

ALERT ID

soc20260601-003

Correct Classification

True Positive – Brute Force su Autenticazione HTTP preceduto da Ricognizione di Rete (Nmap)

Severity

Medium

Report SOC

L'alert è stato generato a seguito del rilevamento di un'attività di brute force sull'autenticazione HTTP del web server, compatibile con l'utilizzo dello strumento Hydra. L'attività è stata correlata a una precedente scansione di rete eseguita tramite Nmap dallo stesso indirizzo IP sorgente, indicando una chiara progressione dell'attacco dalla fase di ricognizione alla fase di tentativo di compromissione.

Nel medesimo intervallo temporale sono stati osservati anche tentativi di accesso legittimi da parte di un host Windows interno, associati a un comportamento coerente con errore umano e chiaramente distinguibili dall'attacco automatizzato.

Time of Activity

06/01/2026 tra le 20:31 e le 20:36

List of Affected Entities

Source IP:

192.168.50.10

Destination IP:

192.168.50.40

Target Host:

WEBSRV01

Additional Host Observed:

WINHOST-01

Network Segment:

DMZ

Source of Detection:

Log di rete / Firewall e log web server (nginx)

Reason for Classifying as True Positive / False Positive

Questo alert è classificato come True Positive. L'indirizzo IP 192.168.50.10 ha inizialmente eseguito una scansione di rete rumorosa tramite Nmap verso il web server (alert soc20260601-001), seguita da circa 3800 tentativi di accesso in un intervallo temporale di pochi minuti. I tentativi presentano un pattern altamente ripetitivo, una frequenza anomala e un User-Agent riconducibile allo strumento Hydra, elementi che confermano la natura automatizzata e malevola dell'attività.

In parallelo, sono stati osservati tentativi di accesso HTTP falliti provenienti dall'host WINHOST-01 associati all'utente alice. Tali tentativi risultano limitati nel numero, distribuiti nel tempo e generati da un browser legittimo, indicando un errore umano dovuto a credenziali errate e non un tentativo di brute force. La marcata differenza nel volume e nel comportamento consente di distinguere chiaramente l'attività legittima dall'attacco.

Reason for Escalating the Alert

L'escalation non è necessaria. Sebbene l'attività osservata rappresenti un tentativo diretto di compromissione di un servizio esposto, non sono state rilevate autenticazioni riuscite né evidenze di compromissione del sistema. L'evento è stato completamente contenuto tramite il blocco dell'indirizzo IP attaccante e rientra nelle responsabilità operative del SOC Level 1.

Indicators of Compromise (IoC)

L'attività malevola è associata all'indirizzo IP sorgente 192.168.50.10, responsabile di un volume elevato di richieste HTTP verso il web server WEBSRV01 in DMZ, indirizzo 192.168.50.40. Tra gli indicatori applicativi rilevati figurano l'uso di un User-Agent riconducibile allo strumento Hydra, la ripetizione sistematica di richieste di autenticazione HTTP e la presenza ricorrente di risposte HTTP 401 Unauthorized.

Sono stati inoltre osservati tentativi di accesso legittimi provenienti dall'host WINHOST-01 associati all'utente alice, correttamente esclusi dagli IoC in quanto riconducibili a comportamento benigno.

MITRE ATT&CK Mapping

L'attività osservata coinvolge più fasi della matrice MITRE ATT&CK. La scansione iniziale del web server è riconducibile alla tattica Reconnaissance (TA0043), in particolare alla tecnica Active Scanning (T1595).

Il brute force sull'autenticazione HTTP rientra nella tattica Credential Access (TA0006) ed è coerente con la tecnica Brute Force (T1110), nello specifico Password Guessing (T1110.001).

Non sono state osservate tecniche riconducibili a Execution, Persistence o Command and Control, in quanto l'attacco non ha portato a una compromissione riuscita.

