Challenge: T1110-003 Lab

Platform: CyberDefenders

Category: Threat Hunting

Difficulty: Easy

Tools Used: ELK

Summary: This lab involves investigating a password spraying attack targeting RDP. You can use either ELK or Splunk to investigate the logs, in my case, I chose ELK. This lab is useful for testing your ability to detect authentication related attacks, along with your understanding of RDP and the logs it produces. Whilst I found this lab a tad boring, it was still worthwhile.

Scenario: Adversaries may use a single or small list of commonly used passwords against many different accounts to attempt to acquire valid account credentials. Password spraying uses one password (e.g. 'Password01'), or a small list of commonly used passwords, that may match the complexity policy of the domain. Logins are attempted with that password against many different accounts on a network to avoid account lockouts that would normally occur when brute forcing a single account with many passwords. [1]

Typically, management services over commonly used ports are used when password spraying. Commonly targeted services include the following:

- SSH (22/TCP)
- Telnet (23/TCP)
- FTP (21/TCP)
- NetBIOS / SMB / Samba (139/TCP & 445/TCP)
- LDAP (389/TCP)
- Kerberos (88/TCP)
- RDP / Terminal Services (3389/TCP)
- HTTP/HTTP Management Services (80/TCP & 443/TCP)
- MSSQL (1433/TCP)
- Oracle (1521/TCP)
- MySQL (3306/TCP)
- VNC (5900/TCP)

In addition to management services, adversaries may "target single sign-on (SSO) and cloud-based applications utilizing federated authentication protocols," as well as externally facing email applications, such as Office 365.[2]

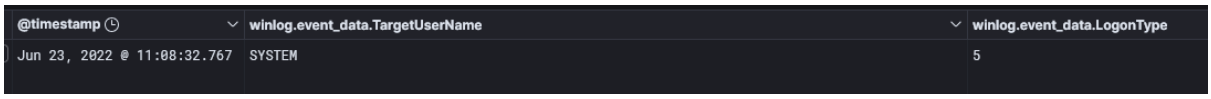
In default environments, LDAP and Kerberos connection attempts are less likely to trigger events over SMB, which creates Windows "logon failure" event ID 4625.

Who was the last logged-in user?

Each time a user successfully authenticates on a Windows host, it generates event ID 4624:

- `event.code : 4624`

In my case, the first logged-in user is SYSTEM for the service logon type:



@timestamp	winlog.event_data.TargetUserName	winlog.event_data.LogonType
Jun 23, 2022 @ 11:08:32.767	SYSTEM	5

If we filter for interactive logon:

- `event.code : 4624 AND winlog.event_data.LogonType : 2`

We can see that one of the last logged-in users is the Administrator account:

May 18, 2022 @ 18:08:42.367	Administrator	2

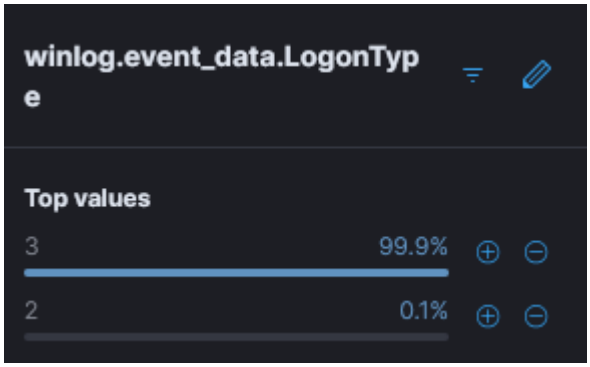
Answer: Administrator

What is the logon type of the failed logons?

Failed authentication attempts are logged with event ID 4625:

- `event.code : 4625`

If you view the winlog.event_data.LogonType field, we can see that logon type 3 makes up 99.9% of the failed authentication types:



Logon type 3 refers to a network logon, which occurs when a user or computer accesses another computer from the network to access a shared resources like a folder or printer. It can also be generated for RDP if NLA is enabled.

