Network Intrusion Detection System (NIDS)

Project Overview

In this project, I will set up a NIDS using Security Onion deployed in VMware Workstation Pro. To test it, I will perform a few attacks on a vulnerable machine, Metasploitable, using Kali Linux. Security Onion will monitor the traffic between the virtual machines and is expected to generate alerts if any intrusions occur.

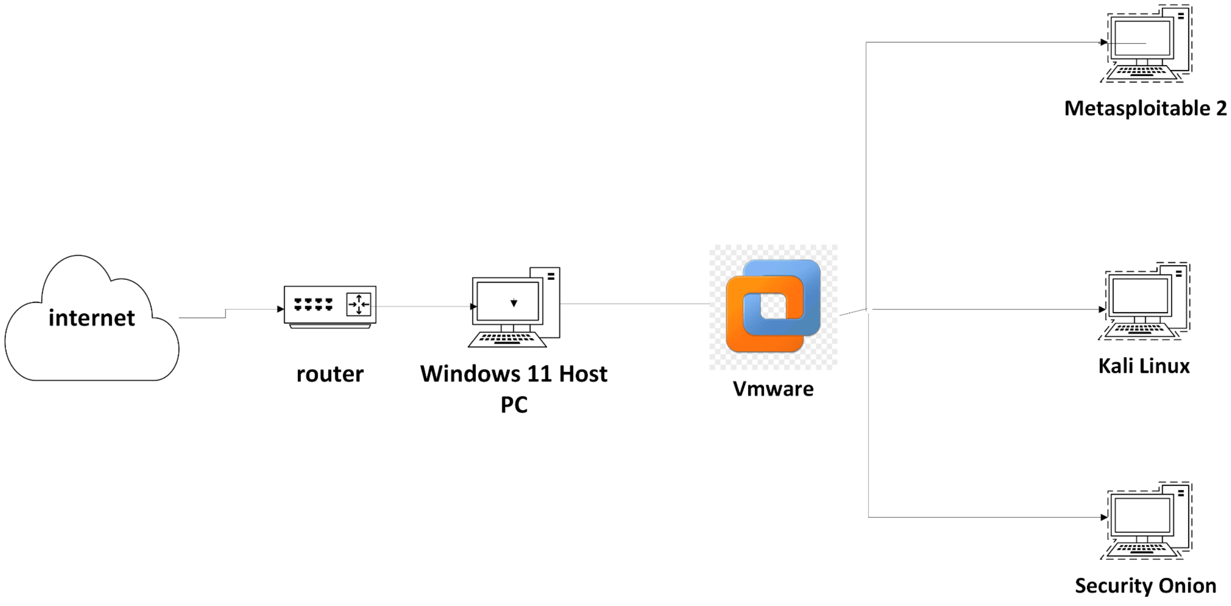
Objectives

- Configure a secure lab environment.
- Deploy Security Onion for intrusion detection.
- Simulate attacks using Kali Linux on Metasploitable.
- Monitor and analyze intrusion alerts.

Project Components

- **Security Onion**: NIDS deployment and monitoring.
- **Kali Linux**: Attack simulation tools (e.g. Nmap, Hydra).
- **Metasploitable**: Vulnerable target machine.

Network Setup



Project Setup

Security Onion requires two network interfaces for proper setup: one for management, configured on NAT with an IP address to access the web interface, and another for sniffing, configured on Host-Only without an IP address. To enable Security Onion to sniff and monitor traffic effectively, other virtual machines must also use the Host-Only network. For example, Kali Linux should have two network interfaces—one on NAT (optional) and the other on Host-Only—while Metasploitable should be set to Host-Only.

IP Configurations:

- **Security Onion**: 192.168.19.140 on NAT
- **Kali Linux**: 192.168.128.19 on NAT, 192.168.189.130 on Host-Only
- **Metasploitable**: 192.168.189.129 on Host-Only

VMware Workstation Pro was used to host the virtual machines.