Recommended Actions

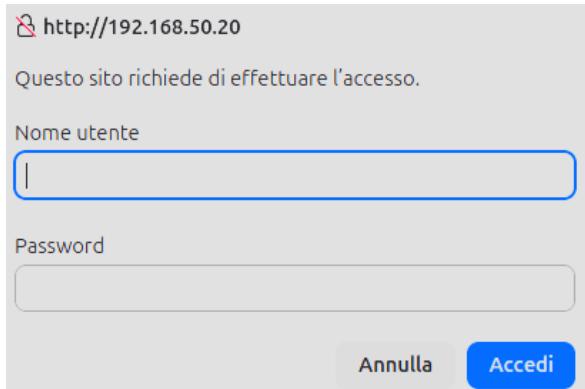
Bloccare l'indirizzo IP 192.168.50.10 sul firewall per interrompere ulteriori tentativi di accesso. Verificare l'assenza di autenticazioni HTTP riuscite durante e dopo la finestra temporale dell'attacco. Continuare il monitoraggio del web server per individuare eventuali tentativi di bypass o attività anomale successive. Non è richiesta alcuna azione correttiva sull'account alice, trattandosi di tentativi di accesso legittimi falliti.

```
(kali㉿kali)-[~]
$ hydra -l admin -P /usr/share/wordlists/rockyou.txt \
http-get://192.168.50.20/ \
-t 4 -V

Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-01-06 14:
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip

[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p
[DATA] attacking http-get://192.168.50.20:80/
[ATTEMPT] target 192.168.50.20 - login "admin" - pass "123456" - 1 of 1434439
[ATTEMPT] target 192.168.50.20 - login "admin" - pass "12345" - 2 of 14344399
[ATTEMPT] target 192.168.50.20 - login "admin" - pass "123456789" - 3 of 1434
[ATTEMPT] target 192.168.50.20 - login "admin" - pass "password" - 4 of 14344
[ATTEMPT] target 192.168.50.20 - login "admin" - pass "iloveyou" - 5 of 14344
[ATTEMPT] target 192.168.50.20 - login "admin" - pass "princess" - 6 of 14344
[ATTEMPT] target 192.168.50.20 - login "admin" - pass "1234567" - 7 of 143443
[ATTEMPT] target 192.168.50.20 - login "admin" - pass "rockyou" - 8 of 143443
[ATTEMPT] target 192.168.50.20 - login "admin" - pass "12345678" - 9 of 14344
[ATTEMPT] target 192.168.50.20 - login "admin" - pass "abc123" - 10 of 143443
[ATTEMPT] target 192.168.50.20 - login "admin" - pass "nicole" - 11 of 143443
[ATTEMPT] target 192.168.50.20 - login "admin" - pass "daniel" - 12 of 143443
```

L'attacker 192.168.50.10 effettua un brute-force da dizionario noto (rockyou.txt) cercando di forzare l'accesso HTTP su porta 80 dell'asset WEBSRV-01 192.168.50.20



L'utente Alice dall'endpoint WINHOST-01 tenta di effettuare l'accesso, non ricordando la password e il nome utente

```
index** src_ip**
| eval service=case(
    match(_raw,"(?i)nmap"), "nmap",
    match(_raw,"(?i)hydra"), "hydra",
    match(_raw,"(?i)sshd|Failed password|Invalid user|Accepted password"), "ssh",
    match(_raw,"(?i)nginx|apache|GET |POST |http"), "http",
    true(), "other"
)
| stats count as tentativi by src_ip service
| sort - tentativi
```

I log linux generalmente non sono facilmente interrogabili, non consentono una semplice estrazione dei campi, per cui è necessario utilizzare delle apposite regex per permettere di individuare correttamente certi campi e classificarli; nella Query in alto andiamo a disporre in tabella gli ip sorgente e il servizio di riferimento ricavato tramite regex, ordinati in base al numero di tentativi.

```
index** src_ip*
| eval service=case(
| match(_raw,"(?:nmap)", "nmap",
| match(_raw,"(?:hydra)", "hydra",
| match(_raw,"(?:sshd|Failed password|Invalid user|Accepted password)", "ssh",
| match(_raw,"(?:nginx|apache|GET |POST |http)", "http",
| true(), "other"
)
| stats count as tentativi by src_ip service
| sort - tentativi
```

3.856 eventi (06/01/26 18:00:00,000 - 06/01/26 21:39:32,000) Nessun campionamento degli eventi ▾

Eventi Pattern Statistiche (4) Visualizzazione

Mostra: 20 per pagina ▾ Formato ▾ Anteprima: on

src_ip	service	tentativi
192.168.50.10	hydra	3803
192.168.50.10	nmap	35
192.168.50.30	http	14
192.168.50.10	http	4

Ora il quadro è molto più chiaro, l'ip noto 192.168.50.30 ha effettuato 14 tentativi con tempistiche umane e irregolari, l'attacker 192.168.50.10 ha effettuato un Brute Force con Hydra con 3803 tentativi in breve tempo.

