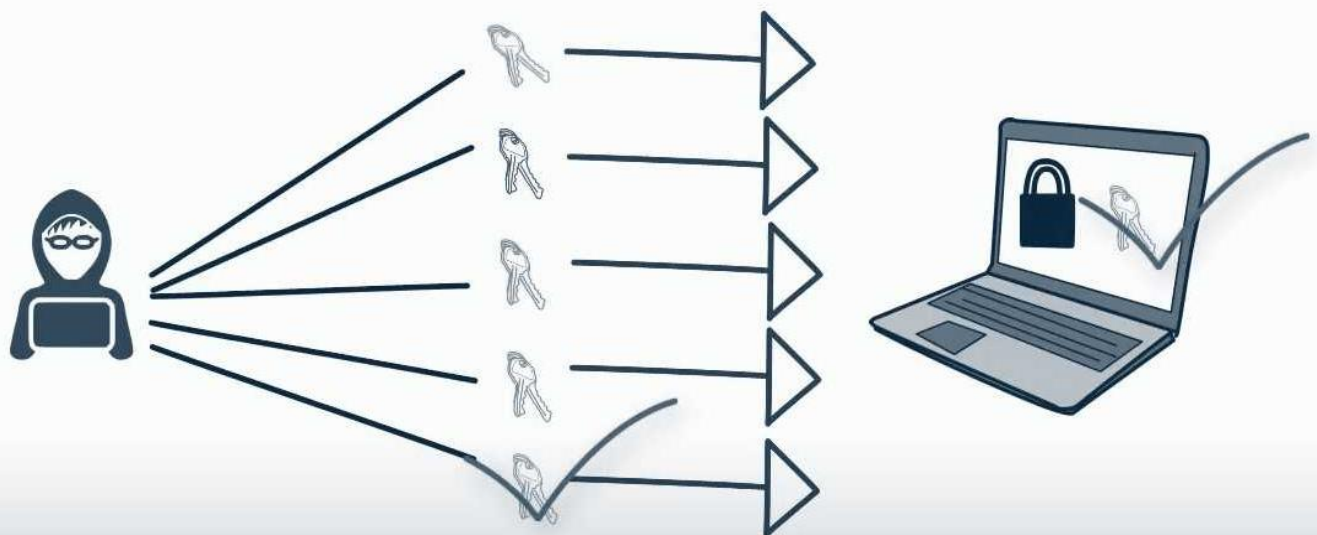










Detecting Brute Force Attacks



Nelson Ojovbo

<https://www.linkedin.com/in/nelson-ojovbo/>

Table of Contents

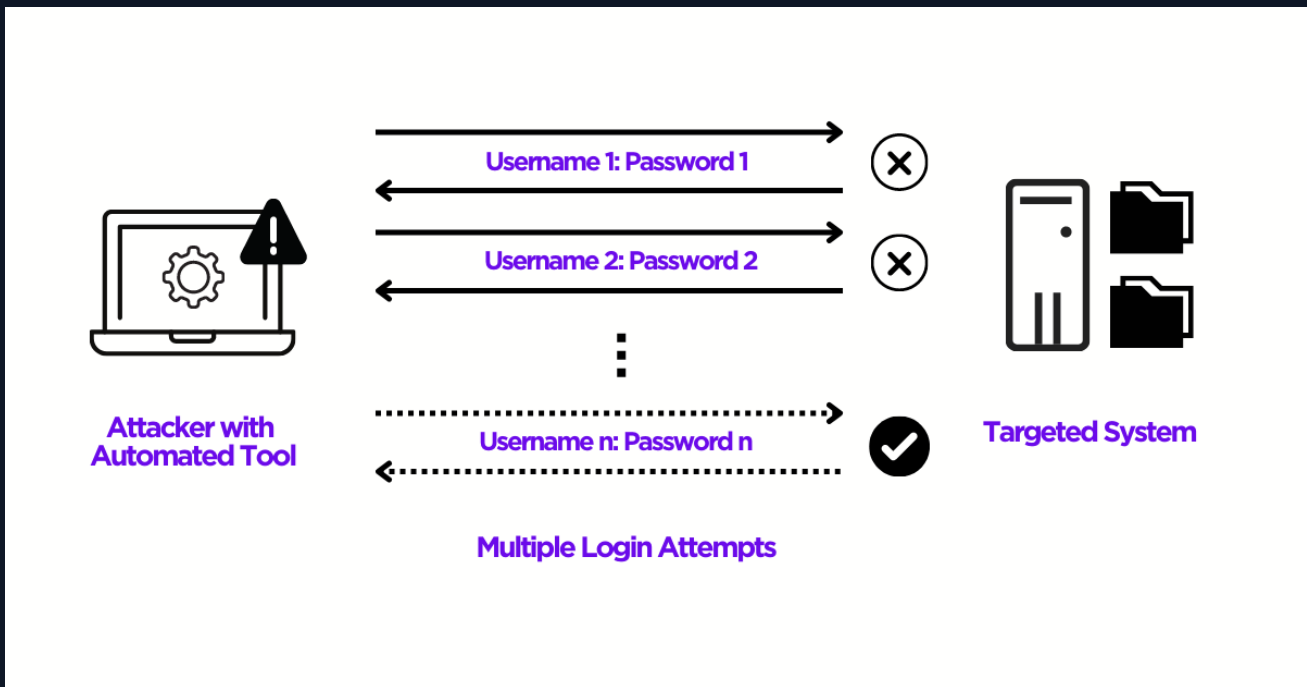
-  [Introduction to Detecting Brute Force Attacks](#)
-  [Brute Force Attacks](#)
-  [Protocol/Services That Can Be Attacked by Brute Force](#)
-  [Tools Used in a Brute Force Attacks](#)
-  [How to Avoid Brute Force Attacks?](#)
-  [SSH Brute Force Attack Detection Example](#)
-  [HTTP Login Brute Force Attack Detection Example](#)
-  [Windows Login Brute Force Detection Example](#)

Brute Force Attacks

is a trial-and-error technique attackers use to discover valid user credentials by guessing every possible combination of characters until they find the correct combination.

