RDP Brute Force Attack and Log Review with Wazuh

What is RDP Brute Force Attack?

Remote Desktop Protocol (RDP) attack is an attack that provides remote access to the target computer. The aim of the attack is to try matching pre-determined username and password lists on the target computer until a correct match is found. In Windows operating systems, port 3389 is used for remote access (remote desktop). For this attack to be carried out on the target computer, this port must be open.

RDP Brute Force Scenario

Target Machine: Windows 10 Pro

Main Machine: Kali Linux

Tools Used: Hydra, Nmap

Before starting an example of an RDP Brute Force attack, it should be noted that the “Remote Desktop” feature must be enabled on the target computer running Windows operating system. This can be activated by navigating through “Start>Settings>System>Remote Desktop”.

Firstly, we scan the IP address of the target computer using Nmap with the help of Kali Linux.

```
┌──(root㉿kalinew)-[/home/kalitest9]
└─# nmap 192.168.
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-02 07:19 EDT
Nmap scan report for 192.168.
Host is up (0.00049s latency).
Not shown: 993 closed tcp ports (reset)
PORT     STATE    SERVICE
135/tcp  filtered msrpc
139/tcp  filtered netbios-ssn
445/tcp  filtered microsoft-ds
902/tcp  open     iss-realsecure
912/tcp  open     apex-mesh
2179/tcp open     vmrdp
3389/tcp open     ms-wbt-server
MAC Address:                (Hon Hai Precision Ind.)

Nmap done: 1 IP address (1 host up) scanned in 1.79 seconds
```

Figure 1.1

As shown in Figure 1.1, with port 3389 open, we wrote various username and password combinations into the userlisthydra.txt and passlisthydra.txt files that we created on the desktop of our Kali Linux computer. We will perform an RDP brute force attack on the target computer using these lists with “Hydra”.

In Figure 1.2, we see that a successful RDP Brute Force attack was performed on the target machine. Since our .txt files were unable to detect a successful username or password, we received an output of “0 valid password”.

```
┌──(root㉿kali99)-[/home/kali99/Desktop]
└─# hydra -L userlisthydra.txt -P passlisthydra.txt rdp://192.168.
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizat
ions, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-05-02 14:14:12
[WARNING] rdp servers often don't like many connections, use -t 1 or -t 4 to reduce the number of parallel connect
ions and -W 1 or -W 3 to wait between connection to allow the server to recover
[INFO] Reduced number of tasks to 4 (rdp does not like many parallel connections)
[WARNING] the rdp module is experimental. Please test, report - and if possible, fix.
[DATA] max 4 tasks per 1 server, overall 4 tasks, 9 login tries (l:3/p:3), ~3 tries per task
[DATA] attacking rdp://192.168.    :3389/
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-05-02 14:14:15
```

Figure 1.2

How to Detect RDP Brute Force Attack with Wazuh?

After performing the RDP Brute Force attack, we will examine all successful and unsuccessful brute force attempts using our Wazuh product. We connect to the Wazuh server with our Kali Linux operating system and access the Wazuh dashboard. We will perform our log analysis here.

