## SMB Brute Force Saldırısı ve OSSIM ile Alarm İncelemesi

Ana Makine: Kali Linux

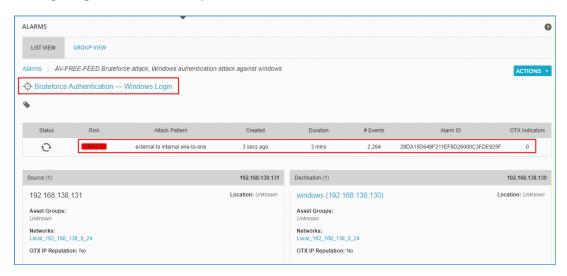
Hedef Makine: Windows 10

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

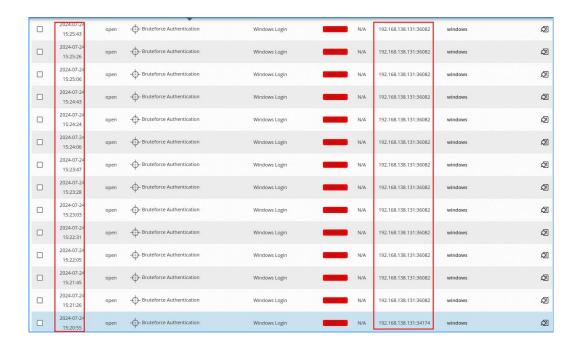
Nmap, nse scriptleri kullanılarak hedef makineye (192.168.138.130) SMB brute force saldırı denemesi gerçekleştirilmiştir.

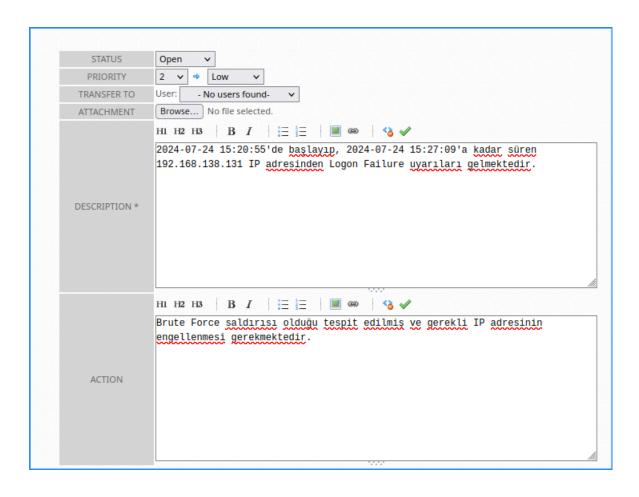
```
| map -script smb-brute.nse -p445 192.168.138.130 |
| Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-24 15:22 EDT |
| Stats: 0:00:55 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan |
| NSE Timing: About 0.00% done |
| Nmap scan report for 192.168.138.130 |
| Host is up (0.00051s latency). |
| PORT STATE SERVICE |
| 445/tcp open microsoft-ds |
| MAC Address: 00:0C:29:8A:30:10 (VMware) |
| Host script results: | smb-brute: | administrator:<br/>| blank> ⇒ Valid credentials, account disabled |
| guest:<br/>| 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 kurulı ajanların logladığı alarmları inceliyoruz.





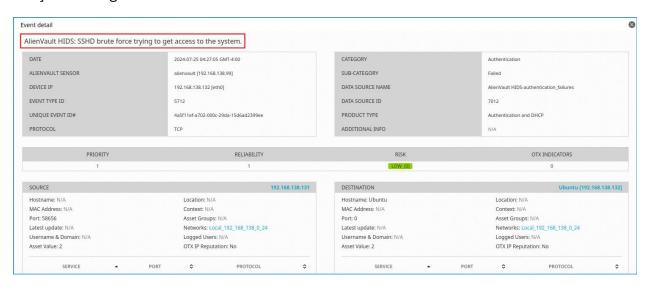




## SSH Brute Force Saldırısı ve OSSIM ile Alarm İncelemesi

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

## Oluşan alarm görüntüleri





## Alarm sonrası False positive kontrolü ve ticket açılması