How Brute Force Attacks Work

Attackers have a handful of readily and freely available tools (such as Metasploit, John the Ripper, Hydra, etc.).



6 indicators of a brute force attack

1

Unusual pattern of failed login attempts

2

Failed login attempts from the same IP address into many accounts

3

Logging into an account from an unusual IP address

4

Successfully logging into an account followed by numerous failed login attempts

5

Unusual user behavior after a successful login

6

Increased internet use after a successful login

Example of Brute Force Attack Using Hydra Tool

```
root@kali:~# hydra -L /root/Desktop/user.txt -P /root/Desktop/pass.txt 192.168.1.128 mssql
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service org
Hydra (http://www.thc.org/thc-hydra) starting at 2018-03-15 04:01:36
[DATA] max 16 tasks per 1 server, overall 16 tasks, 16 login tries (l:4/p:4), ~1 try per ta
[DATA] attacking mssql://192.168.1.128:1433/
[ERROR] Child with pid 1536 terminating, can not connect
[ERROR] Child with pid 1535 terminating, can not connect
[ERROR] Child with pid 1524 terminating, can not connect
[ERROR] Child with pid 1525 terminating, can not connect
[ERROR] Child with pid 1530 terminating, can not connect
[ERROR] Child with pid 1527 terminating, can not connect
[ERROR] Child with pid 1522 terminating, can not connect
[ERROR] Child with pid 1534 terminating, can not connect
[ERROR] Child with pid 1529 terminating, can not connect
[ERROR] Child with pid 1523 terminating, can not connect
[ERROR] Child with pid 1526 terminating, can not connect
[ERROR] Child with pid 1528 terminating, can not connect
[ERROR] Child with pid 1531 terminating, can not connect
[ERROR] Child with pid 1532 terminating, can not connect
[ERROR] Child with pid 1533 terminating, can not connect
[ERROR] Child with pid 1537 terminating, can not connect
[1433][mssql] host: 192.168.1.128 login: sa password: apple@123456
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2018-03-15 04:01:43
```

NOTE:

- ❖ The duration of the attack will vary according to the length of the sensitive data sought. If attempts are being made for a simple password or a username, this may take a short time or it may take years for complex expressions.

We can basically explain brute-force attacks into two categories.

1.1. Online Brute force attacks

In online brute force attacks, the attacker and the victim are online at the same time and contact each other depending on the situation. It is also possible to categorize these attacks as Active and Passive.

A. Passive Online Brute Force Attacks

The attacker and the victim are on the same network, but do not have direct contact with each other. Usually, the attacker tries to obtain the password in passive ways without establishing a one-to-one connection with the victim machine. We can give the following examples of this type of attack.

Man in the Middle: In this attack style, traffic related to the environment and the target machine is listened to and the password etc. is attempted to be captured.

Sniffing: Sniffing style attacks are effective if there is a connection on the same network and a network tool such as a hub is used in the system because the hub sends a package to all the ports the whole LAN can see this package. If tools such as switches are used, then these tools will filter what is to be sent to the target system, and sniffing is not effective here.

B. Active Online Brute Force Attacks

In active online brute force attacks, the attacker communicates directly with the victim machine and makes the necessary trials to the relevant service on the victim machine. For example, user/password attempts made to a web server, email server, SSH service, RDP service or a database service can be given as an example for this title.

This is a very advantageous method for simple passwords, but it usually doesn't work for strong passwords in the short term. It may cause situations such as account lockout and disabling the target system.

1.2. Offline Brute force attacks

Offline brute-force attacks are used for previously captured encrypted or hashed data. In this type of attack, the attacker does not need to establish an active connection directly with the victim machine. Attacker can perform an offline attack on the password file that he/she somehow gained access to. The password information to be attacked can be obtained in different ways. For example;

- By capturing packets on wireless network
- Capturing a package with a mitm attack
- Dumping hashes from db with a SQLi weakness
- SAM or NTDS.dit database on windows systems

Usually, these attacks are carried out in 3 different ways.

1.2.1. Dictionary Attacks

This is a problem caused by the use of a common password. This is an attack method that usually occurs as a result of more than one person using the same password accidentally. First, the attacker creates a dictionary for himself/herself from the passwords he/she will try. He/she can find a prepared dictionary on the internet or create it as he/she wishes. Then, each word in this dictionary is tested on the target system as a password.

1.2.2. Brute Force Attacks

Brute force attacks are a method performed by trying all possibilities in a certain range one by one. For example, if the password we are looking for consists of up to 5 characters, the attacker tries all the possibilities one by one, including uppercase and lowercase letters, digits and special characters. If an attack is made to find a complex password, the attack time may be quite long depending on the condition of the hardware used.

1.2.3. Rainbow Table Attacks

We should keep in mind that all password possibilities in a certain range are calculated with the relevant function in a rainbow attack. In this attack type, the attacker quickly compares the pre-calculated hash file with the password summary he/she wants to crack and obtains the password if there is a match.

The biggest problem here is to calculate these hashes or to somehow get access to the calculated form.