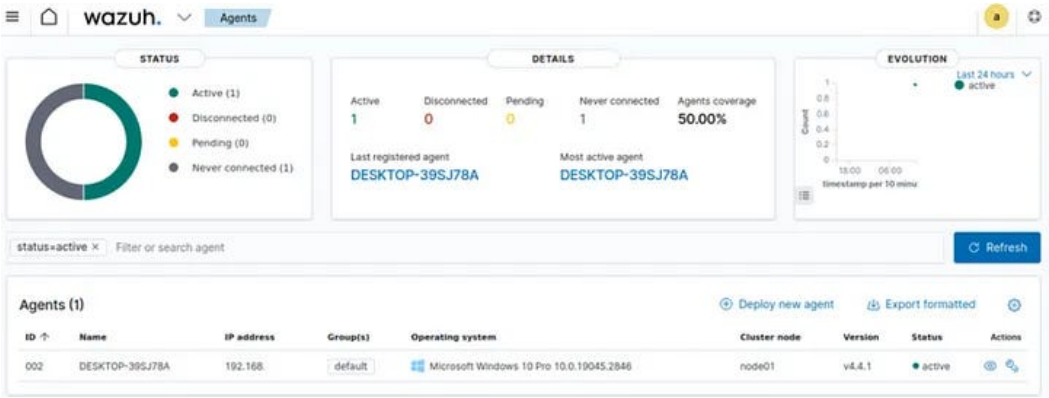


Figure 2.1

The Wazuh Dashboard interface is shown in Figure 2.1. In the Agents section, we can see the Wazuh Agent installed on the target machine running Windows operating system actively. After clicking on our Wazuh Agent, we can view all the logs recorded in the 'Security Events' section.

We can identify RDP Brute Force attacks with two rule.ids for computers running Windows OS, which are rule.id: (60122 or 60204).

rule.id: 60122 indicates login failures (logon failure),

rule.id: 60204 indicates multiple login failures (multiple logon failure), which means brute force attacks.

Additionally, **rule.id: 60106** shows that a successful login occurred on the Windows computer. We can see all of them in detail in Figure 2.2

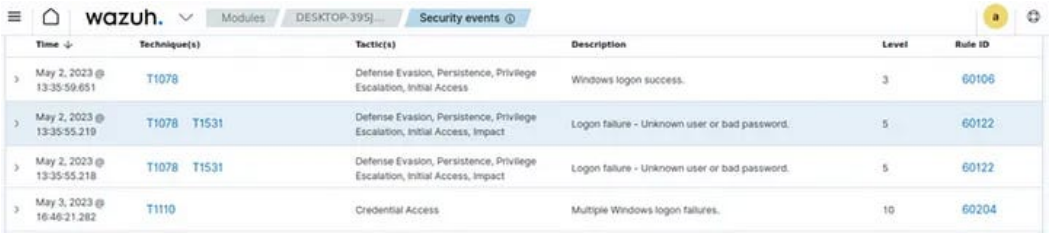


Figure 2.2

Detected Logs for RDP Brute Force Attack

To detect RDP brute force attacks, we can check for event IDs 4624 and 4625. We will use the Windows Event Viewer to examine these two event IDs more closely. To access Event Viewer, we use the path "Control Panel > System and Security > Administrative Tools".

We had performed an RDP brute force attack on our target Windows computer and had installed the Wazuh Agent on it. We can view the logs

of this attack in Event Viewer, as shown in Figure 3.1.

Dene...	3.05.2023 23:47:37	Micr...	4624	Logon
Hata...	3.05.2023 23:46:20	Micr...	4625	Logon
Hata...	3.05.2023 23:46:20	Micr...	4625	Logon
Hata...	3.05.2023 23:46:20	Micr...	4625	Logon
Hata...	3.05.2023 23:46:20	Micr...	4625	Logon
Hata...	3.05.2023 23:46:20	Micr...	4625	Logon
Hata...	3.05.2023 23:46:19	Micr...	4625	Logon
Hata...	3.05.2023 23:46:19	Micr...	4625	Logon
Hata...	3.05.2023 23:46:19	Micr...	4625	Logon
Hata...	3.05.2023 23:46:19	Micr...	4625	Logon
Hata...	3.05.2023 23:46:19	Micr...	4625	Logon
Hata...	3.05.2023 23:46:19	Micr...	4625	Logon
Hata...	3.05.2023 23:46:18	Micr...	4625	Logon
Hata...	3.05.2023 23:46:18	Micr...	4625	Logon

Figure 3.1

Event ID 4625

Event ID 4625 indicates a failed logon attempt. If someone is repeatedly trying to log in and providing incorrect username or password each time, we can see this with Event Viewer using 4625. We can see a detailed view of this in Figure 3.2.