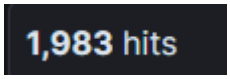
Answer: 3

What is the protocol the attacker tried to bruteforce?

Due to the large number of failed authentication attempts with logon type 3, this could indicate RDP brute-forcing given that if NLA is enabled, a failed RDP login will often be logged as a type 3 failure, because the pre-authentication occurs over the network. When a network connection is made to the RDP service, it generates event ID 261 in the Remote Connection Manager logs:

- `event.code : 261`

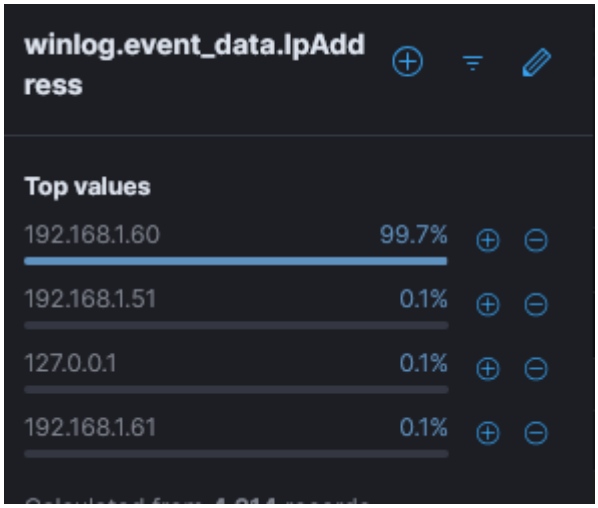
Here we can find many connections made to the RDP service:



Answer: RDP

How many users did the attacker succeed in getting their accounts?

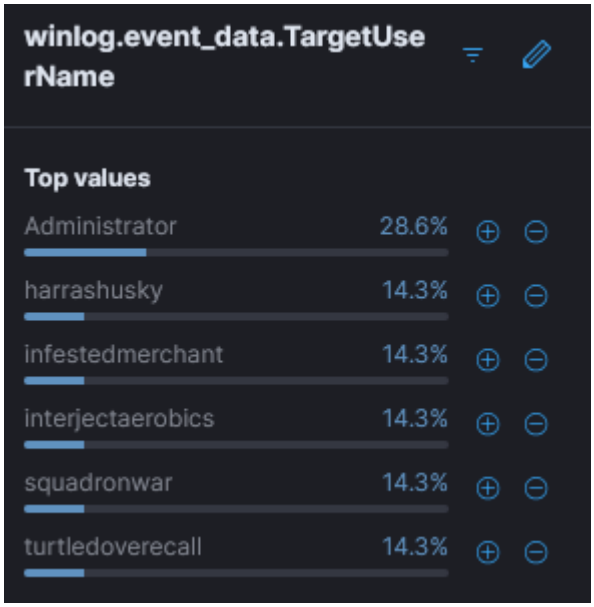
When you look at the failed authentication attempts, they were mostly coming from 192.168.1.60:



As we established previously, RDP logon events can be logged with logon type 3. Using the following query:

- `event.code : 4624 AND winlog.event_data.IpAddress : 192.168.1.60 AND winlog.event_data.LogonType : 3`

We can hunt for all successful type 3 events from the host associated with the password spraying activity. Here we can see 7 successful authentications for 6 unique users:



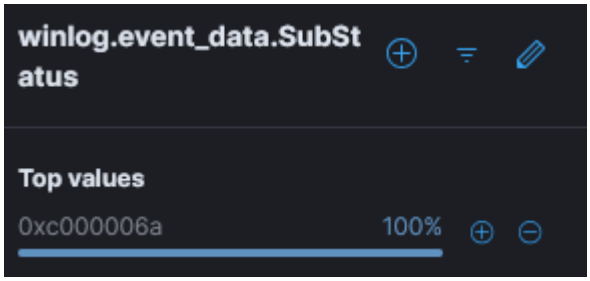
Answer: 6

According to Microsoft. What is the description of the "Sub Status" code for event id 4625?