Protocol/Services That Can Be Attacked by Brute Force

Brute force attacks are mostly encountered in the following areas in institutions.

- **Web application login pages**
- **RDP services**
- **SSH services**
- **Mail server login pages**
- **LDAP services**
- **Database services (MySQL, MySQL, PostgreSQL, oracle, etc.)**
- **Web application home directories (directory brute force)**
- **DNS servers, in order to detect DNS records (dns brute force)**

Tools Used in a Brute Force Attacks

Aircrack-ng: aircrack-ng is an 802.11a/b/g WEP/WPA cracking program that can recover a 40-bit, 104-bit, 256-bit or 512-bit WEP key once enough encrypted packets have been gathered. Also it can attack WPA1/2 networks with some advanced methods or simply by brute force.

John the Ripper: John the Ripper is a tool designed to help systems administrators to find weak (easy to guess or crack through brute force) passwords, and even automatically mail users alert them about it, if it is desired. Runs on 15 different platforms including Unix, Windows, and OpenVMS.

L0phtCrack: a tool for cracking Windows passwords. It uses rainbow tables, dictionaries, and multiprocessor algorithms.

Hashcat: Hashcat supports five unique modes of attack for over 300 highly-optimized hashing algorithms. hashcat currently supports CPUs, GPUs, and other hardware accelerators on Linux, and has facilities to help distribute password cracking.

Ncrack: a tool for cracking network authentication. It can be used on Windows, Linux, and BSD. It was built to help companies secure their networks by proactively testing all their hosts and networking devices for poor passwords.

Hydra: Hydra is a parallelized login cracker which supports numerous protocols to attack. It is very fast and flexible, and new modules are easy to add.

Reference: kali.org/tools/

How to Avoid Brute Force Attacks?

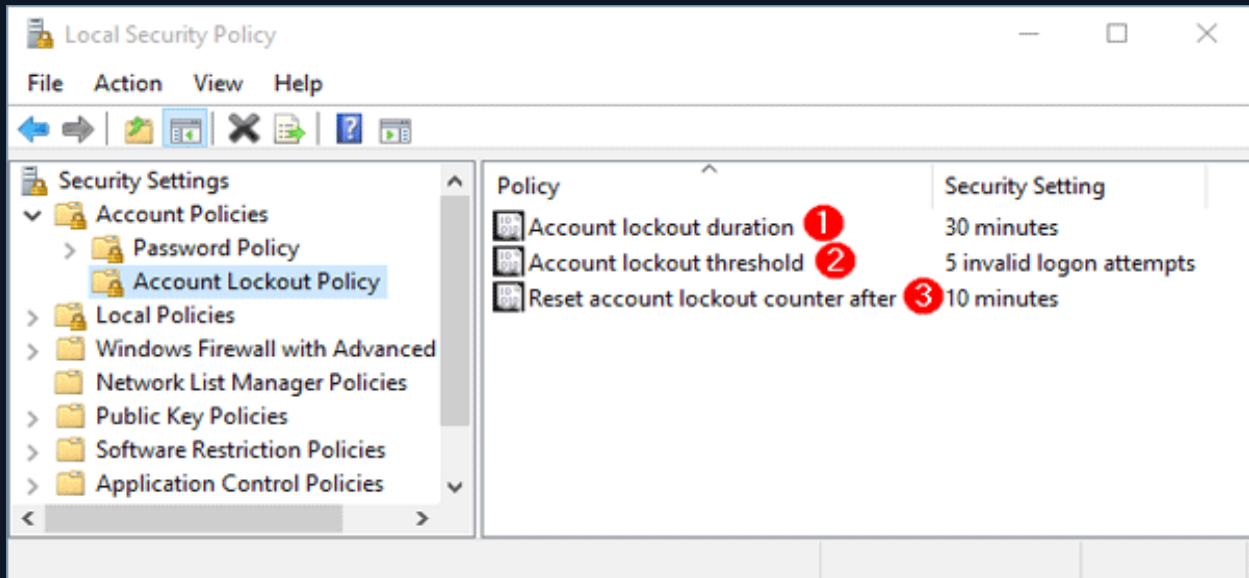
To protect your organization from brute force attack, enforce the use of strong passwords.

You can find some best practices for passwords below:

- **Never use information that can be found online (like names of family members).**
- **Have as many characters as possible.**
- **Combine letters, numbers, and symbols.**
- **Minimum 8 characters.**
- **Each user account is different.**
- **Avoid common patterns.**

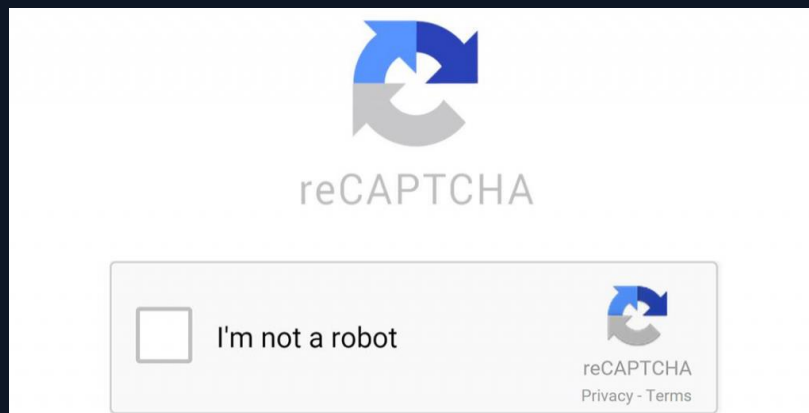
Here are some ways you can protect users from brute-force attacks as administrators of an organization:

Lock Policy - After a certain number of failed login attempts, you can lock accounts and then unlock them as an administrator



Progressive delays - You can lock accounts for a limited time after a certain number of failed login attempts.