i	Ora	Evento
>	06/01/26 20:36:42,000	192.168.50.30 - alice [06/Jan/2026:20:36:42 +0100] "GET /favicon.ico HTTP/1.1" 404 196 "http://192.168.50.20/login.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36 Edg/143.0.0.0"
		host = ubuntuadmin001-VirtualBox index = web source = /var/log/nginx/access.log sourcetype = nginx:access src_ip = 192.168.50.30
>	06/01/26 20:36:42,000	192.168.50.30 - alice [06/Jan/2026:20:36:42 +0100] "GET /login.php HTTP/1.1" 404 196 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36 Edg/143.0.0.0"
		host = ubuntuadmin001-VirtualBox index = web source = /var/log/nginx/access.log sourcetype = nginx:access src_ip = 192.168.50.30
>	06/01/26 20:36:38,000	192.168.50.30 - alice [06/Jan/2026:20:36:38 +0100] "GET /login.php HTTP/1.1" 401 590 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36 Edg/143.0.0.0"
		host = ubuntuadmin001-VirtualBox index = web source = /var/log/nginx/access.log sourcetype = nginx:access src_ip = 192.168.50.30
>	06/01/26 20:36:33,000	192.168.50.30 - alice password [06/Jan/2026:20:36:33 +0100] "GET /login.php HTTP/1.1" 401 590 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36 Edg/143.0.0.0"
		host = ubuntuadmin001-VirtualBox index = web source = /var/log/nginx/access.log sourcetype = nginx:access src_ip = 192.168.50.30
>	06/01/26 20:36:30,000	192.168.50.30 - alice [06/Jan/2026:20:36:30 +0100] "GET /login.php HTTP/1.1" 401 590 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36 Edg/143.0.0.0"
		host = ubuntuadmin001-VirtualBox index = web source = /var/log/nginx/access.log sourcetype = nginx:access src_ip = 192.168.50.30
>	06/01/26 20:36:26,000	192.168.50.30 - - [06/Jan/2026:20:36:26 +0100] "GET /login.php HTTP/1.1" 401 590 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36 Edg/143.0.0.0"
		host = ubuntuadmin001-VirtualBox index = web source = /var/log/nginx/access.log sourcetype = nginx:access src_ip = 192.168.50.30

Notare l'irregolarità del timestamp che evidenzia dei tentativi "umani".

>	06/01/26 20:36:22,000	192.168.50.10 - admin [06/Jan/2026:20:36:22 +0100] "GET / HTTP/1.1" 401 188 "-" "Mozilla/4.0 (Hydra)"
>	06/01/26 20:36:22,000	host = ubuntuadmin001-VirtualBox index = web source = /var/log/nginx/access.log sourcetype = nginx:access src_ip = 192.168.50.10
>	06/01/26 20:36:22,000	192.168.50.10 - admin [06/Jan/2026:20:36:22 +0100] "GET / HTTP/1.1" 401 188 "-" "Mozilla/4.0 (Hydra)"
>	06/01/26 20:36:22,000	host = ubuntuadmin001-VirtualBox index = web source = /var/log/nginx/access.log sourcetype = nginx:access src_ip = 192.168.50.10
>	06/01/26 20:36:22,000	192.168.50.10 - admin [06/Jan/2026:20:36:22 +0100] "GET / HTTP/1.1" 401 188 "-" "Mozilla/4.0 (Hydra)"
>	06/01/26 20:36:22,000	host = ubuntuadmin001-VirtualBox index = web source = /var/log/nginx/access.log sourcetype = nginx:access src_ip = 192.168.50.10
>	06/01/26 20:36:22,000	192.168.50.10 - admin [06/Jan/2026:20:36:22 +0100] "GET / HTTP/1.1" 401 188 "-" "Mozilla/4.0 (Hydra)"
>	06/01/26 20:36:22,000	host = ubuntuadmin001-VirtualBox index = web source = /var/log/nginx/access.log sourcetype = nginx:access src_ip = 192.168.50.10
>	06/01/26 20:36:22,000	192.168.50.10 - admin [06/Jan/2026:20:36:22 +0100] "GET / HTTP/1.1" 401 188 "-" "Mozilla/4.0 (Hydra)"
>	06/01/26 20:36:22,000	host = ubuntuadmin001-VirtualBox index = web source = /var/log/nginx/access.log sourcetype = nginx:access src_ip = 192.168.50.10
>	06/01/26 20:36:22,000	192.168.50.10 - admin [06/Jan/2026:20:36:22 +0100] "GET / HTTP/1.1" 401 188 "-" "Mozilla/4.0 (Hydra)"
>	06/01/26 20:36:22,000	host = ubuntuadmin001-VirtualBox index = web source = /var/log/nginx/access.log sourcetype = nginx:access src_ip = 192.168.50.10
>	06/01/26 20:36:22,000	192.168.50.10 - admin [06/Jan/2026:20:36:22 +0100] "GET / HTTP/1.1" 401 188 "-" "Mozilla/4.0 (Hydra)"
>	06/01/26 20:36:22,000	host = ubuntuadmin001-VirtualBox index = web source = /var/log/nginx/access.log sourcetype = nginx:access src_ip = 192.168.50.10

Notare l'estrema velocità (e rumorosità) dell'attacco che si palesa.