Using the following query:

- `event.code : 4625 AND winlog.event_data.IpAddress : 192.168.1.60 AND winlog.event_data.LogonType : 3`

We can identify failed authentication attempts from the threat actor. If you view the winlog.event_data.SubStatus field, we can see that they are all 0xc000006a:



Using the Microsoft documentation on event ID 4625, we can see that this sub status maps to “User logon with misspelled or bad password”:

Failure Information\Status or **Failure Information\Sub Status**	0xC000006A – "User logon with misspelled or bad password" for critical accounts or service accounts. Especially watch for a number of such events in a row.

Answer: User logon with misspelled or bad password

How long did the bruteforce last? MM:SS

Using the query from the previous question, we can see the first failed authentication attempt occurred at 16:29:09.460, with the last being at 16:34:57.623. Therefore, the attack lasted 5 minutes, and 48 seconds.

Answer: 05:48

How many minutes passed before the attacker logged into the machine again?

The last failed authentication occurred at 16:34:57.623. Using the following query:

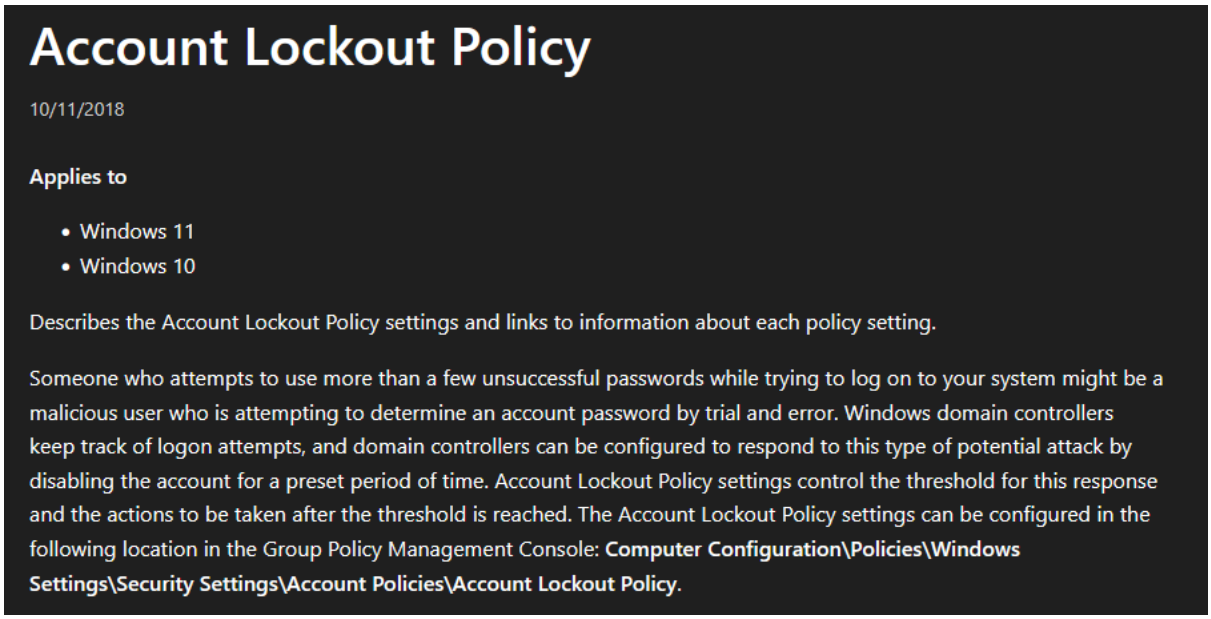
- `event.code : 4624 AND winlog.event_data.IpAddress : 192.168.1.60 AND winlog.event_data.LogonType : 3`

We can see that the first failed authentication attempt occurred at 16:46:09.987.

Answer: 11

What is the name of the policy used to lock the account after a certain number of failed login attempts?

The policy used to lock the account after a certain number of failed login attempts is called the Account Lockout policy:



Answer: Account Lockout