Recaptcha - With tools such as Captcha-reCAPTCHA, you can make it mandatory for users to complete simple tasks in order to log on to a system.



Strong Password Policy - You can force users to define long and complex passwords and force them to change their password periodically.

2FA - It is the method where a second verification is required from the user with an additional verification mechanism (SMS, mail, token, push notification, etc.) after entering the username and password.



4.1. Brute Force Attack Detection

Specific rules are usually defined on SIEM systems to detect brute force attacks. When defining these rules, we consider how many unsuccessful login attempts are made by the user within a certain period of time. While analyzing the relevant alarms, the logs of the trial protocol/application are examined and the necessary inferences are made. Examples of some brute force attacks are given below.

SSH Brute Force Attack Detection Example

Simple passwords used on the server with an SSH brute force attack can be easily found by the attackers. If such attacks fail, the attacker will only attempt a certain number of failed passwords. If successful, the password is entered successfully after a certain number of unsuccessful login attempts. **In an example SSH brute force analysis, when we view a linux machine log with the contents of the “/var/log/auth.log.1” file and failed login attempts, we can see who the failed login attempts belong to.**

```
cat auth.log.1 | grep "Failed password" | cut -d " " -f10 | sort | uniq -c | sort
```

```
root@ip-172-31-18-193:/var/log# cat auth.log.1 | grep "Failed password" | cut -d " " -f10 | sort | uniq -c | sort
  1 times:
  2 from
 13 invalid
 13 root
 14 analyst
 614 letsdefend
root@ip-172-31-18-193:/var/log#
```

A command below can be used to locate the IP addresses that made these attempts.

```
cat auth.log.1 | grep "Failed password" | cut -d " " -f12 | sort | uniq -c | sort
```

```
root@ip-172-31-18-193:/var/log# cat auth.log.1 | grep "Failed password" | cut -d " " -f12 | sort | uniq -c | sort
  1 Failed
  2 port
 13 admin
 30 188.58.65.203
 96 173.249.51.74
232 46.31.148.75
283 176.40.39.151
root@ip-172-31-18-193:/var/log#
```

Users who successfully log in can also be detected with the following command.

```
cat auth.log.1 | grep "Accepted password"
```

```
root@ip-172-31-18-193:/var/log# cat auth.log.1 | grep "Accepted password"
Jul 14 08:48:35 ip-172-31-1-195 sshd[1166]: Accepted password for analyst from 172.31.1.195 port 52516 ssh2
Sep  4 19:15:49 ip-172-31-12-170 sshd[1899]: Accepted password for analyst from 172.31.12.170 port 39284 ssh2
Sep  4 19:17:13 ip-172-31-12-170 sshd[2055]: Accepted password for analyst from 172.31.12.170 port 39288 ssh2
Sep  4 19:18:43 ip-172-31-12-170 sshd[2191]: Accepted password for analyst from 172.31.12.170 port 39298 ssh2
Sep  4 19:18:48 ip-172-31-12-170 sshd[2302]: Accepted password for analyst from 172.31.12.170 port 39300 ssh2
Sep  4 19:22:14 ip-172-31-12-170 sshd[2419]: Accepted password for analyst from 172.31.12.170 port 39302 ssh2
Sep  4 19:34:45 ip-172-31-12-170 sshd[2633]: Accepted password for analyst from 172.31.12.170 port 39312 ssh2
Sep  4 19:39:43 ip-172-31-12-170 sshd[2908]: Accepted password for analyst from 172.31.12.170 port 39326 ssh2
Sep  4 19:39:46 ip-172-31-12-170 sshd[3012]: Accepted password for analyst from 172.31.12.170 port 39328 ssh2
Sep  4 20:11:04 ip-172-31-12-170 sshd[3425]: Accepted password for letsdefend from 188.58.65.203 port 52313 ssh2
Sep  4 20:11:57 ip-172-31-12-170 sshd[3550]: Accepted password for letsdefend from 188.58.65.203 port 51855 ssh2
root@ip-172-31-18-193:/var/log#
```

