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.

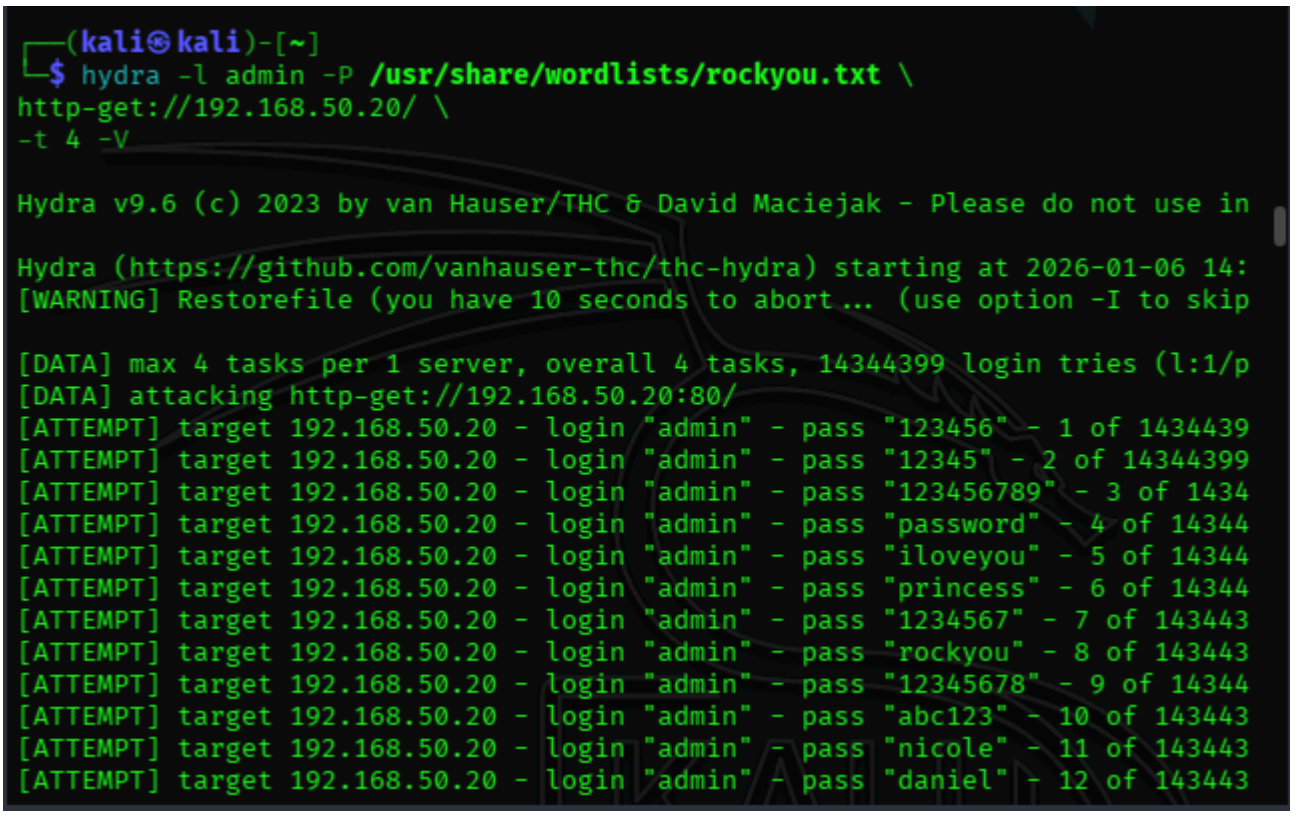
Reason for Escalating the Alert
L'escalation non è necessaria. Sebbene l'attività osservata rappresenti un tentativo diretto di compromissione di un servizio esposto, non sono state rilevate autenticazioni riuscite né evidenze di compromissione del sistema. L'evento è stato completamente contenuto tramite 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.

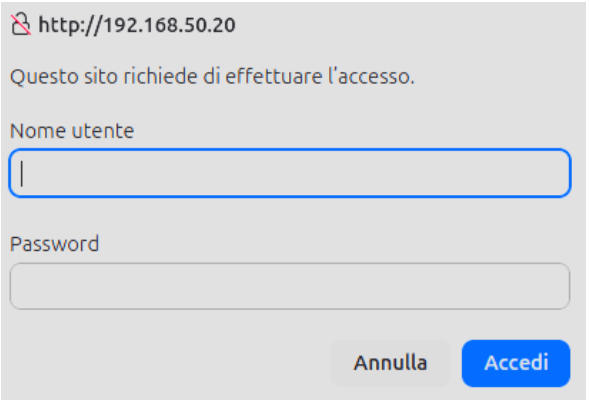
MITRE ATT&CK Mapping
L'attività osservata coinvolge più fasi della matrice MITRE ATT&CK. La scansione iniziale del web server è riconducibile alla tattica Reconnaissance (TA0043), in particolare alla tecnica Active Scanning (T1595).
Il brute force sull'autenticazione HTTP rientra nella tattica Credential 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.