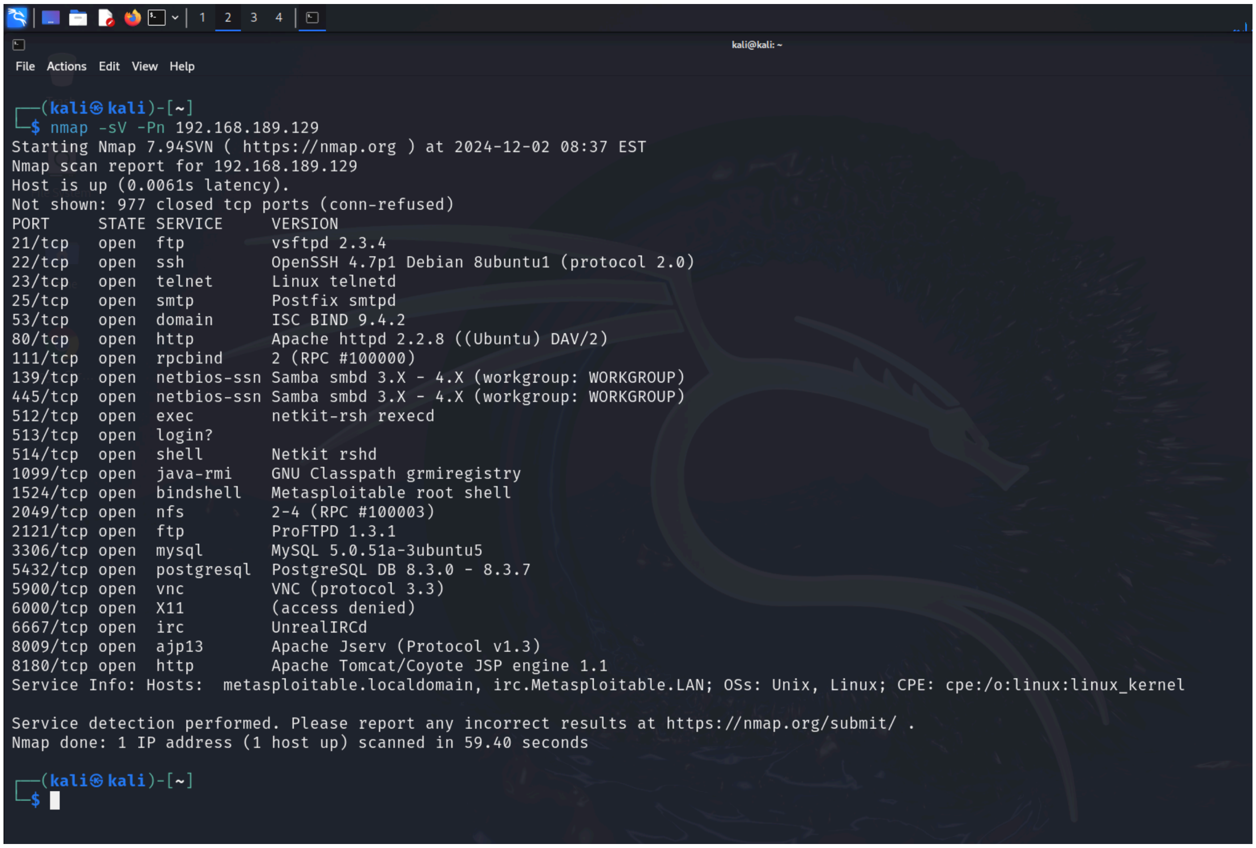
Security Onion Console (SOC)