NOTE

- ❖ As can be seen here, successful login attempts are seen with two different users from two different IP addresses.
- ❖ When the previous failed login attempts are compared, it is seen that the "analyst" user did not have an unsuccessful login attempt before from the ip address he successfully logged in.
- ❖ However, it is clearly seen that many unsuccessful attempts were made with the "letsdefend" user at the IP address of 188.58.65.203. This shows us that the attacker successfully logged in with the letsdefend user during the brute force.

```

Sep  4 20:11:03 ip-172-31-12-170 sshd[3420]: Failed password for letsdefend from 188.58.65.203 port 51653 ssh2
Sep  4 20:11:03 ip-172-31-12-170 sshd[3425]: Failed password for letsdefend from 188.58.65.203 port 52313 ssh2
Sep  4 20:11:03 ip-172-31-12-170 sshd[3426]: Failed password for letsdefend from 188.58.65.203 port 51977 ssh2
Sep  4 20:11:03 ip-172-31-12-170 sshd[3423]: Failed password for letsdefend from 188.58.65.203 port 51927 ssh2
Sep  4 20:11:03 ip-172-31-12-170 sshd[3418]: Failed password for letsdefend from 188.58.65.203 port 51960 ssh2
Sep  4 20:11:03 ip-172-31-12-170 sshd[3428]: Failed password for letsdefend from 188.58.65.203 port 52092 ssh2
Sep  4 20:11:03 ip-172-31-12-170 sshd[3424]: Failed password for letsdefend from 188.58.65.203 port 51645 ssh2
Sep  4 20:11:03 ip-172-31-12-170 sshd[3427]: Failed password for letsdefend from 188.58.65.203 port 52204 ssh2
Sep  4 20:11:03 ip-172-31-12-170 sshd[3431]: Failed password for letsdefend from 188.58.65.203 port 52642 ssh2
Sep  4 20:11:03 ip-172-31-12-170 sshd[3422]: Failed password for letsdefend from 188.58.65.203 port 52560 ssh2
Sep  4 20:11:03 ip-172-31-12-170 sshd[3430]: Failed password for letsdefend from 188.58.65.203 port 52373 ssh2
Sep  4 20:11:03 ip-172-31-12-170 sshd[3429]: Failed password for letsdefend from 188.58.65.203 port 52523 ssh2
Sep  4 20:11:03 ip-172-31-12-170 sshd[3417]: Failed password for letsdefend from 188.58.65.203 port 51994 ssh2
Sep  4 20:11:04 ip-172-31-12-170 sshd[3446]: Failed password for letsdefend from 188.58.65.203 port 52598 ssh2
Sep  4 20:11:04 ip-172-31-12-170 sshd[3425]: Accepted password for letsdefend from 188.58.65.203 port 52313 ssh2
Sep  4 20:11:04 ip-172-31-12-170 sshd[3425]: pam_unix(sshd:session): session opened for user letsdefend by (uid=0)
Sep  4 20:11:04 ip-172-31-12-170 systemd-logind[464]: New session 14 of user letsdefend.

```

NOTE

As seen above, successful and unsuccessful logged in users can be easily found with basic Linux commands. When these two results are examined in detail, it is seen that there is a successful entry after many unsuccessful attempts by the `letsdefend` user from the `188.58.65.203` IP address.

HTTP Login Brute Force Attack Detection Example

In HTTP login brute force attacks, the attacker usually tries a password with a dictionary attack on a login page. In order to analyze this, the content of the relevant log file should be opened with a text editor and the logs should be examined.

The following screenshot shows an HTTP login brute force attack. It is seen that the user found the password by successfully entering the password after a certain number of unsuccessful login attempts.

```

173.249.51.74 - - [24/Sep/2021:14:04:52 +0000] "POST /bwAPP/login.php HTTP/1.1" 200 4092 "http://3.128.26.67:8090/bwAPP/login.php" "Mozilla/5.0
173.249.51.74 - - [24/Sep/2021:14:04:54 +0000] "POST /bwAPP/login.php HTTP/1.1" 200 4092 "http://3.128.26.67:8090/bwAPP/login.php" "Mozilla/5.0
173.249.51.74 - - [24/Sep/2021:14:04:56 +0000] "POST /bwAPP/login.php HTTP/1.1" 200 4092 "http://3.128.26.67:8090/bwAPP/login.php" "Mozilla/5.0
173.249.51.74 - - [24/Sep/2021:14:04:59 +0000] "POST /bwAPP/login.php HTTP/1.1" 200 4092 "http://3.128.26.67:8090/bwAPP/login.php" "Mozilla/5.0
173.249.51.74 - - [24/Sep/2021:14:05:02 +0000] "POST /bwAPP/login.php HTTP/1.1" 200 4092 "http://3.128.26.67:8090/bwAPP/login.php" "Mozilla/5.0
173.249.51.74 - - [24/Sep/2021:14:05:04 +0000] "POST /bwAPP/login.php HTTP/1.1" 200 4092 "http://3.128.26.67:8090/bwAPP/login.php" "Mozilla/5.0
173.249.51.74 - - [24/Sep/2021:14:05:07 +0000] "POST /bwAPP/login.php HTTP/1.1" 200 4092 "http://3.128.26.67:8090/bwAPP/login.php" "Mozilla/5.0
173.249.51.74 - - [24/Sep/2021:14:05:10 +0000] "POST /bwAPP/login.php HTTP/1.1" 200 4092 "http://3.128.26.67:8090/bwAPP/login.php" "Mozilla/5.0
173.249.51.74 - - [24/Sep/2021:14:05:13 +0000] "POST /bwAPP/login.php HTTP/1.1" 200 4092 "http://3.128.26.67:8090/bwAPP/login.php" "Mozilla/5.0
173.249.51.74 - - [24/Sep/2021:14:05:16 +0000] "POST /bwAPP/login.php HTTP/1.1" 200 4092 "http://3.128.26.67:8090/bwAPP/login.php" "Mozilla/5.0
173.249.51.74 - - [24/Sep/2021:14:05:19 +0000] "POST /bwAPP/login.php HTTP/1.1" 200 4092 "http://3.128.26.67:8090/bwAPP/login.php" "Mozilla/5.0
173.249.51.74 - - [24/Sep/2021:14:05:22 +0000] "POST /bwAPP/login.php HTTP/1.1" 200 4092 "http://3.128.26.67:8090/bwAPP/login.php" "Mozilla/5.0
173.249.51.74 - - [24/Sep/2021:14:05:25 +0000] "POST /bwAPP/login.php HTTP/1.1" 200 4092 "http://3.128.26.67:8090/bwAPP/login.php" "Mozilla/5.0
173.249.51.74 - - [24/Sep/2021:14:05:28 +0000] "POST /bwAPP/login.php HTTP/1.1" 200 4092 "http://3.128.26.67:8090/bwAPP/login.php" "Mozilla/5.0
173.249.51.74 - - [24/Sep/2021:14:05:31 +0000] "POST /bwAPP/login.php HTTP/1.1" 302 6 "http://3.128.26.67:8090/bwAPP/login.php" "Mozilla/5.0 (M
173.249.51.74 - - [24/Sep/2021:14:05:35 +0000] "POST /bwAPP/login.php HTTP/1.1" 200 4092 "http://3.128.26.67:8090/bwAPP/login.php" "Mozilla/5.0
173.249.51.74 - - [24/Sep/2021:14:05:38 +0000] "POST /bwAPP/login.php HTTP/1.1" 200 4092 "http://3.128.26.67:8090/bwAPP/login.php" "Mozilla/5.0
173.249.51.74 - - [24/Sep/2021:14:05:41 +0000] "POST /bwAPP/login.php HTTP/1.1" 200 4092 "http://3.128.26.67:8090/bwAPP/login.php" "Mozilla/5.0
173.249.51.74 - - [24/Sep/2021:14:05:51 +0000] "POST /bwAPP/login.php HTTP/1.1" 302 6 "http://3.128.26.67:8090/bwAPP/login.php" "Mozilla/5.0 (M

