ALERT ID
soc20260601-001

Correct Classification
True Positive – Attività di Ricognizione di Rete (Scansione Nmap)

Severity
Low

Report SOC
L'alert è stato generato a seguito del rilevamento di un'attività di scansione di rete rumorosa compatibile con l'utilizzo dello strumento Nmap. Il comportamento osservato indica un'attività di enumerazione sistematica e ad alta frequenza dei servizi esposti sull'unico web server presente nell'ambiente. L'attività non risulta associata a test autorizzati né a operazioni di manutenzione note e rappresenta una fase di ricognizione potenzialmente preliminare ad azioni malevole successive.

Time of Activity
06/01/2026 20:31

List of Affected Entities

Source IP:
192.168.50.10

Destination IP:
192.168.50.40

Target Host:
WEBSRV01

Network Segment:
DMZ

Source of Detection:
Log di rete / Firewall

Reason for Classifying as True Positive / False Positive
Questo alert è classificato come True Positive. L'indirizzo IP sorgente ha generato numerosi tentativi di connessione verso porte differenti del web server in un intervallo temporale ristretto. Il pattern, la frequenza e la distribuzione delle richieste sono coerenti con un'attività di port scanning automatizzata e non risultano compatibili con traffico applicativo legittimo o con il normale utilizzo da parte di un utente.

Reason for Escalating the Alert
L'escalation non è necessaria in questa fase. Sebbene l'attività sia confermata come ricognizione malevola, non sono stati osservati tentativi di sfruttamento, autenticazioni sospette o altre evidenze di compromissione. L'evento deve essere monitorato e correlato con eventuali alert successivi per individuare una possibile evoluzione dell'attacco.

Indicators of Compromise (IoC)
L'attività di ricognizione è associata all'indirizzo IP sorgente 192.168.50.10, che ha effettuato tentativi di connessione ripetuti verso il web server WEBSRV01 in DMZ, indirizzo 192.168.50.40. Il pattern osservato è caratterizzato da numerose richieste verso porte differenti in rapida successione, coerenti con l'utilizzo di strumenti di scanning attivo. Non sono stati identificati indicatori di compromissione a livello applicativo o di sistema.

MITRE ATT&CK
L'attività osservata è riconducibile alla tattica Reconnaissance (TA0043). In particolare, il comportamento rilevato è coerente con la tecnica Active Scanning (T1595), utilizzata per individuare servizi e porte esposte su un sistema accessibile dalla rete. Non sono state osservate tecniche riconducibili a fasi successive della kill chain, come Credential Access, Execution o Persistence.

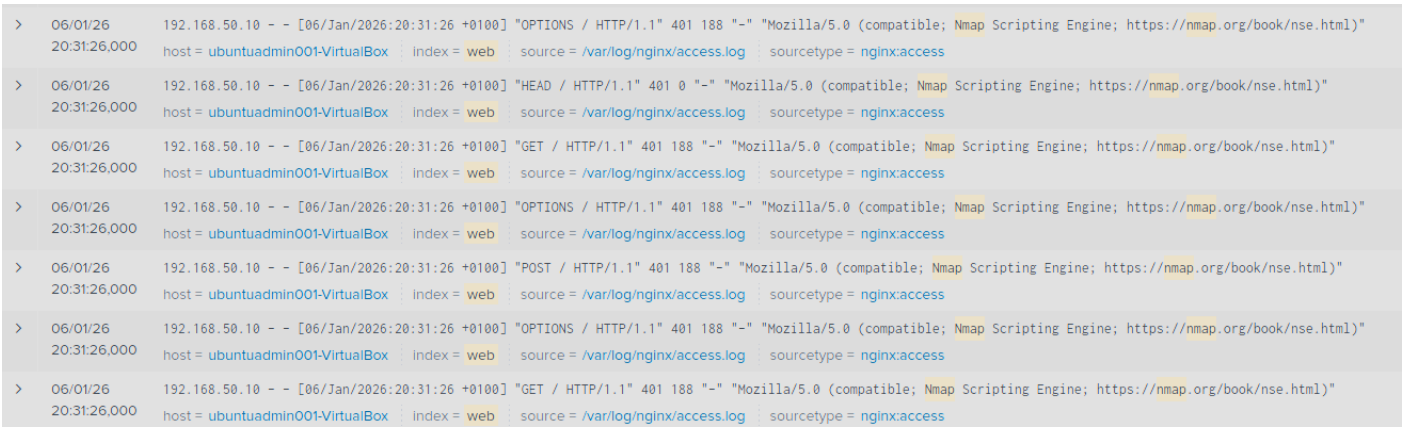
Recommended Actions
Continuare il monitoraggio dell'indirizzo IP sorgente per identificare eventuali attività successive, come tentativi di brute force o di exploit. Verificare se l'attività di scansione sia autorizzata; in caso contrario, valutare il blocco o il rate limiting dell'indirizzo IP. Rafforzare il monitoraggio del web server per rilevare tempestivamente comportamenti anomali successivi alla fase di scansione.

ALLEGATI ALERT soc20260601-001

```
┌──(kali㉿kali)-[~]
└─$ nmap -A -T4 192.168.50.20

Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 14:31 EST
Nmap scan report for 192.168.50.20 (192.168.50.20)
Host is up (0.00048s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.6p1 Ubuntu 3ubuntu13.14 (Ubuntu Linux; protoco
l 2.0)
| ssh-hostkey:
|   256 c4:07:1a:48:24:ba:f7:0b:f0:af:59:bb:a3:bc:1b:a8 (ECDSA)
|_  256 f9:d0:d3:e9:13:90:1d:7f:73:c6:1b:67:07:93:fc:62 (ED25519)
80/tcp open  http    nginx 1.24.0 (Ubuntu)
|_http-title: 401 Authorization Required
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=Restricted Area
|_http-server-header: nginx/1.24.0 (Ubuntu)
MAC Address: 08:00:27:30:CD:68 (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:mikrot
ik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7
.2 - 7.5 (Linux 5.6.3)
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.48 ms 192.168.50.20 (192.168.50.20)

OS and Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.01 seconds
```

L'attacker 192.168.50.10 KALI-LINUX effettua una scansione Nmap particolarmente rumorosa

Il SOC Analyst dopo aver notato un agent-user Nmap, restringe il campo su quell'user-agent per confermare la ricognizione attiva in corso



Dai 35 risultati in una frazione di secondo, è palese che 192.168.50.10 si trovi in fase di footprinting e sta analizzando WEBSRV-01