

Day 26 -Investigate SSH Brute Force Attack

Investigate SSH Brute Force Attack

Ci colleghiamo alla web UI di **Elasticsearch** ed andiamo su Security->Alerts, possiamo investigare su degli eventi usando le Timeline.

Prima di procedere dobbiamo individuare le info importanti per investigare su un attacco Brute Force:

-Questo indirizzo ip è conosciuto per eseguire attività di brute force?

-Ci sono altri utenti che colpisce? E' riuscito ad autenticarsi con successo?

Possiamo rispondere a queste domande servendoci di portali esterni come **abuseipdb** e **greynoise** (prossime 2 slides), possiamo quindi cercare un Ip registrato in uno degli alert sui siti appena indicati.

[Expand details](#)



Low

Oct 9, 2024 @ 21:10:02.182

[SSH Brute Force Attempt - johndoe](#)

Status	Risk score	Assignees
Open	21	+

Overview

Table

JSON

[Investigation guide](#)

There's no investigation guide for this rule.

Highlighted fields

Field	Value
source.ip	61.152.124.178
user.name	root
kibana.alert.rule.type	threshold
kibana.alert.threshold_result.count	30
kibana.alert.threshold_result.term.s.value	root 61.152.124.178



LOGIN

SIGN UP

Home

Report IP

Bulk Reporter

Pricing

About

FAQ

Documentation ▾

Statistics

IP Tools ▾

Contact

AbuseIPDB » 61.152.124.178

Check an IP Address, Domain Name, or Subnet
e.g. 45.87.212.182, microsoft.com, or 5.188.10.0/24

45.87.212.182

CHECK

61.152.124.178 was found in our database!

This IP was reported 67 times. Confidence of Abuse is 100%: ?

100%

ISP	Shanghai Data Solution Co.
Usage Type	Data Center/Web Hosting/Transit
Hostname(s)	a178.innovx.net
Domain Name	shuxun.net
Country	 China
City	Shanghai, Shanghai

IP info including ISP, Usage Type, and Location provided by [IP2Location](#).
Updated monthly.

REPORT 61.152.124.178

WHOIS 61.152.124.178

IP Abuse Reports for 61.152.124.178:

feedback



> MALICIOUS

ISP

61.152.124.178

ORGANIZATION

China Telecom (Group)

ACTOR

unknown



Not Spoofable [?]

Observed Activity

Shows the ports & protocols that this IP scanned, along with the paths that this IP requested. In addition, fingerprints of the SSH & TLS negotiation between this IP and the GreyNoise sensor are shown.

SUMMARY

TIMELINE

PORT 8080 PROTOCOL TCP

WEB PATH /tmui/login.jsp

USER AGENT Googlebot/2.1

PATH /.env

PORT 80 PROTOCOL TCP

USER AGENT python-requests/2.26.0

WEB

Create a free account or log in to view activity from this IP

Examine the ports and protocols that this IP scanned. Get a list of requested web paths and user agents in addition to SSH and TLS fingerprints captured by GreyNoise sensors.

We use cookies to ensure you get the best experience on our website. [Learn more](#)

Got it!

CREATE A FREE ACCOUNT

LOGIN

[View Similar IPs](#) →

FIRST SEEN

2024-08-26

LAST SEEN

2024-10-09

COUNTRY

China

REGION

Shanghai

CITY

Shanghai

ASN

AS4812

Tags [?]

EXPAND DETAILS ▾

SSH Bruteforcer

Generic IoT Default Password Attempt



Investigate SSH Brute Force Attack

Per rispondere invece a «Ci sono altri utenti che colpisce? E' riuscito ad autenticarsi con successo?» Possiamo utilizzare il Discover di Elasticsearch inserendo l'indirizzo IP in questione, abbiamo come risultato solo l'utente root.

The screenshot shows the Elasticsearch Discover interface. At the top, the 'Discover' tab is active. The search bar contains the query `.alerts-security.alerts-default,apm-...` and the filter `61.152.124.178`. Below the search bar, the 'user.name' field is selected, showing 0 results. A sidebar on the left lists 'Popular fields' (1), 'Available fields' (2), 'Empty fields' (20), and 'Meta fields' (0). The 'Available fields' section shows `user.name` and `winlog.user.name`. A right-hand panel displays the 'user.name' field analysis, showing 'Top values' with 'root' at 100% (calculated from 2,123 records) and 'Multi fields' with `user.name.text`. A 'Visualize' button is at the bottom.