ALLEGATI ALERT soc20260601-003

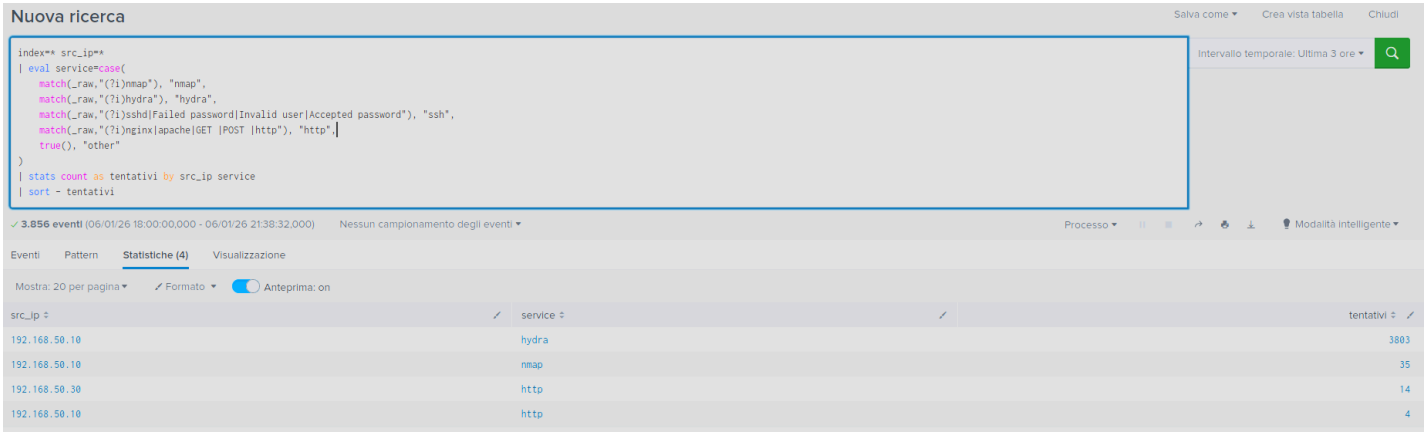


L'attacker 192.168.50.10 effettua un brute-force da dizionario noto (rockyou.txt) cercando di forzare l'accesso HTTP su porta 80 dell'asset WEBSRV-01 192.168.50.20