```

Windows Login Brute Force Detection Example 7.1 Windows Login Records

Considering the general situation, a login activity appears in all successful or unsuccessful cyberattacks. An attacker often wants to log into the server to take over the system. For this purpose, it can perform brute force attack or directly login with the password in hand. In both cases (successful login / unsuccessful login attempt) the log will be created.

Let's consider an attacker logged into the server after a brute force attack. To better analyze what the attacker did after entering the system, we need to find the login date. For this, we need "Event ID 4624 – An account was successfully logged on".

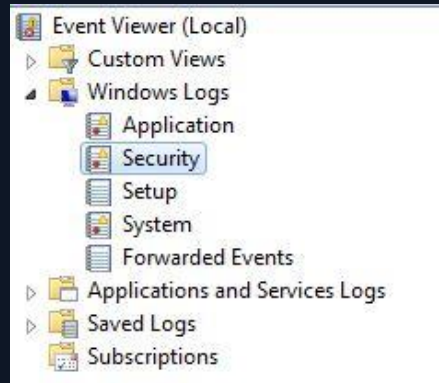
Each event log has its own ID value. Filtering, analyzing and searching the log title is more difficult, so it is easy to use the ID value.

You can find the details of which Event ID value means what from the URL address below.
<https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/default.aspx>

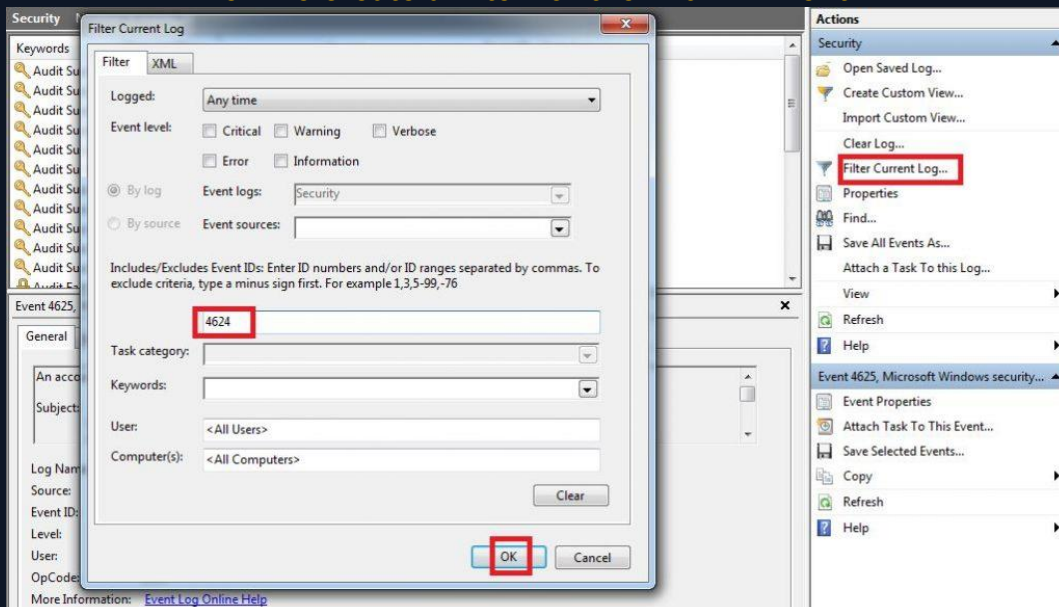
❖ Log file for lesson: [Log_File.zip](#) Pass=321

(https://app.letsdefend.io/download/downloadfile/Log_File.zip)

To reach the result, we open the "Event Viewer" and select "Security" logs.



Then we create a filter for the "4624" Event ID



And now we see that the number of logs has decreased significantly and we are only listing logs for successful login activities.

Looking at the log details, we see that the user of “LetsDefendTest” first logged in at 23/02/2021 10:17 PM.