- Kali Linux Screenshot
- Kali Linux Screenshot 2

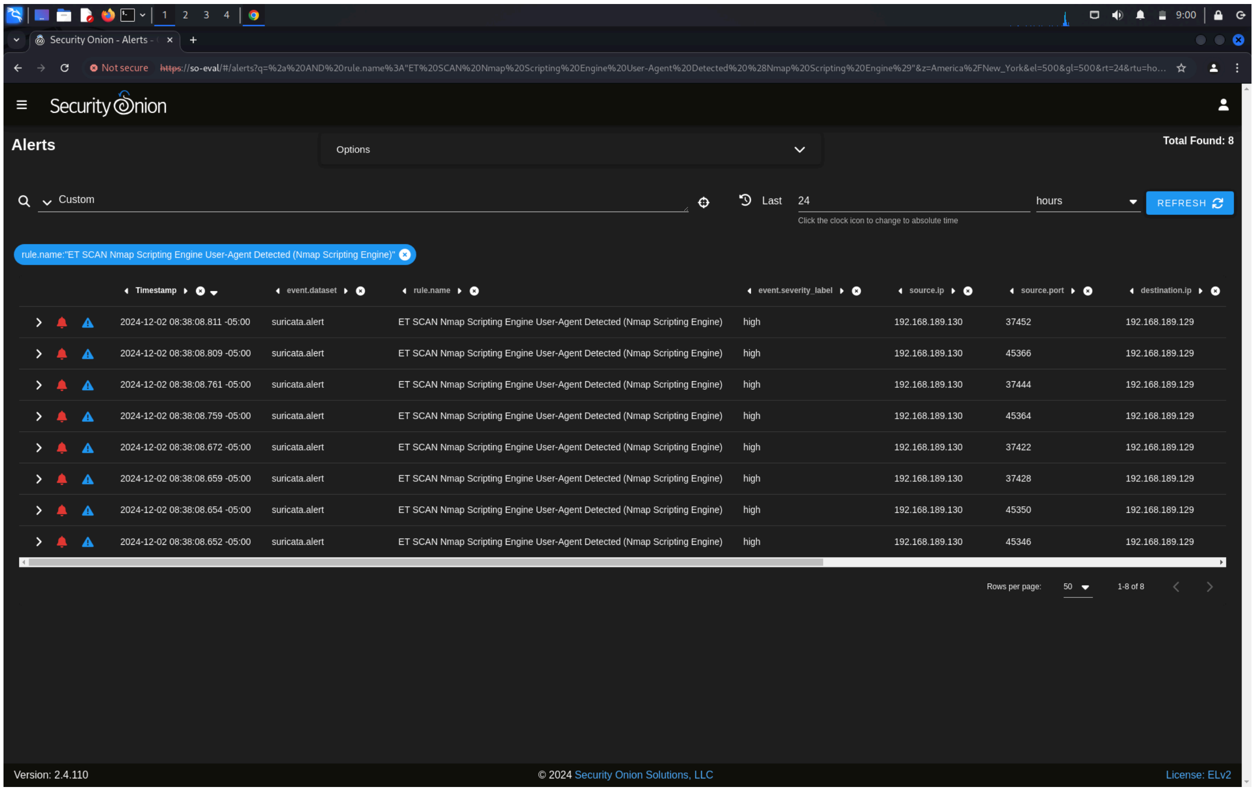
Testing/Attack

Nmap Scanning

- **Experiment**: I've performed a network scan using Nmap to identify open ports and services on the Metasploitable machine.
- **Results**: The Nmap scan successfully identified several open ports and services, and Security Onion detected the scan activity and generated alerts.

