

FINAL PROJECT BOOTCAM

CYBERWARRIOR



DIBUAT OLEH :
GARUDA SECURITY



DENGAN ANGGOTA :

**ILHAM KUSUMA
MUHAMMAD LUTFI KIRANSYAH
MUHAMMAD FARID
JESAYA FERNANDO NAPITULU
REZA SATRIA TAMA**

DAFTAR ISI

DAFTAR ISI.....	ii
1. EXECUTIVE SUNMARY	1
2. METHODOLOGY	2
2.1. Perangkat Yang Digunakan.....	2
2.2. Sistem Operasi.....	2
2.3. Infrastruktur Jaringan	3
2.4. Asset Yang Digunakan.....	3
2.5. Wazuh integrations.....	5
3. DETAILED FINDINGS.....	7
3.1. Port Scanning	7
3.2. Terjadinya Brute-Force/Dictionary Attack Pada Ssh Login	7
3.3. Privilege Escalation Attack	8
3.4. Peringatan suspicious file	9
4. RECOMMENDATIONS	10
4.1. Incident Response Plan	10
4.2. Port Scanning	14
4.3. Terjadinya Dictionary Attack Pada Ssh Login.....	14
4.4. Privilege Escalation.....	15
4.5. Mencegah suspicious file pada server	16
5. REFERENCE.....	19

1. EXECUTIVE SUMMARY

Pembuatan lab ini bertujuan untuk memonitoring sebuah server dari serangan-serangan oleh attacker. Dengan menggunakan SIEM atau security information and event management dalam hal ini kami menggunakan wazuh. Kami dapat mendeteksi beberapa serangan dengan memunculkan alert atau peringatan dari wazuh. Sehingga kami tahu bahwa serangan sedang atau telah terjadi.

Dalam lab ini kami bisa melakukan beberapa aktivitas seperti berikut ini :

1. Mendeteksi Port scanning
2. Mendeteksi SSH dictionary attack
3. Block SSH dictionary attack/brute-force
4. Mendeteksi local privilege escalation
5. Mendeteksi suspicious file
6. File integrity monitoring

2. METHODOLOGY

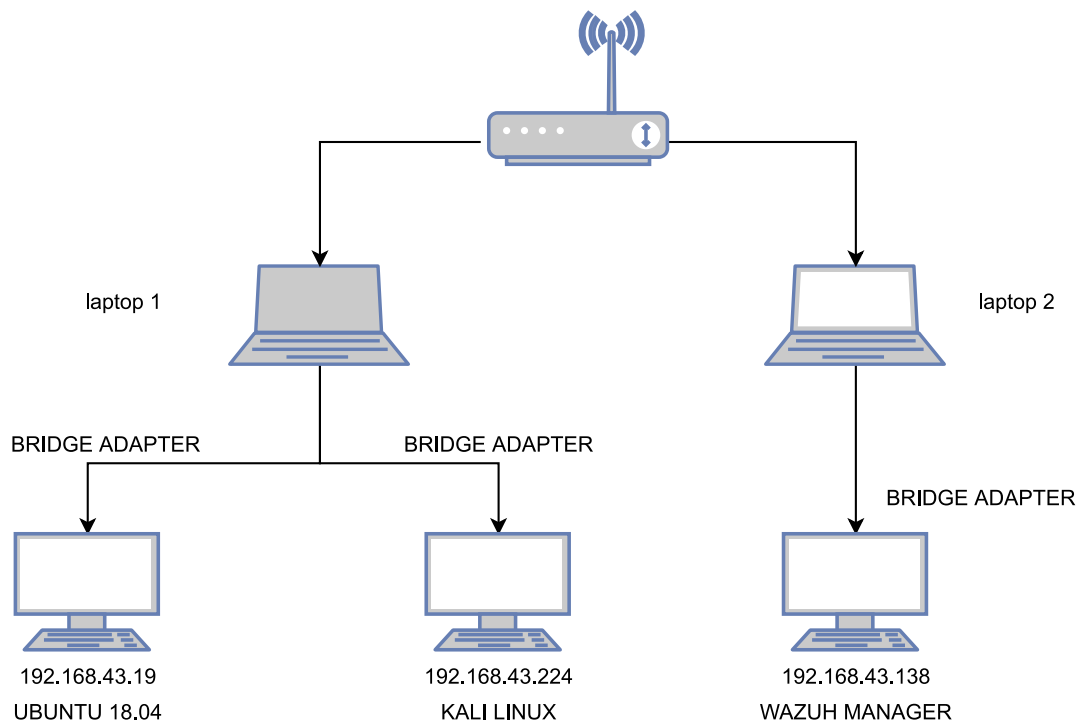
2.1. Perangkat Yang Digunakan

Kami menggunakan dua laptop untuk membuat lab ini. Karena jika hanya memakai 1 laptop maka laptop akan sangat lag. Jadi kami menggunakan 2 laptop.