The screenshot shows the Windows Security Event Viewer interface. At the top, it says "Security Number of events: 24". Below that, a filter is applied: "Filtered: Log: Security; Source: ; Event ID: 4624. Number of events: 3". A table lists three "Audit Success" events from "Microsoft Windows security auditing" on 2/23/2021 at 10:17:31 PM and 10:17:20 PM, all with Event ID 4624 and Task Category "Logon". The third event is highlighted with a red box. Below the table, the "Event 4624, Microsoft Windows security auditing" details are shown. The "Details" tab is active, showing the "Subject" section with fields: Security ID: SYSTEM, Account Name: WIN-CGAK3CTL9KRS, Account Domain: WORKGROUP, Logon ID: 0x3e7. The "Logon Type" is 10. The "New Logon" section shows: Security ID: WIN-CGAK3CTL9KR\LetsDefendTest, Account Name: LetsDefendTest (highlighted with a red box), Account Domain: WIN-CGAK3CTL9KR, Logon ID: 0x1b3e0ce. At the bottom, a summary of event details is provided: Log Name: Security, Source: Microsoft Windows security, Logged: 2/23/2021 10:17:20 PM, Event ID: 4624, Task Category: Logon, Level: Information, Keywords: Audit Success, User: N/A, Computer: WIN-CGAK3CTL9KR, OpCode: Info, and More Information: [Event Log Online Help](#).

When we look at the “Logon Type” field, we see the value 10. This indicates that you are logged in with “Remote Desktop Services” or “Remote Desktop Protocol”.

You can find the meaning of the logon type values on Microsoft’s page.

<https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4624>

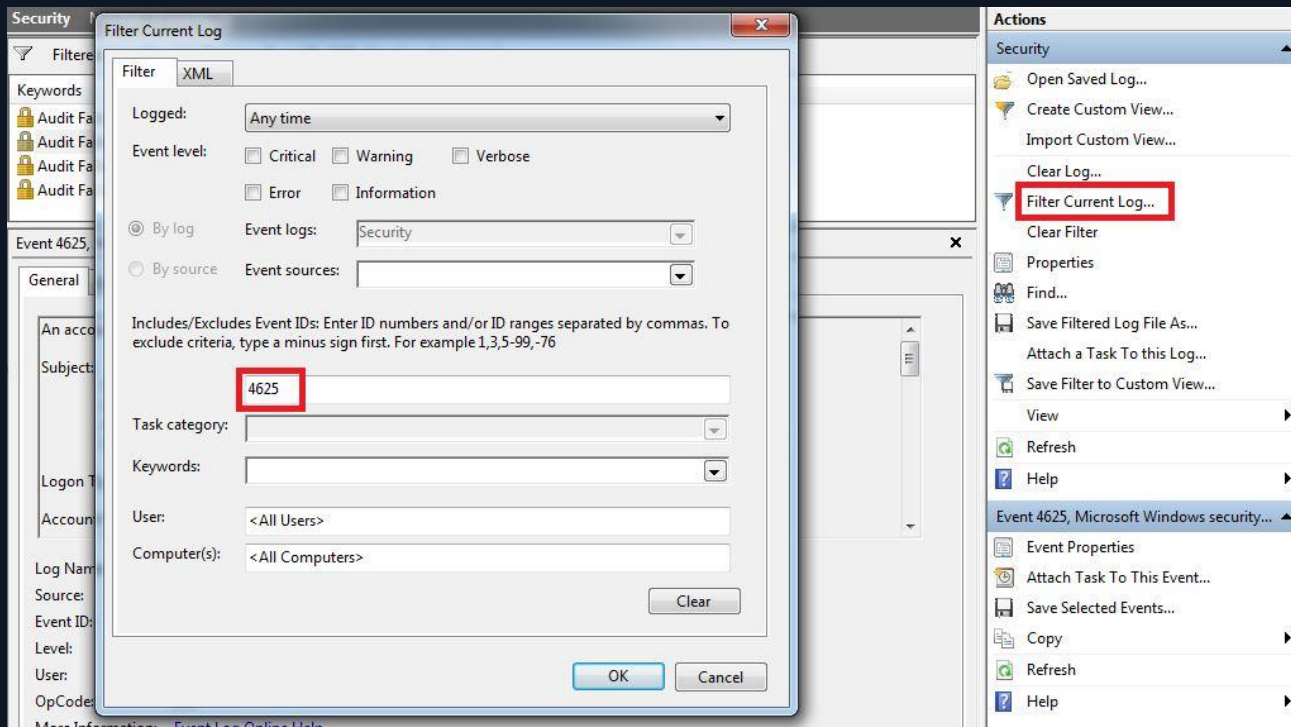
In the next section, we will detect the Brute force attack the attacker made before logging in.

7.2 windows RDP Brute Force Detection

In this section, we will catch an attacker who is in the lateral movement phase. The attacker is trying to jump to the other machine by brute force over RDP.

- ❖ Download log file: Log_File.zip Pass=321
[Log_File.zip Pass=321 \(https://app.letsdefend.io/download/downloadfile/Log_File.zip\)](https://app.letsdefend.io/download/downloadfile/Log_File.zip)

When an unsuccessful login operation is made on RDP, the "Event ID 4625 - An account failed to log on" log is generated. If we follow this log, we can track down the attacker.



After filtering, we see 4 logs with 4625 Event IDs.