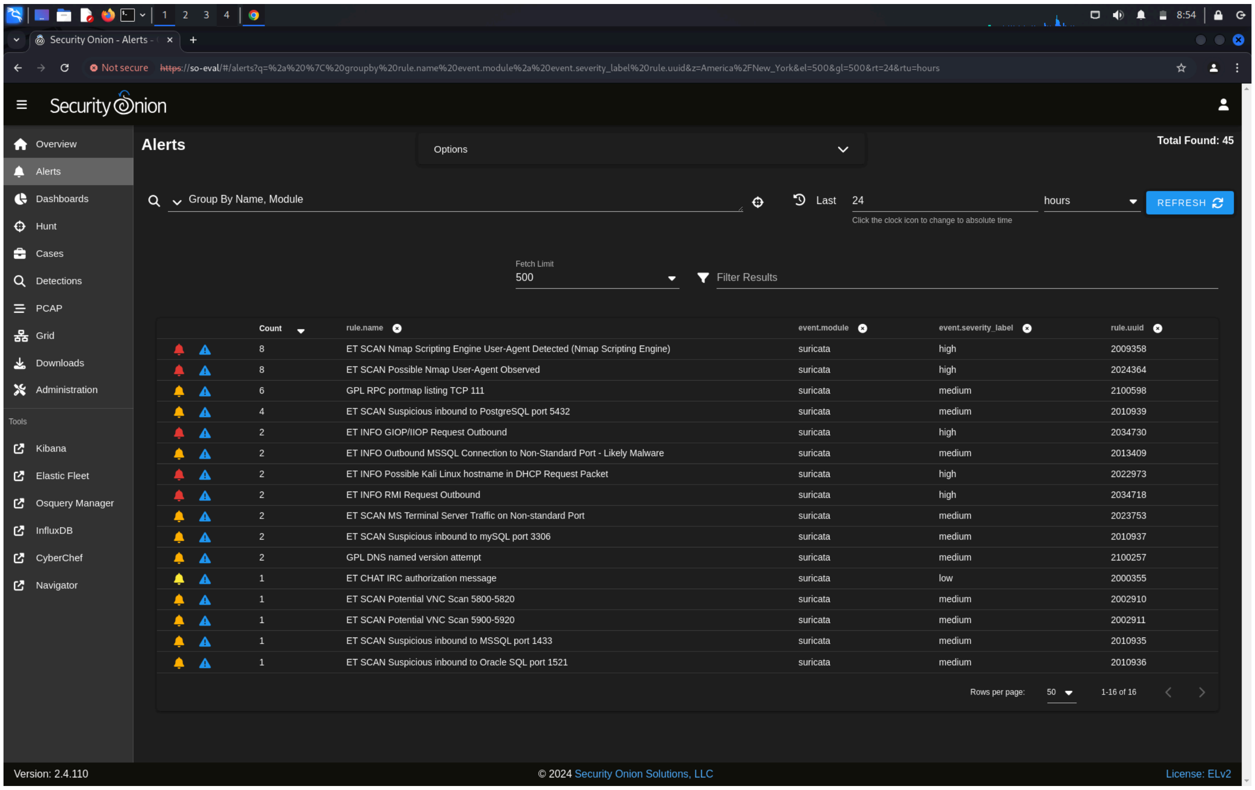


```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -Pn 192.168.189.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-02 08:37 EST
Nmap scan report for 192.168.189.129
Host is up (0.0061s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 59.40 seconds

┌──(kali㉿kali)-[~]
└─$ 
```



1 2 3 4
9:00
Security Onion - Alerts -
Not secure
https://so-eval/#/alerts?q=%2a%20AND%20rule.name%3A"ET%20SCAN%20Nmap%20Scripting%20Engine%20User-Agent%20Detected%20%28Nmap%20Scripting%20Engine%29"&z=America%2FNew_York&el=500&gl=500&rt=24&rtu=ho...
Security Onion
Alerts
Options
Total Found: 8
Custom
Last
24
hours
REFRESH
Click the clock icon to change to absolute time
rule.name:"ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)"

Timestamp	event.dataset	rule.name	event.severity_label	source.ip	source.port	destination.ip
2024-12-02 08:38:08.811 -05:00	suricata.alert	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	high	192.168.189.130	37452	192.168.189.129
2024-12-02 08:38:08.809 -05:00	suricata.alert	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	high	192.168.189.130	45366	192.168.189.129
2024-12-02 08:38:08.761 -05:00	suricata.alert	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	high	192.168.189.130	37444	192.168.189.129
2024-12-02 08:38:08.759 -05:00	suricata.alert	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	high	192.168.189.130	45364	192.168.189.129
2024-12-02 08:38:08.672 -05:00	suricata.alert	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	high	192.168.189.130	37422	192.168.189.129
2024-12-02 08:38:08.659 -05:00	suricata.alert	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	high	192.168.189.130	37428	192.168.189.129
2024-12-02 08:38:08.654 -05:00	suricata.alert	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	high	192.168.189.130	45350	192.168.189.129
2024-12-02 08:38:08.652 -05:00	suricata.alert	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	high	192.168.189.130	45346	192.168.189.129



https://so-eval/#/alerts?q=%2a%20%7C%20groupby%20rule.name%20event.module%2a%20event.severity_label%20rule.uuid&z=America%2FNew_York&el=500&gl=500&rt=24&rtu=hours