2.2. Sistem Operasi

- **Wazuh VM**
Wazuh VM kami gunakan untuk lab kali ini sebagai SIEM atau security information and event managemen yaitu wazuh. Wazuh ini digunakan untuk mengumpulkan informasi dan mendeteksi intrusion, threat, dan anomali.
Kelebihan wazuh VM adalah kita hanya perlu meng-import file wazuh vm ke software virtualisasi dan langsung siap pakai. Sehingga kami tidak perlu menginstall satu-persatu.
- **Ubuntu 18.04**
Ubuntu ini digunakan sebagai server yang di monitor oleh SIEM untuk mendeteksi serangan.
Ubuntu yang kami gunakan pada lab ini adalah ubuntu 18.04. karena ubuntu ini memiliki kerentanan CVE-2021-4034 yang digunakan pada lab ini untuk mendeteksi serangan local privilege escalation.
- **Kali linux**
Kali linux digunakan untuk melakukan penyerangan ke server ubuntu yang memiliki kerentanan. Kali linux juga memiliki tools yang lengkap dan sudah terinstall secara default. Jadi kami tidak perlu menginstall satu per satu tools yang akan digunakan.

2.3. Infrastruktur Jaringan



Topologi Jaringan

Untuk menghubungkan wazuh, ubuntu, kali linux dalam 2 laptop. Kami menggunakan adapter virtualbox bridge ke jaringan wifi untuk menghubungkan vm ubuntu, kali linux dan wazuh vm. Agar semua vm pada kedua laptop tersebut dapat saling terhubung.

2.4. Asset Yang Digunakan

- **Virtualbox**

Virtualbox digunakan dalam membuat lab virtual. Virtualbox digunakan untuk menginstall berbagai macam sistem operasi mulai dari linux, windows, mac os dan lain-lain. Pada lab ini kami menggunakan virtualbox untuk menginstall wazuh VM, ubuntu, dan kali linux.

- **Virustotal**

Virustotal digunakan untuk mendeteksi adanya suspicious file yang ada di server ubuntu. Virustotal juga kami integrasikan dengan wazuh. Sehingga jika ada file yang berbahaya maka akan terdeteksi oleh virustotal dan mengirim peringatan ke wazuh.

- **MITRE ATT&CK**

MITRE ATT&CK adalah salah satu framework yang populer untuk threat hunting.

MITRE ATT&CK juga digunakan untuk mengetahui taktik, teknik, dan prosedur yang digunakan oleh penyerang. Sehingga kami menggunakan MITRE ATT&CK pada lab ini.

- **Metasploit framework**

Metasploit framework pada lab ini digunakan untuk mencoba melakukan serangan dictionary attack terhadap server ssh. Serangan tersebut dilakukan untuk mendapatkan username dan password server ubuntu

- **Fail2ban**

Pada lab ini fail2ban digunakan untuk mengamankan proses login layanan ssh. Dengan fail2ban, jika proses autentikasi gagal dalam beberapa kali maka ip dari ssh client tersebut akan di blok selama waktu yang ditentukan.

- **Nmap**

Nmap atau network mapper adalah tools yang biasa digunakan untuk scanning suatu jaringan atau host. Pada lab ini, nmap digunakan untuk port scanning terhadap server ubuntu yang rentan. Nmap juga digunakan untuk mencari kerentanan dari port atau layanan yang dijalankan di server ubuntu.

- **UFW**

Pada lab ini, kami menggunakan firewall bawaan dari sistem operasi ubuntu. UFW ini berfungsi untuk memfilter trafik yang masuk ke server. Mulai dari memblok alamat IP penyerang, sehingga tidak dapat terkoneksi ke server ubuntu.

- **CVE-2021-4034 Proof of Concept By [MEBEIM](#)**

Script ini digunakan untuk melakukan eksploitasi kerentanan CVE-2021-4034 yang terdapat pada server ubuntu.

2.5. Wazuh integrations

Berikut ini adalah cara-cara mengintegrasikan wazuh manager dengan virustotal dan juga integrasi file integrity monitoring pada server ubuntu.

a. Mengintegrasikan wazuh manager dengan virustotal

Virustotal adalah sebuah framework yang dapat mengidentifikasi file, URL, domain, hash file, dan alamat IP yang mencurigakan untuk mendeteksi adanya malware. Pada lab ini, virustotal diintegrasikan dengan siem dalam lab ini adalah Wazuh VM. Interasinya wazuh dan virustotal pada lab ini adalah untuk mendeteksi adanya file-file berbahaya pada server. Karena jika ada malware atau bahkan ransomware, maka itu sangat berbahaya bagi confidentiality, integrity, dan availability data pada server ubuntu.

```
<!-- virustotal -->
<integration>
<name>virustotal</name>
<api_key>1c61eb0ad7a88a991db9f882502c28dad4ff7eaca8cb7ac3732b8697726ceb3d</api_key>
<group>syscheck</group>
<alert_format>json</alert_format>
</integration>
```