EventData

SubjectUserSid	S-1-0-0
SubjectUserName	-
SubjectDomainName	-
SubjectLogonId	0x0
TargetUserSid	S-1-0-0
TargetUserName	hg62sa
TargetDomainName	
Status	0xc000006d
FailureReason	%%2313
SubStatus	0xc0000064
LogonType	3
LogonProcessName	NtLmSsp
AuthenticationPackageName	NTLM
WorkstationName	kali99
TransmittedServices	-
LmPackageName	-
KeyLength	0
ProcessId	0x0
ProcessName	-
IpAddress	192.168.
IpPort	0

Bir hesap oturum açamadı.

Konu:
Güvenlik Kimliği: NULL SID
Hesap Adı: -
Hesap Etki Alanı: -
Oturum Açma Kimliği: 0x0

Oturum Türü: 3

Oturumu Açılamayan Hesap:
Güvenlik Kimliği: NULL SID
Hesap Adı: hg62sa
Hesap Etki Alanı:

Hata Bilgileri:
Hata Nedeni: Bilinmeyen kullanıcı adı veya yanlış parola.
Durum: 0xC000006D
Alt Durum: 0xC0000064

İşlem Bilgileri:
Çağıran İşlem Kimliği: 0x0
Çağıran İşlem Adı: -

Ağ Bilgileri:

Günlük Adı:	Güvenlik		
Kaynak:	Microsoft Windows security audit	Günlüğe kaydedilen:	3.05.2023 23:46:20
Olay Kimliği:	4625	Görev Kategorisi:	Logon

Figure 3.2

Important information that can be obtained with **Event 4625** is as follows:

Logon Type: This section shows how the user attempted to log in. The most common Logon Types are 2 and 3, which are considered danger

signs. Looking at the output above, we can see that the Logon Type is 3, which is the Logon Type used for logging in over the network.

Another piece of information we can obtain is the “Account For Which Logon Failed.” As we can see in the output above, the username of the user who attempted to log in to our computer is visible in the **Workstation Name** section.

Finally, the information we can obtain is the **Failure Information**. In the above output, the error message we received, “0xC000006D,” means “incorrect username or password.”

Event ID 4624

Event ID 4624, represents a successful login to an account. When we perform an RDP Brute Force attack on a target Windows computer and correctly guess the username and password information to gain entry, event ID 4624 is generated. An example of an event 4624 is shown in Figure 4.1.

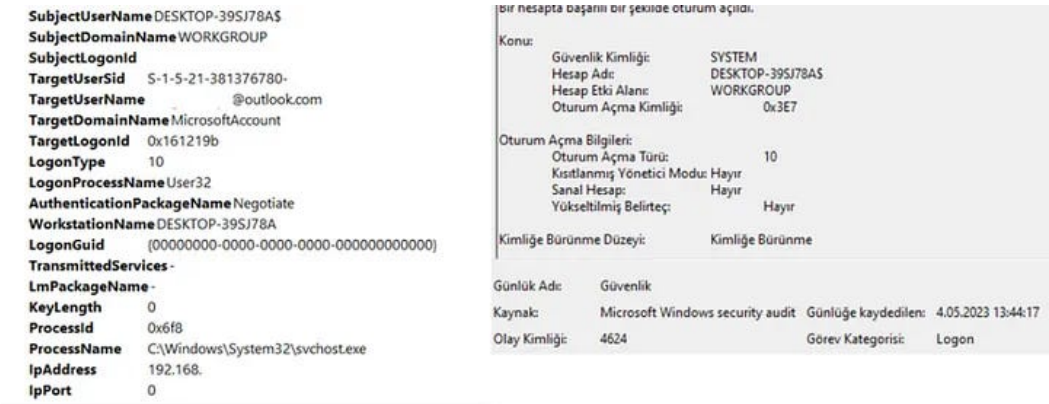


Figure 4.1

Important information that can be obtained from Event 4624 includes the Logon Type, which in the above output we see is 10. This indicates Remote Desktop connections, meaning there was an attempt at accessing via RDP. In some cases, we may see Logon Type 7, indicating a user reconnecting to an existing RDP session.