Alerts

Total Found: 45

Group By Name, Module

Last 24 hours

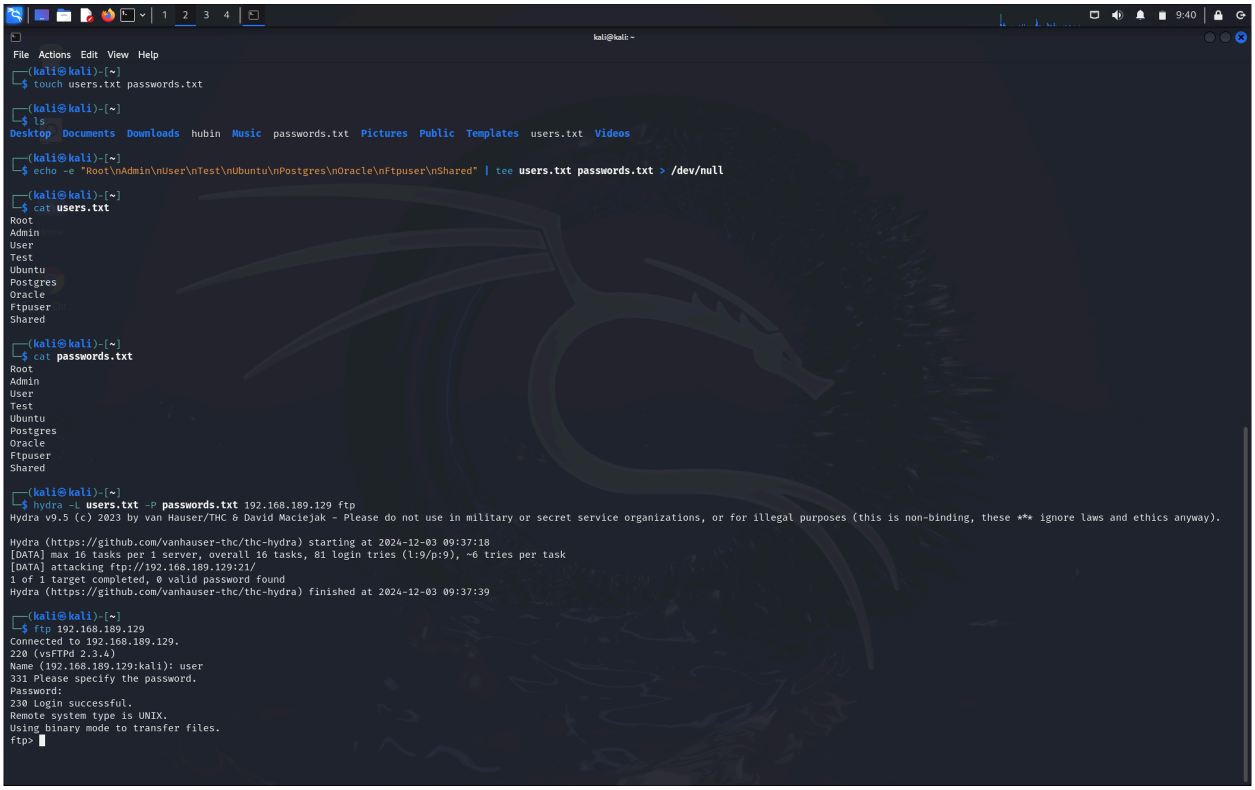
Fetch Limit 500

Count	rule.name	event.module	event.severity_label	rule.uuid
8	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	suricata	high	2009358
8	ET SCAN Possible Nmap User-Agent Observed	suricata	high	2024364
6	GPL RPC portmap listing TCP 111	suricata	medium	2100598
4	ET SCAN Suspicious inbound to PostgreSQL port 5432	suricata	medium	2010939
2	ET INFO GIOP/IIOP Request Outbound	suricata	high	2034730
2	ET INFO Outbound MSSQL Connection to Non-Standard Port - Likely Malware	suricata	medium	2013409
2	ET INFO Possible Kali Linux hostname in DHCP Request Packet	suricata	high	2022973
2	ET INFO RMI Request Outbound	suricata	high	2034718
2	ET SCAN MS Terminal Server Traffic on Non-standard Port	suricata	medium	2023753
2	ET SCAN Suspicious inbound to mySQL port 3306	suricata	medium	2010937
2	GPL DNS named version attempt	suricata	medium	2100257
1	ET CHAT IRC authorization message	suricata	low	2000355
1	ET SCAN Potential VNC Scan 5800-5820	suricata	medium	2002910
1	ET SCAN Potential VNC Scan 5900-5920	suricata	medium	2002911
1	ET SCAN Suspicious inbound to MSSQL port 1433	suricata	medium	2010935
1	ET SCAN Suspicious inbound to Oracle SQL port 1521	suricata	medium	2010936