Cara Mengintegrasikan Wazuh Dengan Virustotal

Cara mengintegrasikan virustotal dengan wazuh. Pertama, kami mendaftar terlebih dahulu di website virustotal untuk mendapatkan API KEY. Lalu masukan api key tersebut dengan script tambahan di wazuh-manager yang terdapat di file `/var/ossec/etc/ossec.conf`.

b. Mengintegrasikan file integrity monitoring di wazuh manager dan server

Fungsi utama file integrity monitoring adalah mengawasi file atau direktori yang telah dipantau. Jika di direktori atau file yang dipantau, dimodifikasi itu akan memicu peringatan di wazuh. File integrity monitoring di implementasikan pada lab kami, karena ingin mencegah user dengan privilege tertentu untuk memodifikasi direktori atau file yang dipantau.

```
<!-- Directories to check (perform all possible verifications) -->
<directories check_all="yes" whodata="yes">/usr/bin,/usr/sbin</directories>
<directories check_all="yes" whodata="yes">/bin,/sbin,/boot</directories>
<directories check_all="yes" report_changes="yes" whodata="yes" tags="cron">/etc/cron*</directories>
<directories check_all="yes" report_changes="yes" whodata="yes" recursion_level="2">/home,/root</directories>
```

Konfigurasi File Integrity Monitoring

Dengan menambah script yang ditambahkan ke file `/var/ossec/etc/ossec.conf` pada server ubuntu atau wazuh agent. Script ini berisi file yang akan dipantau oleh wazuh manager.

3. DETAILED FINDINGS

3.1. Port Scanning

>	Apr 22, 2022 @ 19:17:16.355	T1043	Command and Control	sshd: insecure connection attempt (scan).	6	5706
>	Apr 22, 2022 @ 19:04:49.116	T1043	Command and Control	sshd: insecure connection attempt (scan).	6	5706

Port Scanning terhadap server Ubuntu

Pada lab kami bisa mendeteksi port scanning. Dengan menggunakan siem wazuh, kami bisa mendeteksi port scanning pada server. Wazuh akan mengirimkan peringatan sehingga kami bisa tau ada percobaan port scanning.

Pada lab ini, wazuh tidak perlu dikonfigurasi. Secara default, wazuh bisa mendeteksi port scanning pada server.

3.2. Terjadinya Brute-Force/Dictionary Attack Pada Ssh Login

Brute Force						×
Credential Access						
>	Apr 22, 2022 @ 00:25:24.766	T1110	Credential Access	5	5710	sshd: Attempt to login using a non-existent user
>	Apr 22, 2022 @ 00:25:22.889	T1110	Credential Access	5	5710	sshd: Attempt to login using a non-existent user
>	Apr 22, 2022 @ 00:25:22.889	T1110	Credential Access	5	5710	sshd: Attempt to login using a non-existent user

Alert pada wazuh mendeteksi brute-force attack

wazuh pada lab ini juga bisa mendeteksi serangan dictionary attack / brute force pada server ubuntu. Dictionary attack terjadi pada server ubuntu yang mencoba untuk mendapatkan username dan password pada layanan ssh. Penyerang mencoba semua kombinasi username dan password di wordlist yang penyerang gunakan.

3.3. Privilege Escalation Attack

Time ↓	Technique(s)	Tactic(s)	Level	Rule ID	Description
> Apr 24, 2022 @ 23:27:45.685	T1078	Defense Evasion, Initial Access, Persistence, Privilege Escalation	3	5501	PAM: Login session opened.
rule.mitre.technique	Valid Accounts				
rule.mitre.id	T1078				
rule.mitre.tactic	Defense Evasion, Initial Access, Persistence, Privilege Escalation				
rule.id	5501				
rule.gpg13	7.8, 7.9				
decoder.parent	pam				
decoder.name	pam				
full_log	Apr 25 02:27:45 osboxes sshd[2640]: pam_unix(sshd:session): session opened for user osboxes by (uid=0)				
location	/var/log/auth.log				

Alert pada wazuh mendeteksi privilege escalation

Pada lab kami, terdeteksi serangan local privilege escalation pada server ubuntu. Penyerang mendapatkan akses dengan menyerang port SSH pada server dan masuk melalui kredensial yang telah di bobol. Hal ini memicu peringatan pada wazuh yang muncul. Sehingga telah terjadi serangan local privilege escalations.

Serangan itu, memanfaatkan celah kerentanan pada pkexec pada server ubuntu 18.04. pkexec sendiri itu merupakan bawaan dari ubuntu 18.04, sehingga kerentanan tersebut belum di patch.