Investigate SSH Brute Force Attack

Normalmente l'attività di investigazione viene gestita tramite il sistema di ticketing, dobbiamo fare in modo che questi alert confluiscono nel sistema di ticketing. Andiamo su Security->Rules->Detection Rules , clicco poi sulla regola **"SSH Brute Force Attempt – johndoe"** da lì vado su Edit Rule settings->Action e vediamo che c'è già scelto 'Webhook' che permette di trasmettere l'alert sul sistema di ticketing. Come frequency impostiamo 'for each alert', modifichiamo poi il body e come subject grazie ad una variabile impostiamo stesso il nome della regola, lo stesso anche per il messaggio.

Actions

Choose when to perform actions or snooze them. Notifications are not created for snoozed actions. [Learn more](#)

 Notify when alerts generated

▼  osTicket

Webhook connector

[Add connector](#)

osTicket ▼

Action frequency

For each alert ▼

Per rule run ▼

☐ If alert matches a query

☐ If alert is generated during timeframe

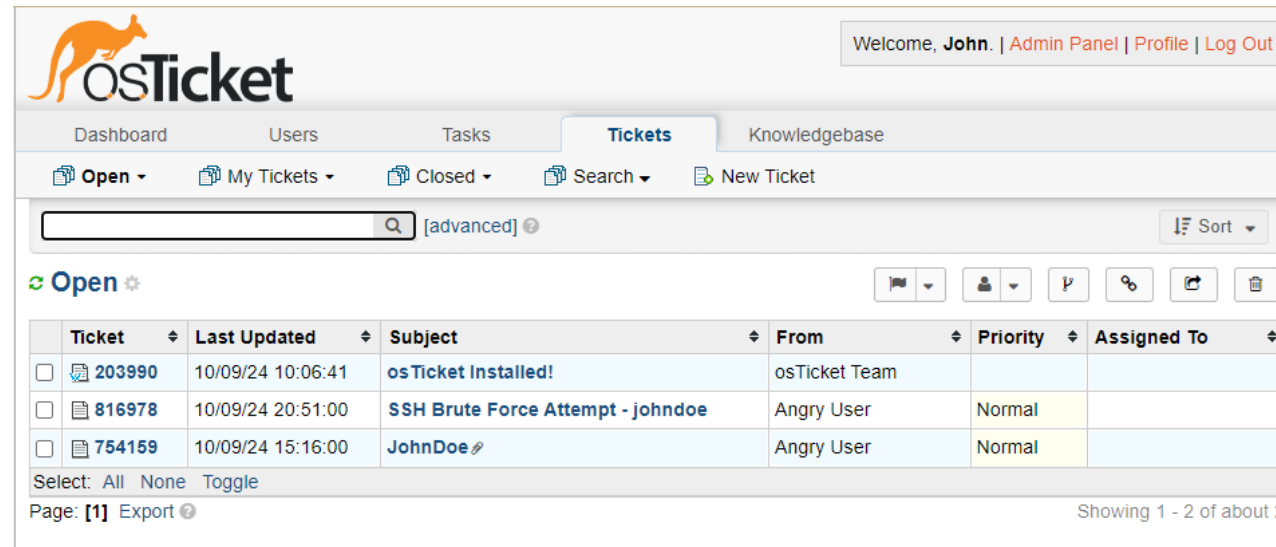
Body

```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <ticket alert="true" autorespond="true" source="API">
3   <name>Elasticsearch</name>
4   <email>api@osticket.com</email>
5   <subject>{{rule.name}}</subject>
6   <phone>318-555-8634X123</phone>
7   <message type="text/plain"><![CDATA[Please investigate the rule: {{rule.name}}]]></message>
8 </ticket>
```

Investigate SSH Brute Force Attack

Verifichiamo su osTicket e troveremo un ticket generato per un nuovo alert che rispetta la struttura indicata:

```
Alert: <Alert Name>  
Source IP: <Source IP>  
User: <User>  
Computer:|
```



Welcome, **John.** | [Admin Panel](#) | [Profile](#) | [Log Out](#)

Dashboard Users Tasks **Tickets** Knowledgebase

[Open](#) [My Tickets](#) [Closed](#) [Search](#) [New Ticket](#)

[advanced] [Sort](#)

[Open](#)

	Ticket	Last Updated	Subject	From	Priority	Assigned To
<input type="checkbox"/>	203990	10/09/24 10:06:41	osTicket Installed!	osTicket Team		
<input type="checkbox"/>	816978	10/09/24 20:51:00	SSH Brute Force Attempt - johndoe	Angry User	Normal	
<input type="checkbox"/>	754159	10/09/24 15:16:00	JohnDoe	Angry User	Normal	

Select: [All](#) [None](#) [Toggle](#)

Page: **[1]** [Export](#)

Showing 1 - 2 of about 2

Consultando la documentazione di Elastic possiamo vedere tutte le variabili che possiamo includere cosa contengono esattamente.