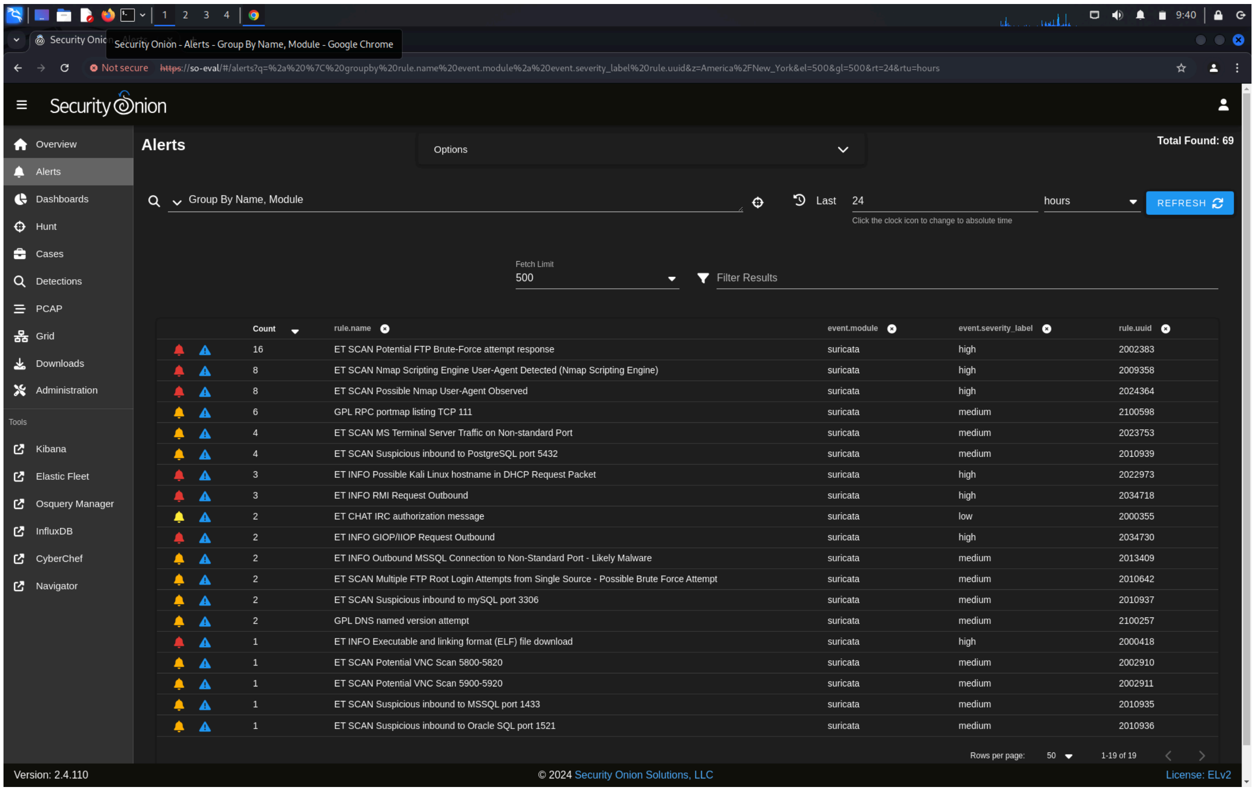
Rows per page: 50 1-16 of 16

Brute Force Attack

- **Experiment**: I've performed a brute force attack on an FTP service running on Metasploitable using Hydra.
- **Results**:I successfully exploited the FTP service by conducting a brute force attack. Security Onion detected the intrusion and generated corresponding alerts.



```
┌──(kali㉿kali)-[~]
└─$ touch users.txt passwords.txt

┌──(kali㉿kali)-[~]
└─$ ls
Desktop  Documents  Downloads  hubin  Music  passwords.txt  Pictures  Public  Templates  users.txt  Videos

┌──(kali㉿kali)-[~]
└─$ echo -e "Root\nAdmin\nUser\nTest\nUbuntu\nPostgres\nOracle\nFtpuser\nShared" | tee users.txt passwords.txt > /dev/null

┌──(kali㉿kali)-[~]
└─$ cat users.txt
Root
Admin
User
Test
Ubuntu
Postgres
Oracle
Ftpuser
Shared

┌──(kali㉿kali)-[~]
└─$ cat passwords.txt
Root
Admin
User
Test
Ubuntu
Postgres
Oracle
Ftpuser
Shared

┌──(kali㉿kali)-[~]
└─$ hydra -L users.txt -P passwords.txt 192.168.189.129 ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-03 09:37:18
[DATA] max 16 tasks per 1 server, overall 16 tasks, 81 login tries (l:9/p:9), ~6 tries per task
[DATA] attacking ftp://192.168.189.129:21/
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-12-03 09:37:39

┌──(kali㉿kali)-[~]
└─$ ftp 192.168.189.129
Connected to 192.168.189.129.
220 (vsFTPd 2.3.4)
Name (192.168.189.129:kali): user
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> 
```