3.4. Peringatan suspicious file

Time ▼	data.virustotal.source.file	data.virustotal.permalink	data.virustotal.malicious
> Apr 24, 2022 @ 02:50:38.416	/home/osboxes/.bash_history	-	0
> Apr 24, 2022 @ 02:43:00: ⊕ ⊖	/home/osboxes/eicar.com	https://www.virustotal.com/ gui/file/275a021bbfb6489e54 d471899f7db9d1663fc695ec2fe 2a2c4538aabf651fd0f/detecti on/f-275a021bbfb6489e54d471 899f7db9d1663fc695ec2fe2a2c 4538aabf651fd0f-1650792807	1

Alert pada wazuh mendeteksi suspicious file

Pada lab ini juga bisa mendeteksi suspicious file yang ada di server. Bisa jadi file tersebut adalah malware atau bahkan ransomware yang sangat berbahaya. Bila file itu telah menginfeksi server, mungkin saja virus tersebut bisa menginfeksi jaringan.

Lab ini mengintegrasikan wazuh dengan virustotal. Sehingga file yang dianggap virustotal berbahaya, maka akan mengirimkan peringatan ke wazuh.

4. RECOMMENDATIONS

4.1. Incident Response Plan

Tools yang digunakan :

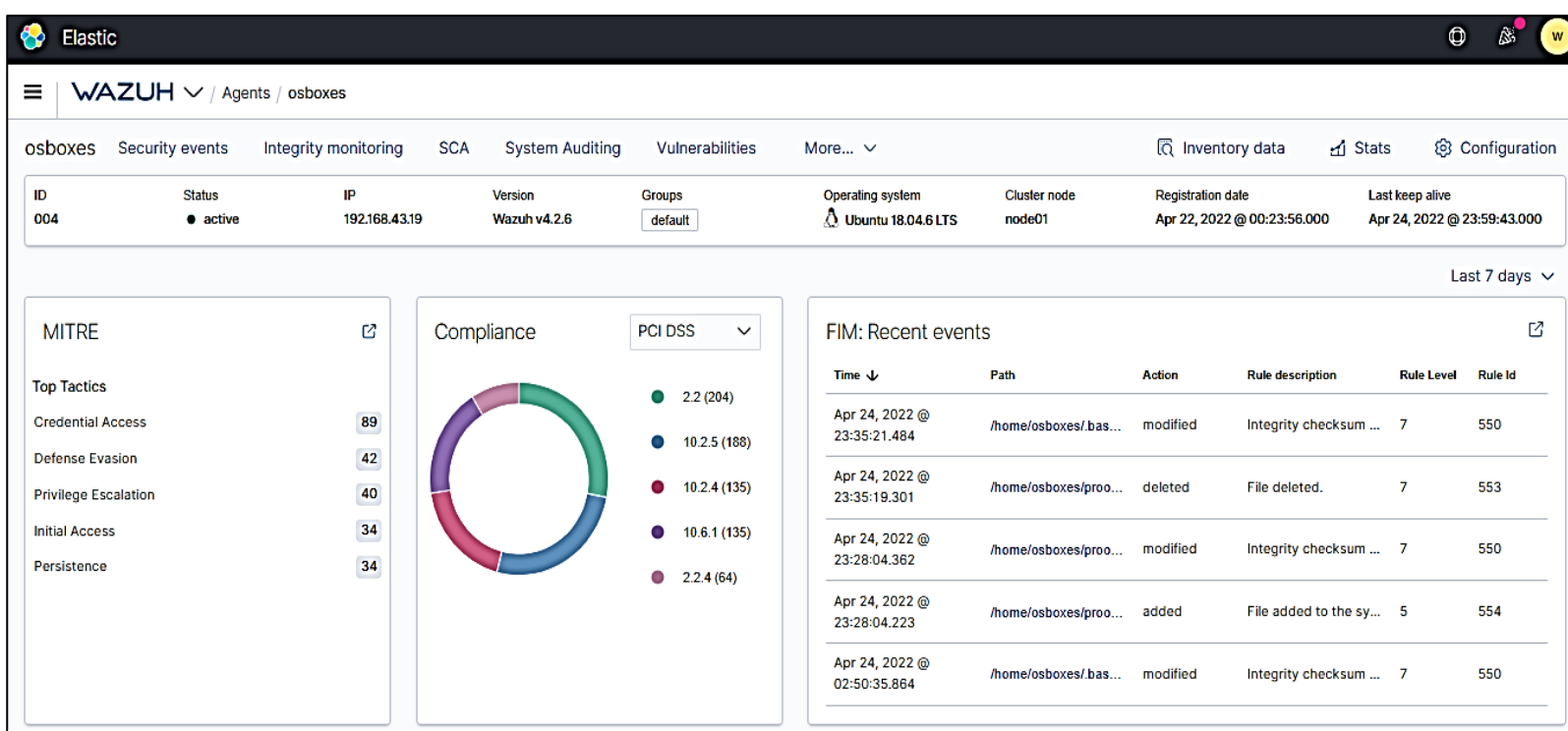
- Siem wazuh
- Astro grep
- UFW
- Fail2ban

A. Preparation

- Mengimplementasikan end point security.
Pada lab ini, untuk melakukan incident response di tahap preparation adalah mengimplementasikan endpoint security. Pada lab ini end point security nya menggunakan wazuh agent yang diintegrasikan dengan wazuh manager.

