

## SMB Brute Force Saldırısı ve OSSIM ile Alarm İncelemesi

Ana Makine: Kali Linux

Hedef Makine: Windows 10

Kali Linux ile OSSIM ajanı kurulu olan bir Windows 10 makineye SMB brute force saldırısı yapılarak alarm ve log incelemesi yapılacaktır.

Nmap, nse scriptleri kullanılarak hedef makineye (192.168.138.130) SMB brute force saldırı denemesi gerçekleştirilmiştir.

```
(root@kali)-[/home/dogukan]
# nmap --script smb-brute.nse -p445 192.168.138.130
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-24 15:22 EDT
Stats: 0:00:55 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 0.00% done
Nmap scan report for 192.168.138.130
Host is up (0.00051s latency).

PORT      STATE SERVICE
445/tcp   open  microsoft-ds
MAC Address: 00:0C:29:8A:30:10 (VMware)

Host script results:
| smb-brute:
|   administrator:<blank> => Valid credentials, account disabled
|_  guest:<blank> => Valid credentials, account disabled

Nmap done: 1 IP address (1 host up) scanned in 57.68 seconds
```

Saldırı tamamlandıktan sonra OSSIM arayüzünden Windows 10 makinesinde kurulu ajanların logladığı alarmları inceliyoruz.

ALARMS

LIST VIEW

GROUP VIEW

Alarms > AV-FREE-FEED Bruteforce attack, Windows authentication attack against windows

Bruteforce Authentication — Windows Login

Status	Risk	Attack Pattern	Created	Duration	# Events	Alarm ID	OTX Indicators
	<b>CRITICAL</b>	external to internal one-to-one	3 secs ago	3 mins	2,264	29DA15D649F211EF8D26000C3FDE925F	0

Source (1)

192.168.138.131

Location: Unknown

Asset Groups: Unknown

Networks: Local\_192\_168\_138\_0\_24

OTX IP Reputation: No

Destination (1)

192.168.138.130

Location: Unknown

Asset Groups: Unknown

Networks: Local\_192\_168\_138\_0\_24

OTX IP Reputation: No

USERNAME	USERDATA1	USERDATA2	USERDATA4	USERDATA5	USERDATA6
root	5	windows.win_authentication_failed,	4625	3	?
USERDATA7	USERDATA8	USERDATA9			
%%2313	-	192.168.138.131			

RAW LOG

AV - Alert - "1721848859" --> RID: "18130"; RL: "5"; RG: "windows.win\_authentication\_failed,"; RC: "Logon Failure - Unknown user or bad password."; USER: "- Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: root "; SRCIP: "192.168.138.131"; HOSTNAME: "(windows) 192.168.138.130->WinEvtLog"; LOCATION: "(windows) 192.168.138.130->WinEvtLog"; EVENT: "[INIT]2024 Jul 24 12:20:36 WinEvtLog: Security: AUDIT FAILURE(4625): Microsoft-Windows-Security-Auditing: (no user): no domain: DESKTOP-F150F68: An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: root Account Domain: ? Failure Information: Failure Reason: %%2313 Status: 0xc000006d Sub Status: 0xc0000064 Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: \\192.168.138.131 Source Network Address: 192.168.138.131 Source Port: 36082 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: WVM Transmitted Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted.[END]";

VIEW MORE

<input type="checkbox"/>	2024-07-24 15:25:43	open	Bruteforce Authentication	Windows Login	Failed	N/A	192.168.138.131:36082	windows	
<input type="checkbox"/>	2024-07-24 15:25:26	open	Bruteforce Authentication	Windows Login	Failed	N/A	192.168.138.131:36082	windows	
<input type="checkbox"/>	2024-07-24 15:25:06	open	Bruteforce Authentication	Windows Login	Failed	N/A	192.168.138.131:36082	windows	
<input type="checkbox"/>	2024-07-24 15:24:43	open	Bruteforce Authentication	Windows Login	Failed	N/A	192.168.138.131:36082	windows	
<input type="checkbox"/>	2024-07-24 15:24:24	open	Bruteforce Authentication	Windows Login	Failed	N/A	192.168.138.131:36082	windows	
<input type="checkbox"/>	2024-07-24 15:24:06	open	Bruteforce Authentication	Windows Login	Failed	N/A	192.168.138.131:36082	windows	
<input type="checkbox"/>	2024-07-24 15:23:47	open	Bruteforce Authentication	Windows Login	Failed	N/A	192.168.138.131:36082	windows	
<input type="checkbox"/>	2024-07-24 15:23:28	open	Bruteforce Authentication	Windows Login	Failed	N/A	192.168.138.131:36082	windows	
<input type="checkbox"/>	2024-07-24 15:23:03	open	Bruteforce Authentication	Windows Login	Failed	N/A	192.168.138.131:36082	windows	
<input type="checkbox"/>	2024-07-24 15:22:31	open	Bruteforce Authentication	Windows Login	Failed	N/A	192.168.138.131:36082	windows	
<input type="checkbox"/>	2024-07-24 15:22:05	open	Bruteforce Authentication	Windows Login	Failed	N/A	192.168.138.131:36082	windows	
<input type="checkbox"/>	2024-07-24 15:21:45	open	Bruteforce Authentication	Windows Login	Failed	N/A	192.168.138.131:36082	windows	
<input type="checkbox"/>	2024-07-24 15:21:26	open	Bruteforce Authentication	Windows Login	Failed	N/A	192.168.138.131:36082	windows	
<input type="checkbox"/>	2024-07-24 15:20:55	open	Bruteforce Authentication	Windows Login	Failed	N/A	192.168.138.131:34174	windows	