Security Onion - Alerts - Group By Name, Module - Google Chrome
Not secure
https://so-eval/#/alerts?q=%2a%20%7C%20groupby%20rule.name%20event.module%2a%20event.severity_label%20rule.uuid&z=America%2FNew_York&el=500&gl=500&rt=24&rtu=hours
Security Onion
Overview
Alerts
Dashboards
Hunt
Cases
Detections
PCAP
Grid
Downloads
Administration
Tools
Kibana
Elastic Fleet
Osquery Manager
InfluxDB
CyberChef
Navigator
Options
REFRESH
Click the clock icon to change to absolute time

Alerts

Total Found: 69

Group By Name, Module

Last 24 hours

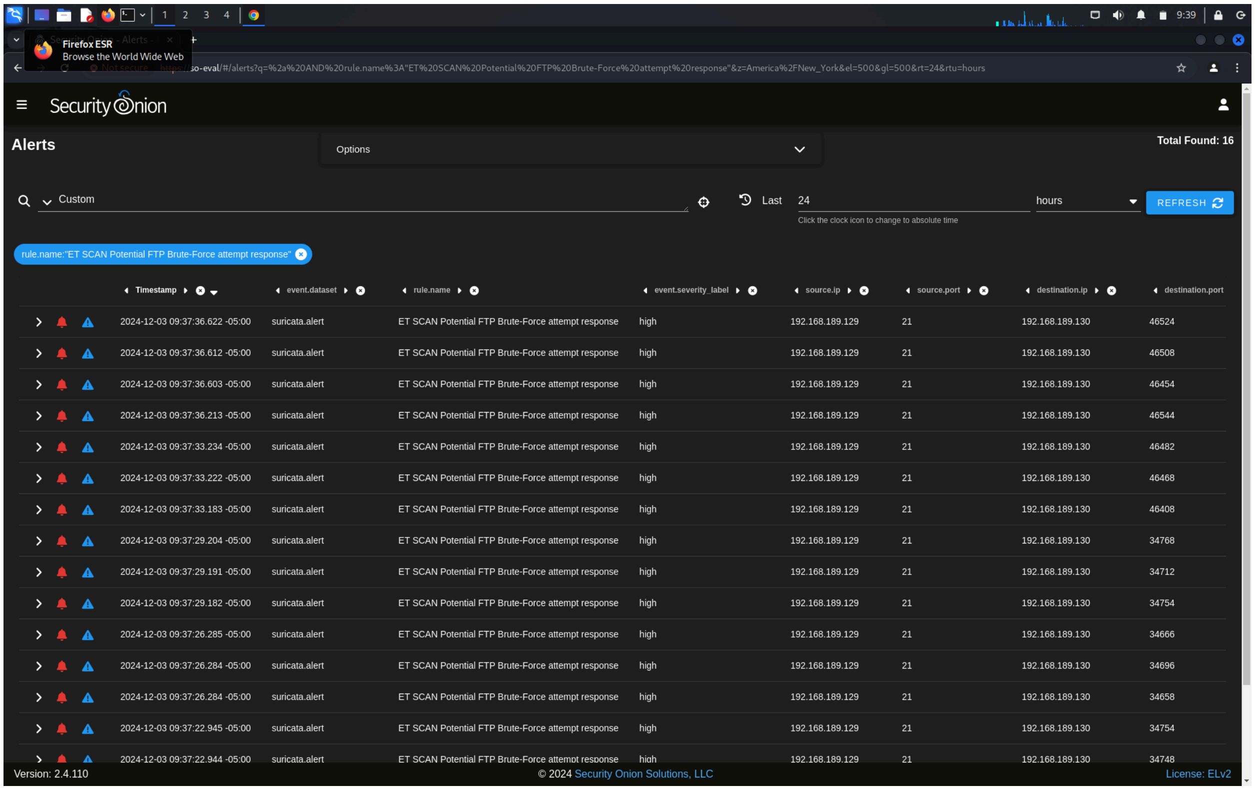
Fetch Limit 500

Filter Results

Count	rule.name	event.module	event.severity_label	rule.uuid
16	ET SCAN Potential FTP Brute-Force attempt response	suricata	high	2002383
8	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	suricata	high	2009358
8	ET SCAN Possible Nmap User-Agent Observed	suricata	high	2024364
6	GPL RPC portmap listing TCP 111	suricata	medium	2100598
4	ET SCAN MS Terminal Server Traffic on Non-standard Port	suricata	medium	2023753
4	ET SCAN Suspicious inbound to PostgreSQL port 5432	suricata	medium	2010939
3	ET INFO Possible Kali Linux hostname in DHCP Request Packet	suricata	high	2022973
3	ET INFO RMI Request Outbound	suricata	high	2034718
2	ET CHAT IRC authorization message	suricata	low	2000355
2	ET INFO GIOP/IIOP Request Outbound	suricata	high	2034730
2	ET INFO Outbound MSSQL Connection to Non-Standard Port - Likely Malware	suricata	medium	2013409
2	ET SCAN Multiple FTP Root Login Attempts from Single Source - Possible Brute Force Attempt	suricata	medium	2010642
2	ET SCAN Suspicious inbound to mySQL port 3306	suricata	medium	2010937
2	GPL DNS named version attempt	suricata	medium	2100257
1	ET INFO Executable and linking format (ELF) file download	suricata	high	2000418
1	ET SCAN Potential VNC Scan 5800-5820	suricata	medium	2002910