Event ID 1149

Event 1149 is logged when user authentication is successful. It can be examined through the file path “Windows\System32\wine\Logs\TerminalServices/RemoteConnectionManager/Oper
An example output of Event 1149 is shown in Figure 4.2

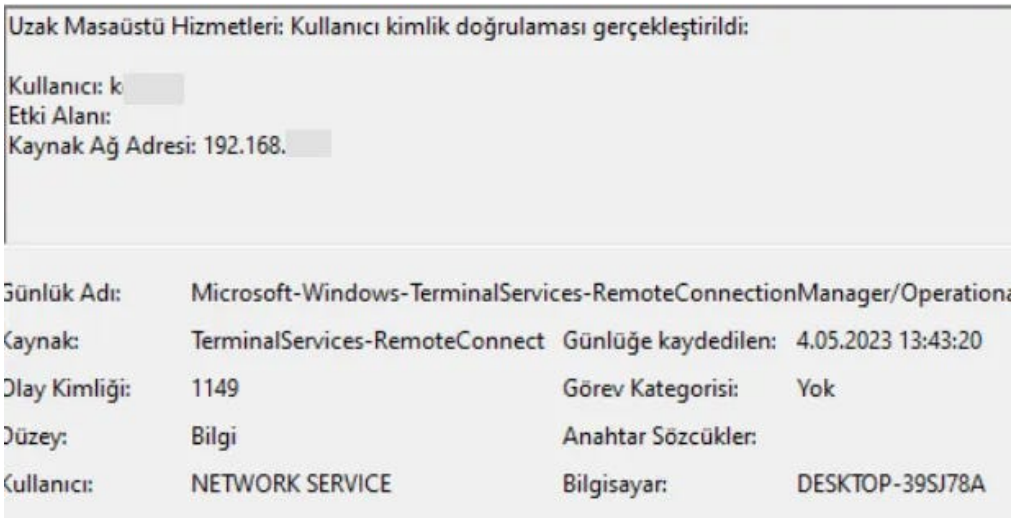


Figure 4.2

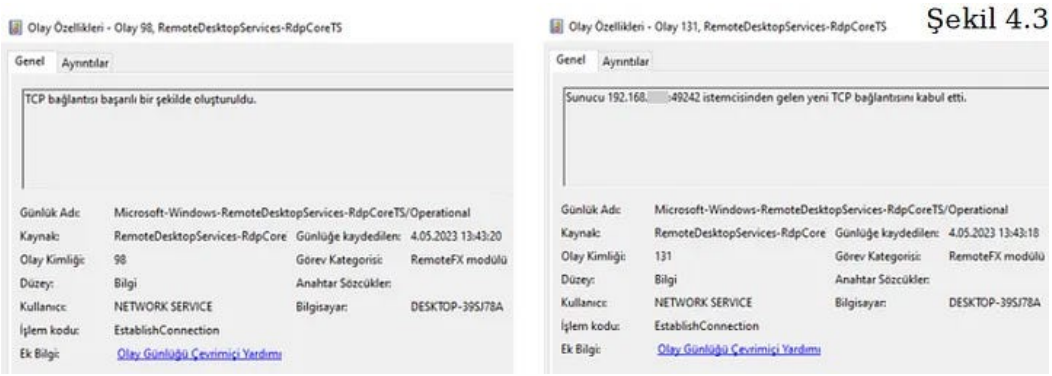
Event ID 98 | 131

Event ID 98 and 131 are records of the acceptance and establishment of a TCP connection for an RDP session.

They can be examined using the "Windows\System32\winevt\Logs\RemoteDesktopServices-RDPCoreTS\Operational" file path.

Event 131 indicates that the server has accepted a new TCP connection from the client.

Event 98 records the successful establishment of the TCP connection. Example outputs of Event 131 and Event 98 are shown in Figure 4.3.



Şekil 4.3

Figure 4.3

Event ID 21 | 22 | 25

Windows\System32\winevt\Logs\TerminalServices-LocalSessionManager" path can be used to examine these events.