STATUS	Open
PRIORITY	2 Low
TRANSFER TO	User: - No users found-
ATTACHMENT	Browse... No file selected.
DESCRIPTION *	<p>H1 H2 H3   B I        </p> <p>2024-07-24 15:20:55'de başlayıp, 2024-07-24 15:27:09'a kadar süren 192.168.138.131 IP adresinden Logon Failure uyarıları gelmektedir.</p>
ACTION	<p>H1 H2 H3   B I        </p> <p>Brute Force saldırısı olduğu tespit edilmiş ve gerekli IP adresinin engellenmesi gerekmektedir.</p>

## SSH Brute Force Saldırısı ve OSSIM ile Alarm İncelemesi

Kali Linux makinesinden Ubuntu hedef makinesine SSH Brute Force saldırısı yapılmıştır.

```
(root@kali)~[/home/dogukan]
# nmap -p 22 --script ssh-brute --script-args userdb= /Desktop/passwords.txt passdb= /Desktop/users.txt / --script-args ssh-brute.timeout=4s 192.168.138.132
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-25 04:27 EDT
Unable to split netmask from target expression: "/Desktop/passwords.txt"
Failed to resolve "passdb-".
Unable to split netmask from target expression: "/Desktop/users.txt"
Unable to split netmask from target expression: "/"
NSE: [ssh-brute] Trying username/password pair: root:root
NSE: [ssh-brute] Trying username/password pair: admin:admin
NSE: [ssh-brute] Trying username/password pair: administrator:administrator
NSE: [ssh-brute] Trying username/password pair: webadmin:webadmin
NSE: [ssh-brute] Trying username/password pair: sysadmin:sysadmin
NSE: [ssh-brute] Trying username/password pair: netadmin:netadmin
NSE: [ssh-brute] Trying username/password pair: guest:guest
NSE: [ssh-brute] Trying username/password pair: user:user
NSE: [ssh-brute] Trying username/password pair: web:web
NSE: [ssh-brute] Trying username/password pair: test:test
NSE: [ssh-brute] Trying username/password pair: root:
```

### Oluşan alarm görüntüleri

Event detail

AlienVault HIDS: SSHD brute force trying to get access to the system.

DATE	2024-07-25 04:27:05 GMT-4:00	CATEGORY	Authentication
ALIENVAULT SENSOR	alienvault [192.168.138.99]	SUB-CATEGORY	Failed
DEVICE IP	192.168.138.132 [eth0]	DATA SOURCE NAME	AlienVault HIDS-authentication_failures
EVENT TYPE ID	5712	DATA SOURCE ID	7012
UNIQUE EVENT ID#	4a5f11ef-a702-000c-29da-15d6ad2399ee	PRODUCT TYPE	Authentication and DHCP
PROTOCOL	TCP	ADDITIONAL INFO	N/A

PRIORITY	RELIABILITY	RISK	OTX INDICATORS
1	1	LOW (0)	0

SOURCE

192.168.138.131

Hostname: N/A  
MAC Address: N/A  
Port: 58656  
Latest update: N/A  
Username & Domain: N/A  
Asset Value: 2

Location: N/A  
Context: N/A  
Asset Groups: N/A  
Networks: Local\_192\_168\_138\_0\_24  
Logged Users: N/A  
OTX IP Reputation: No

DESTINATION

Ubuntu [192.168.138.132]

Hostname: Ubuntu  
MAC Address: N/A  
Port: 0  
Latest update: N/A  
Username & Domain: N/A  
Asset Value: 2





















































Location: N/A  
Context: N/A  
Asset Groups: N/A  
Networks: Local\_192\_168\_138\_0\_24  
Logged Users: N/A  
OTX IP Reputation: No

USERNAME	USERDATA1	USERDATA2	USERDATA3	USERDATA4
webadmin	(Ubuntu) 192.168.138.132->/var/log/auth.log	192.168.138.131	SSHD brute force trying to get access to the system.	syslog.sshd.authentication_failures.

RAW LOG

AV - Alert - "1721896025" -> RID: "5712"; RL: "10"; RG: "syslog.sshd.authentication\_failures,"; RC: "SSHD brute force trying to get access to the system,"; USER: "None"; SRCIP: "192.168.138.131"; HOSTNAME: "(Ubuntu) 192.168.138.132->/var/log/auth.log"; LOCATION: "(Ubuntu) 192.168.138.132->/var/log/auth.log"; EVENT: "[INIT]2024-07-25T11:27:04.938715+03:00 dogukan-VMware-Virtual-Platform sshd[3952]: Failed password for invalid user webadmin from 192.168.138.131 port 58656 ssh2[END]";

## Alarm sonrası False positive kontrolü ve ticket açılması

STATUS	Open
PRIORITY	1 Low
TRANSFER TO	User: - No users found-
ATTACHMENT	Browse... No file selected.
DESCRIPTION *	<div>H1 H2 H3   B I                            </div> <p>2024-07-25 04:27:05 tarihinde 192.168.138.131 IP adresinden SSH Brute Force denemesi tespit edilmiştir.</p>
ACTION	<div>H1 H2 H3   B I                            </div> <p>İlgili IP Adresinin (192.168.138.131) engellenmesi gerekmektedir.</p>