B. Detection

- Melakukan identifikasi peringatan dengan SIEM Wazuh
Jika ada serangan seperti yang telah dibahas di atas, wazuh pada lab kami bisa mendeteksi serangan tersebut. Serangan tersebut



Dashboard siem wazuh

bisa memicu peringatan di wazuh. Sehingga kami bisa tahu bahwa ada serangan terhadap server ubuntu.

C. Analysis

- Melakukan analisis pada peringatan pada wazuh
Dengan menganalisis peringatan pada wazuh, dapat membantu untuk mengetahui data-data dari incident serangan tersebut. Mulai dari ip dari penyerang dan taktik dan teknik yang dipakai oleh penyerang.
- Melakukan analisis log pada server

```
2107 Apr 22 03:04:23 osboxes sshd[1636]: Failed password for invalid user user2 from 192.168.43.224 port 49991 ssh2
2108 Apr 22 03:04:23 osboxes sshd[1636]: Received disconnect from 192.168.43.224 port 49991:11: Bye Bye [preauth]
2109 Apr 22 03:04:23 osboxes sshd[1636]: Disconnected from invalid user user2 192.168.43.224 port 49991 [preauth]
2110 Apr 22 03:04:23 osboxes sshd[1637]: Failed password for invalid user user2 from 192.168.43.224 port 49992 ssh2
2111 Apr 22 03:04:23 osboxes sshd[1641]: Failed password for osboxes from 192.168.43.224 port 49997 ssh2
2112 Apr 22 03:04:23 osboxes sshd[1637]: Received disconnect from 192.168.43.224 port 49992:11: Bye Bye [preauth]
2113 Apr 22 03:04:23 osboxes sshd[1637]: Disconnected from invalid user user2 192.168.43.224 port 49992 [preauth]
2114 Apr 22 03:04:23 osboxes sshd[1641]: Received disconnect from 192.168.43.224 port 49997:11: Bye Bye [preauth]
2115 Apr 22 03:04:23 osboxes sshd[1641]: Disconnected from authenticating user osboxes 192.168.43.224 port 49997 [preauth]
2116 Apr 22 03:04:23 osboxes sshd[1634]: Failed password for invalid user user2 from 192.168.43.224 port 49989 ssh2
2117 Apr 22 03:04:23 osboxes sshd[1642]: Failed password for osboxes from 192.168.43.224 port 50000 ssh2
2118 Apr 22 03:04:23 osboxes sshd[1640]: Failed password for osboxes from 192.168.43.224 port 49995 ssh2
2119 Apr 22 03:04:23 osboxes sshd[1635]: Failed password for invalid user user2 from 192.168.43.224 port 49990 ssh2
2120 Apr 22 03:04:23 osboxes sshd[1639]: Failed password for osboxes from 192.168.43.224 port 49993 ssh2
2121 Apr 22 03:04:23 osboxes sshd[1658]: Invalid user osboxes.org from 192.168.43.224 port 50008
2122 Apr 22 03:04:23 osboxes sshd[1639]: Received disconnect from 192.168.43.224 port 49993:11: Bye Bye [preauth]
2155 Apr 22 03:04:23 osboxes sshd[1657]: pam_unix(sshd:session): session closed for user osboxes
2156 Apr 22 03:04:23 osboxes systemd-logind[750]: Removed session 8.
2157 Apr 22 03:04:24 osboxes sshd[1653]: Failed password for osboxes from 192.168.43.224 port 50004 ssh2
2158 Apr 22 03:04:24 osboxes sshd[1653]: Connection closed by authenticating user osboxes 192.168.43.224 port 50004 [preauth]
2159 Apr 22 03:04:24 osboxes sshd[1655]: Failed password for osboxes from 192.168.43.224 port 50006 ssh2
2160 Apr 22 03:04:24 osboxes sshd[1655]: Connection closed by authenticating user osboxes 192.168.43.224 port 50006 [preauth]
2161 Apr 22 03:04:25 osboxes sshd[1658]: Failed password for invalid user osboxes.org from 192.168.43.224 port 50008 ssh2
2162 Apr 22 03:04:25 osboxes sshd[1658]: Connection closed by invalid user osboxes.org 192.168.43.224 port 50008 [preauth]
2163 Apr 22 03:04:25 osboxes sshd[1661]: Failed password for invalid user osboxes.org from 192.168.43.224 port 50010 ssh2
2164 Apr 22 03:04:25 osboxes sshd[1661]: Connection closed by invalid user osboxes.org 192.168.43.224 port 50010 [preauth]
2165 Apr 22 03:04:25 osboxes sshd[1663]: Failed password for invalid user osboxes.org from 192.168.43.224 port 50014 ssh2
2166 Apr 22 03:04:25 osboxes sshd[1662]: Failed password for invalid user osboxes.org from 192.168.43.224 port 50011 ssh2
2167 Apr 22 03:04:25 osboxes sshd[1663]: Connection closed by invalid user osboxes.org 192.168.43.224 port 50014 [preauth]
2168 Apr 22 03:04:25 osboxes sshd[1666]: Failed password for invalid user user1 from 192.168.43.224 port 50018 ssh2
2169 Apr 22 03:04:25 osboxes sshd[1662]: Connection closed by invalid user osboxes.org 192.168.43.224 port 50011 [preauth]
2170 Apr 22 03:04:25 osboxes sshd[1666]: Connection closed by invalid user user1 192.168.43.224 port 50018 [preauth]
2171 Apr 22 03:04:25 osboxes sshd[1664]: Failed password for invalid user administrator from 192.168.43.224 port 50015 ssh2
2172 Apr 22 03:04:25 osboxes sshd[1665]: Failed password for invalid user administrator from 192.168.43.224 port 50017 ssh2
2173 Apr 22 03:04:25 osboxes sshd[1664]: Connection closed by invalid user administrator 192.168.43.224 port 50015 [preauth]
2174 Apr 22 03:04:25 osboxes sshd[1665]: Connection closed by invalid user administrator 192.168.43.224 port 50017 [preauth]
```

