy bị bruteforce đăng nhập bằng RDP

Microsoft-Windows-TerminalServices-RemoteConnectionManager%4Operational Number of events: 1,990				
Level	Date and Time	Source	Event ID	Task Category
Information	8/1/2022 11:32:17 PM	TerminalServices-RemoteCon...	261	None
Information	8/1/2022 11:32:17 PM	TerminalServices-RemoteCon...	261	None
Information	8/1/2022 11:32:17 PM	TerminalServices-RemoteCon...	261	None
Information	8/1/2022 11:32:17 PM	TerminalServices-RemoteCon...	261	None
Information	8/1/2022 11:32:17 PM	TerminalServices-RemoteCon...	261	None
Information	8/1/2022 11:32:17 PM	TerminalServices-RemoteCon...	261	None
Information	8/1/2022 11:32:17 PM	TerminalServices-RemoteCon...	261	None
Information	8/1/2022 11:32:17 PM	TerminalServices-RemoteCon...	261	None
Information	8/1/2022 11:32:17 PM	TerminalServices-RemoteCon...	261	None
Information	8/1/2022 11:32:17 PM	TerminalServices-RemoteCon...	261	None
Information	8/1/2022 11:32:17 PM	TerminalServices-RemoteCon...	261	None
Information	8/1/2022 11:32:18 PM	TerminalServices-RemoteCon...	261	None
Information	8/1/2022 11:32:18 PM	TerminalServices-RemoteCon...	261	None
Information	8/1/2022 11:32:18 PM	TerminalServices-RemoteCon...	261	None
Information	8/1/2022 11:32:18 PM	TerminalServices-RemoteCon...	261	None
Information	8/1/2022 11:32:18 PM	TerminalServices-RemoteCon...	261	None
Information	8/1/2022 11:32:18 PM	TerminalServices-RemoteCon...	261	None
Information	8/1/2022 11:32:18 PM	TerminalServices-RemoteCon...	261	None
Information	8/1/2022 11:32:18 PM	TerminalServices-RemoteCon...	261	None
Information	8/1/2022 11:32:18 PM	TerminalServices-RemoteCon...	261	None
Information	8/1/2022 11:32:18 PM	TerminalServices-RemoteCon...	261	None
Information	8/1/2022 11:32:18 PM	TerminalServices-RemoteCon...	261	None
Information	8/1/2022 11:32:19 PM	TerminalServices-RemoteCon...	261	None
Information	8/1/2022 11:32:19 PM	TerminalServices-RemoteCon...	261	None
Information	8/1/2022 11:32:19 PM	TerminalServices-RemoteCon...	261	None

Chúng ta có thể thấy số lượng eventid 261 rất nhiều vào time bị bruteforce cho thấy rõ ràng việc attacker đã bruteforce bằng RDP

Microsoft-Windows-TerminalServices-RemoteConnectionManager%4Operational Number of events: 1,990				
Filtered: Log: file:///D:/SOC_intern_NCS_CTF/OneDrive_2024-03-20/Endpoint				
Level	Date and Time	Source	Event ID	Task Category
Information	8/1/2022 11:32:34 PM	TerminalServices-RemoteCon...	1149	None
Information	8/1/2022 11:32:44 PM	TerminalServices-RemoteCon...	1149	None
Information	8/1/2022 11:32:53 PM	TerminalServices-RemoteCon...	1149	None
Information	8/1/2022 11:33:03 PM	TerminalServices-RemoteCon...	1149	None
Information	8/1/2022 11:33:13 PM	TerminalServices-RemoteCon...	1149	None
Information	8/1/2022 11:34:57 PM	TerminalServices-RemoteCon...	1149	None
Information	8/1/2022 11:46:10 PM	TerminalServices-RemoteCon...	1149	None

Event 1149, TerminalServices-RemoteConnectionManager				
General Details				
Remote Desktop Services: User authentication succeeded: User: administrator Domain: Source Network Address: 192.168.1.60				
Log Name: Microsoft-Windows-TerminalServices-RemoteConnectionManager/Operational Source: TerminalServices-RemoteCor Logged: 8/1/2022 11:46:10 PM Event ID: 1149 Task Category: None Level: Information Keywords: User: NETWORK SERVICE Computer: dev.cyberdefenders.org OpCode: Info				

Nó đã bruteforce thành công 6 tài khoản trong đó có administrator . Vào lúc 11:46 attacker có vẻ như đã đăng nhập vào tài khoản này

2 Phân tích file độc hại sự cố

Không có file độc hại

3.IOC

IP : 192[.]168[.]1[.]60

4.Mitre&ATTCK mapping

Brute Force [Brute Force, Technique T1110 - Enterprise | MITRE ATT&CK®](#)