Event ID 21 is recorded when a logon attempt is successful in Remote Desktop Services (Session Logon Succeeded). An example output for Event ID 21 is shown in Figure 4.4.

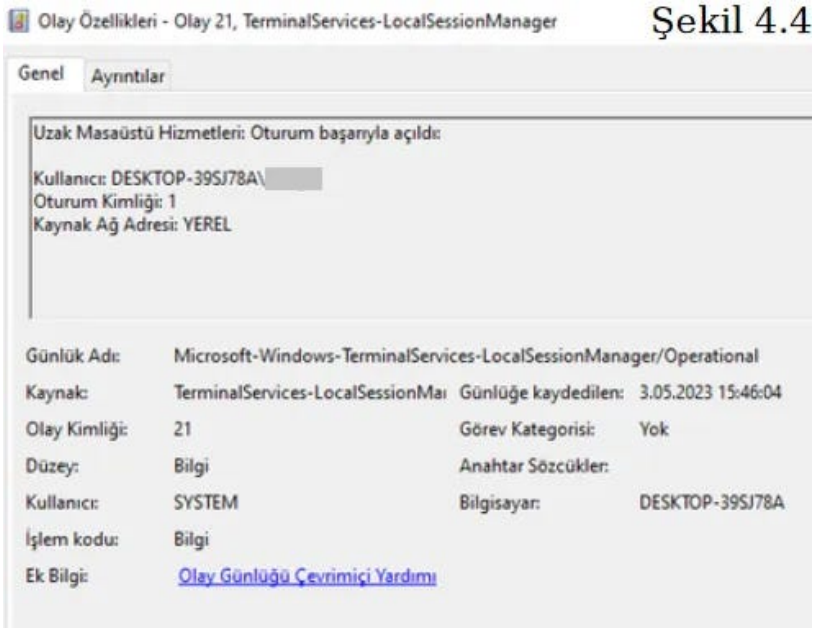


Figure 4.4

Event 22 reports the Shell start notification received status in Remote Desktop Services. It contains much of the same information as Event 21, but records the receipt of the Shell start notification for the interactive logon session, which is also known as the graphical user interface of the windows provided by RDP. An example of an Event 22 output is shown in Figure 4.5.

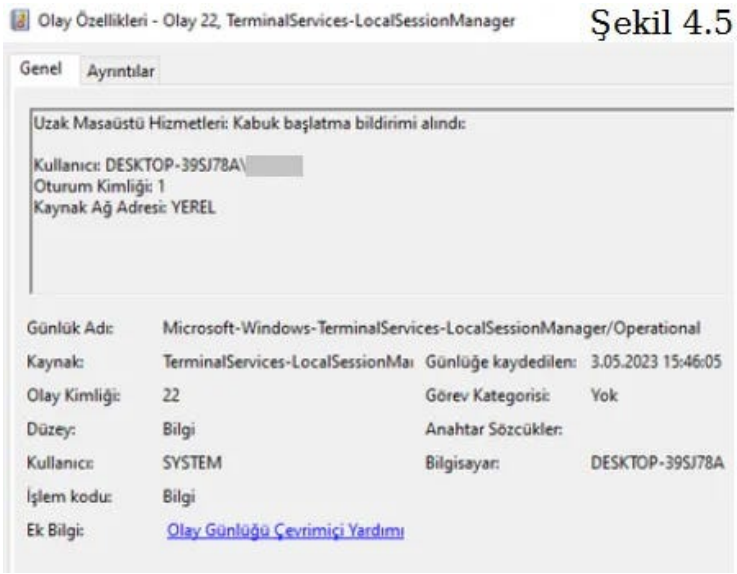


Figure 4.5

Event 25 records the successful reconnection of a session in Remote Desktop Services (RDS). It means that there was an existing session for the user and RDP reconnected to this session. It is shown in Figure 4.6.

Figure 4.6

By Doğukan Kaya on May 8, 2023.

Canonical link

Exported from Medium on June 1, 2023.