Menganalisis log menggunakan astro grep

Untuk menganalisis log, pada lab ini menggunakan tools yang bernama astro grep. Dengan tools astro grep dapat membantu mencari log dari brute-force/dictionary attack. Mulai dari ip penyerang sampai waktu dari penyerang untuk mencoba login.

D. Remediation

- Memblok ip yang dianggap berbahaya

```
C:~ Select root@osboxes: ~
```

```
root@osboxes:~# sudo ufw deny from 192.168.43.224 to any
Rules updated
```

Konfigurasi UFW untuk memblock ip penyerang

```
root@osboxes:~# sudo ufw status
Status: active
```

To	Action	From
--	-----	----
22/tcp	ALLOW	Anywhere
Anywhere	DENY	192.168.43.224
22/tcp (v6)	ALLOW	Anywhere (v6)

Pada lab ini, untuk memblokir alamat IP penyerang menggunakan ufw. Ufw sendiri adalah firewall bawaan dari sistem operasi ubuntu. Sehingga tidak perlu install, hanya perlu untuk mengkonfigurasikannya.

- Mengimplementasikan update pada sistem operasi

```
osboxes@osboxes:~$ sudo apt-get dist-upgrade
[sudo] password for osboxes:
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
The following NEW packages will be installed:
```

Dengan menggunakan perintah `sudo apt-get dist-upgrade` untuk mengupdate sistem operasi pada sistem operasi ubuntu. Update sistem operasi tersebut di update ke versi ubuntu yang lebih aman, sehingga minim sekali kerentanannya.

- Mengimplementasikan pembatasan login gagal pada ssh menggunakan fail2ban

```

root@osboxes: /etc/fail2ban
GNU nano 2.9.3

#[DEFAULT]
#ignoreip = 127.0.0.1/8
#ignorecommand =
#bantime = 23600
#findtime = 100
#maxretry = 2
#enabled = false

[sshd]
enabled = true
port = 22
#action = iptables-multiport[name="bannedssh", port="80,443,22,48"]
logpath = /var/log/auth.log
maxretry = 3
bantime = 5m

```

Mengkonfigurasi Fail2ban

Pertama kami menginstal terlebih dahulu fail2ban pada server ubuntu. Kemudian kami membuat file jail.local. file tersebut berisi aturan, jika terjadi kesalahan pada proses login jika lebih dari 3 kali, maka koneksi nya akan diputus selama 5 menit.

- Menkonfigurasi permission pada file /usr/bin/pkexec

```

osboxes@osboxes: ~/proof
osboxes@osboxes:~$ sudo chmod 0755 /usr/bin/pkexec
[sudo] password for osboxes:
osboxes@osboxes:~$ ls
auth.log  berdav      Desktop    Downloads  examples.desktop  Pictures  Public
auth.log.1 CVE-2021-4034 Documents  eicar.com  Music          proof     Templates
osboxes@osboxes:~$ cd proof
osboxes@osboxes:~/proof$ ./expl.sh
Glib: Cannot convert message: Could not open converter from "UTF-8" to "banana"
pkexec must be setuid root

```

Konfigurasi permission pkexec

Untuk mencegah terjadinya local privilege escalation, salah satu caranya adalah mengkonfigurasi permission pada file /usr/bin/pkexec pada server ubuntu.

E. Post Incident


- Membuat laporan tentang penyebab, akibat, dan tindakan yang dilakukan untuk memitigasi sebuah incident.

4.2. Port Scanning

Menurut techtarget.com tidak mungkin untuk mencegah tindakan port scanning. Karena siapapun dapat memilih alamat ip dan memindai port yang terbuka. Untuk melindungi jaringan, tim it harus mencari tahu apa port yang akan ditemukan penyerang selama port scanning.