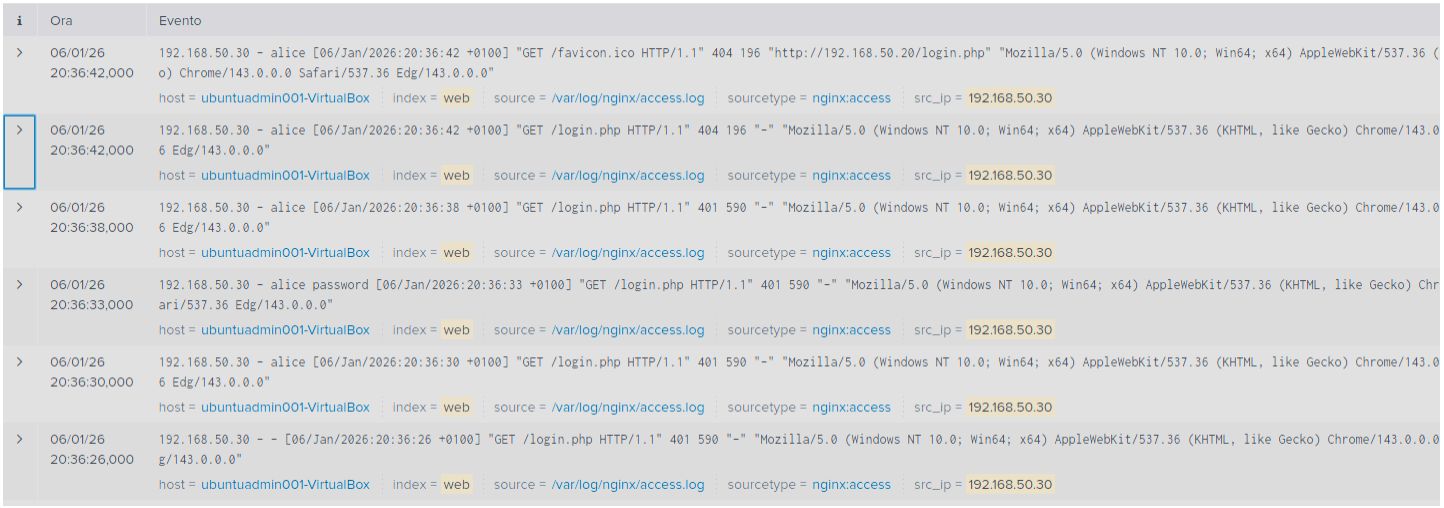


L'utente Alice dall'endpoint WINHOST-01 tenta di effettuare l'accesso, non ricordando la password e il nome utente

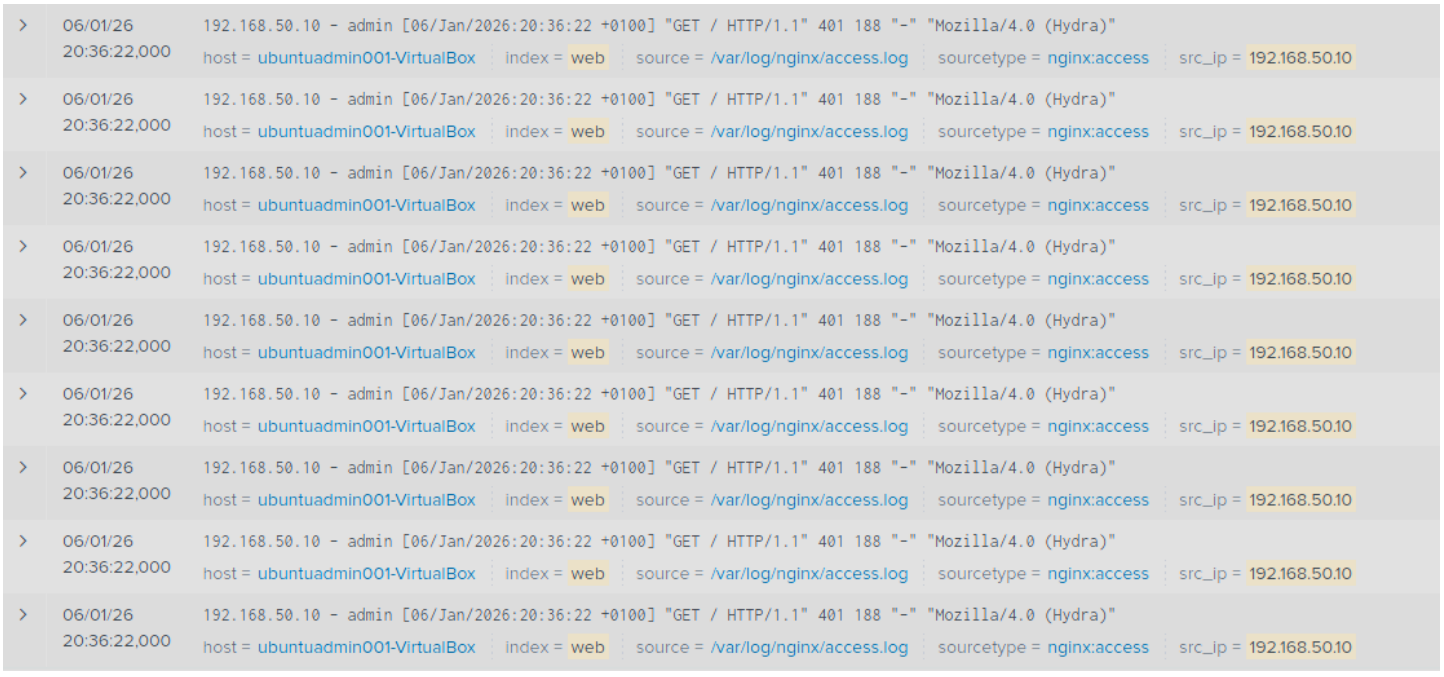
I log linux generalmente non sono facilmente interrogabili, non consentono una semplice estrazione dei campi, per cui è necessario utilizzare delle apposite regex per permettere di individuare correttamente certi campi e classificarli; nella Query in alto andiamo a disporre in tabella gli ip sorgente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



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.



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



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