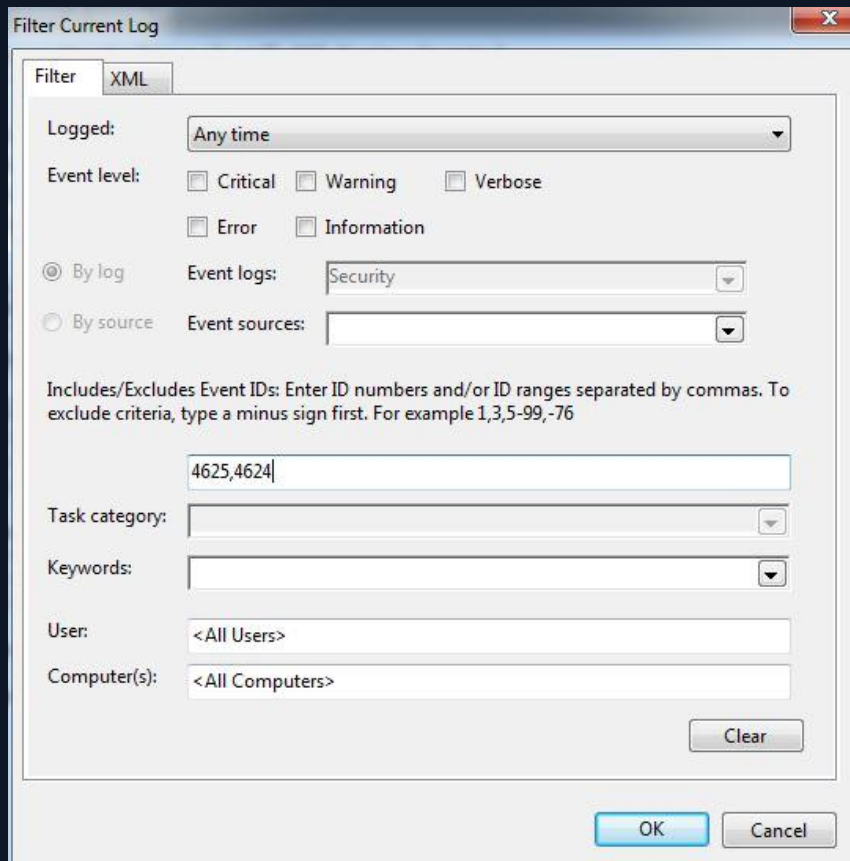
Keywords	Date and Time	Source	Event ID	Task Category
Audit Failure	2/23/2021 10:17:11 PM	Microsoft Wind...	4625	Logon
Audit Failure	2/23/2021 10:17:01 PM	Microsoft Wind...	4625	Logon
Audit Failure	2/23/2021 10:16:58 PM	Microsoft Wind...	4625	Logon
Audit Failure	2/23/2021 10:16:56 PM	Microsoft Wind...	4625	Logon

When we look at the dates, we see that the logs are formed one after the other. When we look at the details, it is seen that all logs are created for the "LetsDefendTest" user.

Keywords	Date and Time	Source	Event ID	Task Category
Audit Failure	2/23/2021 10:17:11 PM	Microsoft Wind...	4625	Logon
Audit Failure	2/23/2021 10:17:01 PM	Microsoft Wind...	4625	Logon
Audit Failure	2/23/2021 10:16:58 PM	Microsoft Wind...	4625	Logon
Audit Failure	2/23/2021 10:16:56 PM	Microsoft Wind...	4625	Logon

Event 4625, Microsoft Windows security auditing.	
General	Details
Account For Which Logon Failed:	
Security ID:	NULL SID
Account Name:	LetsDefendTest
Account Domain:	WIN-CGAK3CTL9KR
Failure Information:	
Failure Reason:	Unknown user name or bad password.
Status:	0xc000006d
Sub Status:	0xc000006a
Process Information:	

As a result, we understand that the attacker has unsuccessfully attempted to login 4 times. To understand whether the attack was successful or not, we can search for the 4624 logs we saw in the previous section.



Filtered: Log: Security; Source: ; Event ID: 4625,4624. Number of events: 14

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	2/23/2021 10:17:20 PM	Microsoft Wind...	4624	Logon
Audit Failure	2/23/2021 10:17:11 PM	Microsoft Wind...	4625	Logon
Audit Failure	2/23/2021 10:17:01 PM	Microsoft Wind...	4625	Logon
Audit Failure	2/23/2021 10:16:58 PM	Microsoft Wind...	4625	Logon
Audit Failure	2/23/2021 10:16:56 PM	Microsoft Wind...	4625	Logon

Event 4624, Microsoft Windows security auditing.

General Details

New Logon:

- Security ID: WIN-CGAK3CTL9KR\LetsDefendTest
- Account Name: LetsDefendTest
- Account Domain: WIN-CGAK3CTL9KR
- Logon ID: 0x1b3e0ce
- Logon GUID: {00000000-0000-0000-0000-000000000000}

Process Information:

- Process ID: 0x1118
- Process Name: C:\Windows\System32\winlogon.exe

As can be seen from the results, the attacker succeeded in connecting to the system with the 4624 log after the 4625 logs.

Protect your organization from a brute force attack in 8 steps

- | | | | |
|----------|-------------------------------------|----------|--|
| 1 | Manage user credentials | 5 | Approve access to sensitive resources manually |
| 2 | Limit the number of login attempts | 6 | Monitor all activity within your network |
| 3 | Enforce multi-factor authentication | 7 | Educate your employees |
| 4 | Configure user access rights | 8 | Consider passwordless authentication |

Possible outcomes of a brute force attack



Examples of Brute Force Attacks

PASSWORD GUESSING

This involves using common passwords or combinations to systematically guess a password. This can also include a dictionary attack, where an attacker uses all known words and combinations in a dictionary.

PASSWORD CRACKING

Attackers may use a pre-computed rainbow table to guess a password used to create a particular password hash.

PASSWORD SPRAYING

Password spraying (also known as a reverse brute-force attack) uses a common password and tests it against multiple possible usernames.

References:

- ❖ <https://www.ekransystem.com/en/blog/brute-force-attacks>
- ❖ <https://www.sentinelone.com/blog/detecting-brute-force-password-attacks/>
- ❖ <https://app.letsdefend.io/training/lessons/detecting-brute-force-attacks>