Maka dari itu, pada lab ini kami mencoba untuk mengamankan port yang terbuka. Pada lab ini port yang terbuka adalah port SSH. Dengan menginstall fail2ban dapat mencegah dari serangan brute-force/dictionary attack. Dengan menginstall fail2ban, jika ada kegagalan sebanyak 3 kali dalam melakukan login, maka ip tersebut akan di ban selama 5 menit. Jadi tidak bisa melakukan login SSH kembali, harus menunggu 5 menit.

4.3. Terjadinya Dictionary Attack Pada Ssh Login

 Command Prompt

```
C:\Users\ASUS>ssh osboxes@192.168.43.19
osboxes@192.168.43.19's password:
Permission denied, please try again.
osboxes@192.168.43.19's password:
Permission denied, please try again.
osboxes@192.168.43.19's password:
ssh_dispatch_run_fatal: Connection to 192.168.43.19 port 22: Connection timed out

C:\Users\ASUS>ssh osboxes@192.168.43.19
ssh: connect to host 192.168.43.19 port 22: Connection timed out
```

Hasil dari implementasi fail2ban

Pada lab ini, setelah terjadi serangan brute-force/dictionary attack, kami mengkonfigurasi tool yang bernama FAIL2BAN. Tool ini digunakan untuk mencegah brute-force/dictionary attack terhadap layanan SSH. Fail2ban bekerja ketika ada yang mencoba login, tetapi proses login tersebut gagal dalam 3 kali percobaan. Maka, koneksi yang terjadi antara SSH server dan SSH client akan diputus oleh fail2ban.

Untuk melindungi server SSH, maka lakukan langkah-langkah sebagai berikut.

- Nonaktifkan akses root jika diperlukan

Menonaktifkan akses root SSH adalah upaya untuk melindungi sistem anda. User root adalah user dengan privilege tertinggi. Jadi anda harus benar-benar menjaganya.

- Nonaktifkan layanan yang tidak digunakan
Jika layanan SSH tidak digunakan, maka sebaiknya layanan tersebut dinonaktifkan. Bisa saja layanan yang tidak digunakan bisa menjadi ancaman, vulnerability atau bahkan jalan masuk penyerang ke sistem anda. Inju juga berlaku pada layanan lain yang tidak digunakan.
- Filter lalu lintas ke ssh server
Anda juga bisa melindungi server SSH dengan membatasi akses ke alamat ip server SSH. Selain itu, bisa menggunakan firewall berbasis jaringan atau host.
- Jalankan SSH pada port non-standar
Hal ini akan mengurangi port scanning untuk server SSH pada port default.
- Menggunakan kata sandi yang kuat
Menggunakan kata sandi yang kuat akan meningkatkan keamanan sistem dari serangan brute-force atau dictionary attack. Misalnya, menggunakan kata sandi yang terdiri dari 8 karakter yang isinya huruf kapital, huruf kecil, angka, simbol unik.

4.4. Privilege Escalation

CVE2021-4034 di ubuntu dapat dicegah dengan melakukan update server atau sistem yang telah dikeluarkan oleh vendor untuk perbaikan OS. Misalnya, ubuntu telah menyediakan update untuk mengatasi kerentanan PolicyKit pada ubuntu versi 18.04, 20.04 dan 21.04.

Selanjutnya anda dapat membuat daftar semua packages yang telah memenuhi syarat untuk di upgrade yang berkaitan dengan eksploitasi Pwnkit. Berikut ini adalah daftarnya:

- gir1.2-polkit-1.0: GObject introspection data for PolicyKit
- libpolkit-agent-1-0: PolicyKit Authentication Agent API
- libpolkit-agent-1-0-dbgsym: debug symbols for libpolkit-agent-1-0
- libpolkit-agent-1-dev: PolicyKit Authentication Agent API - development files
- libpolkit-gobject-1-0: PolicyKit Authorization API
- libpolkit-gobject-1-0-dbgsym: debug symbols for libpolkit-gobject-1-0
- libpolkit-gobject-1-dev: PolicyKit Authorization API - development files

- policykit-1: framework for managing administrative policies and privileges
- policykit-1-dbgsym: debug symbols for policykit-1
- policykit-1-doc: documentation for PolicyKit-1

Jika tidak ada patch yang tersedia untuk sistem operasi tertentu. Maka hapus bit SUID dari pkexec sebagai mitigasi sementara. Dengan menjalankan perintah :

```
# chmod 0755 /usr/bin/pkexec
```

```
osboxes@osboxes: ~/proof
osboxes@osboxes:~$ sudo chmod 0755 /usr/bin/pkexec
[sudo] password for osboxes:
osboxes@osboxes:~$ ls
auth.log  berdav  Desktop  Downloads  examples.desktop  Pictures  Public  tes.txt
auth.log.1  CVE-2021-4034  Documents  eicar.com  Music  proof  Templates  Videos
osboxes@osboxes:~$ cd proof
osboxes@osboxes:~/proof$ ./expl.sh
Glib: Cannot convert message: Could not open converter from "UTF-8" to "banana"
pkexec must be setuid root
osboxes@osboxes:~/proof$
```

Konfigurasi permission pkexec

4.5. Mencegah suspicious file pada server

Yang terpenting anda harus menginstall antivirus pada server. Pada lab ini juga, terdapat wazuh agent yang terdapat di server ubuntu 18.04. Wazuh tersebut di integrasikan dengan virustotal. Sehingga jika ada malicious file ditemukan, maka akan ada peringatan di wazuh-manager. Anda jangan pernah untuk menjalankan file tersebut. Anda harus menghapus file tersebut.