Investigate SSH Brute Force Attack

Possiamo includere nel messaggio anche l'url della regola, ma prima va modificato un parametro nel file di configurazione di kibana e riavviato il servizio.

```
root@ELK: ~  
GNU nano 6.2 /etc/kibana/kibana.yml *  
# For more configuration options see the configuration guide for Kibana in  
# https://www.elastic.co/guide/index.html  
  
# ===== System: Kibana Server =====  
# Kibana is served by a back end server. This setting specifies the port to use.  
server.port: 5601  
  
# Specifies the address to which the Kibana server will bind. IP addresses and host names are both valid values.  
# The default is 'localhost', which usually means remote machines will not be able to connect.  
# To allow connections from remote users, set this parameter to a non-loopback address.  
server.host: [REDACTED]  
  
# Enables you to specify a path to mount Kibana at if you are running behind a proxy.  
# Use the `server.rewriteBasePath` setting to tell Kibana if it should remove the basePath  
# from requests it receives, and to prevent a deprecation warning at startup.  
# This setting cannot end in a slash.  
#server.basePath: ""  
  
# Specifies whether Kibana should rewrite requests that are prefixed with  
# `server.basePath` or require that they are rewritten by your reverse proxy.  
# Defaults to `false`.  
#server.rewriteBasePath: false  
  
# Specifies the public URL at which Kibana is available for end users. If  
# `server.basePath` is configured this URL should end with the same basePath.  
server.publicBaseUrl: "http://[REDACTED]:5601"  
  
# The maximum payload size in bytes for incoming server requests.  
#server.maxPayload: 1048576  
  
# The Kibana server's name. This is used for display purposes.  
#server.name: "your-hostname"  
  
# ===== System: Kibana Server (Optional) =====  
# Enables SSL and paths to the PEM-format SSL certificate and SSL key files, respectively.  
# These settings enable SSL for outgoing requests from the Kibana server to the browser.  
#server.ssl.enabled: false  
#server.ssl.certificate: /path/to/your/server.crt  
#server.ssl.key: /path/to/your/server.key  
  
Last login: Wed Oct  9 15:14:07 2024 from [REDACTED]  
root@ELK:~# nano /etc/kibana/kibana.yml  
root@ELK:~# systemctl restart kibana.service  
root@ELK:~#
```


Investigate SSH Brute Force Attack

Come si può osservare in basso a destra è stato incluso nel messaggio il link alla regola che permetterà di visualizzare maggiori dettagli in merito all'alert.



Welcome, **John.** | [Admin Panel](#) | [Profile](#) | [Log Out](#)

Dashboard

Users

Tasks

Tickets

Knowledgebase









Open

My Tickets

Closed

Search

New Ticket



Ticket #277435



SSH Brute Force Attempt - johndoe

Status: Open

Priority: Normal

Department: Support

Create Date: 10/09/24 21:51:28

User:  Angry User (7)  (Manage Collaborators)

Email: api@osticket.com

Source: API

Assigned To: — Unassigned —

SLA Plan: Default SLA

Due Date: 10/11/24 17:00:00

Help Topic: None

Last Message: 10/09/24 21:51:28

Last Response:

Ticket Thread (1)

Tasks

Angry User posted 10/09/24 21:51:28 SSH Brute Force Attempt - johndoe

Please investigate the rule: SSH Brute Force Attempt - johndoe
Link: [http://\[redacted\]/app/security/detections/rules/id/c245f577-ff28-410c-8da1-b0f3424199c0?timerange=\(global:\(linkTo:!\(timeline\),timerange:\(from:1728510385397,kind:absolute,to:1728510685397\)\),timeline:\(linkTo:!\(global\),timerange:\(from:1728510385397,kind:absolute,to:1728510685397\)\)\)](http://[redacted]/app/security/detections/rules/id/c245f577-ff28-410c-8da1-b0f3424199c0?timerange=(global:(linkTo:!(timeline),timerange:(from:1728510385397,kind:absolute,to:1728510685397)),timeline:(linkTo:!(global),timerange:(from:1728510385397,kind:absolute,to:1728510685397))))