59

/ 66

File distributed by Open Source

275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f

68.00 B

2022-04-25 06:05:38 UTC

eicar.com-38037

attachment

known-distributor

text

via-tor

Community Score

Community Score

Community Score

Community Score

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY 40+

Crowdsourced YARA Rules

Matches rule **SUSP_Just_EICAR** by Florian Roth from ruleset gen_suspicious_strings at <https://github.com/Neo23x0/signature-base>

↳ Just an EICAR test file - this is boring but users asked for it

Matches rule **malw_eicar** by Marc Rivero | McAfee ATR Team from ruleset MALW_Eicar at <https://github.com/advanced-threat-research/Yara-Rules>

Virustotal mendeteksi suspicious file

Selain itu, pada lab kami juga bisa mengetahui nilai hash pada file tersebut. Seperti dibawah ini terdapat nilai hash, tipe file, ukuran file, dan lain-lain.

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY 40+

Basic Properties

MD5

44d88612fea8a8f36de82e1278abb02f

SHA-1

3395856ce81f2b7382dee72602f798b642f14140

SHA-256

275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f

SSDEEP

3:a+JraNvsgzsVqSwHq9:tJuOgzsko

TLSH

T141A022003B0EEE2BA20B00200032E8B00808020E2CE00A3820A020B8C83308803EC228

File type

Text

Magic

ASCII text, with no line terminators

TrID

EICAR antivirus test file (100%)


File size

68.00 B (68 bytes)

Nilai hash pada file yang diduga malware

lab ini juga bisa mengetahui proses yang dijalankan oleh malware tersebut dengan data yang ada di virustotal. Mulai dari sistem operasi windows sampai linux.

DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 40+

 Lastline

Process And Service Actions ⓘ

Processes Created

C:\WINDOWS\system32\ntvdm.exe
/bin/bash

Shell Commands

C:\WINDOWS\system32\ntvdm.exe -f -i1
/bin/bash /private/tmp/eicar.com.sh

Proses yang dijalankan oleh malware tersebut

Untuk mencegah adalah suspicious file pada server, pastikan untuk tidak mendownload file dari website-website tidak resmi atau tidak dipercaya. Karena, biasanya website-website tersebut secara keamanan itu rendah. Jadi pastikan anda tidak mendownload file dari website yang tidak resmi atau dipercaya.

Selain itu, file file tersebut juga bisa datang dari email yang tidak dikenal. Sehingga, jika ada email dari seseorang yang tidak diketahui, anda harus berhati-hati dan tidak sembarangan untuk mengklik atau mendownload file yang terdapat pada email tersebut.

5. REFERENCE

Kingatua, A. (2022, 03 9). *Privilege Escalation Attacks, Prevention Techniques and Tools*. Retrieved from geekflare.com: <https://geekflare.com/privilege-escalation-attacks/>

Lewis, M. C. (n.d.). *What are port scan attacks and how can they be prevented?* Retrieved from [www.techtarget.com](https://www.techtarget.com/searchsecurity/answer/What-is-a-port-scan-attack#:~:text=It%20is%20impossible%20to%20prevent,by%20running%20their%20own%20scan.):
<https://www.techtarget.com/searchsecurity/answer/What-is-a-port-scan-attack#:~:text=It%20is%20impossible%20to%20prevent,by%20running%20their%20own%20scan.>

mebeim/CVE-2021-4034. (2022, 1 26). Retrieved from github:
<https://github.com/mebeim/CVE-2021-4034>

Orsi, A. I. (2022 , March 02). *Detecting PwnKit (CVE-2021-4034) with Wazuh*. Retrieved from WAZUH BLOG: <https://wazuh.com/blog/detecting-pwnkit-cve-2021-4034-with-wazuh/>

Rapid7. (n.d.). *Rapid7*. Retrieved from Brute-Force and Dictionary Attacks:
<https://www.rapid7.com/fundamentals/brute-force-and-dictionary-attacks/>

redhat. (2022, 1 26). *CVE-2021-4034*. Retrieved from acces redhat:
<https://access.redhat.com/security/cve/cve-2021-4034>

University, C. M. (n.d.). *Protect Against Brute-force/Dictionary SSH Attacks*. Retrieved from Carnegie Mellon University: https://www.cmu.edu/iso/aware/be-aware/brute-force_ssh_attack.html