1	ET SCAN Potential VNC Scan 5900-5920	suricata	medium	2002911
1	ET SCAN Suspicious inbound to MSSQL port 1433	suricata	medium	2010935
1	ET SCAN Suspicious inbound to Oracle SQL port 1521	suricata	medium	2010936

Rows per page: 50 1-19 of 19

Version: 2.4.110 © 2024 Security Onion Solutions, LLC License: ELv2



Firefox ESR
Browse the World Wide Web
so-eval/#/alerts?q=%2a%20AND%20rule.name%3A"ET%20SCAN%20Potential%20FTP%20Brute-Force%20attempt%20response"&z=America%2FNew_York&el=500&gl=500&rt=24&rtu=hours
9:39
Security Onion
Options
Custom
Last
REFRESH

Alerts

Total Found: 16

Last 24 hours

Click the clock icon to change to absolute time

rule.name:"ET SCAN Potential FTP Brute-Force attempt response"

Timestamp	event.dataset	rule.name	event.severity_label	source.ip	source.port	destination.ip	destination.port
2024-12-03 09:37:36.622 -05:00	suricata.alert	ET SCAN Potential FTP Brute-Force attempt response	high	192.168.189.129	21	192.168.189.130	46524
2024-12-03 09:37:36.612 -05:00	suricata.alert	ET SCAN Potential FTP Brute-Force attempt response	high	192.168.189.129	21	192.168.189.130	46508
2024-12-03 09:37:36.603 -05:00	suricata.alert	ET SCAN Potential FTP Brute-Force attempt response	high	192.168.189.129	21	192.168.189.130	46454
2024-12-03 09:37:36.213 -05:00	suricata.alert	ET SCAN Potential FTP Brute-Force attempt response	high	192.168.189.129	21	192.168.189.130	46544
2024-12-03 09:37:33.234 -05:00	suricata.alert	ET SCAN Potential FTP Brute-Force attempt response	high	192.168.189.129	21	192.168.189.130	46482
2024-12-03 09:37:33.222 -05:00	suricata.alert	ET SCAN Potential FTP Brute-Force attempt response	high	192.168.189.129	21	192.168.189.130	46468
2024-12-03 09:37:33.183 -05:00	suricata.alert	ET SCAN Potential FTP Brute-Force attempt response	high	192.168.189.129	21	192.168.189.130	46408
2024-12-03 09:37:29.204 -05:00	suricata.alert	ET SCAN Potential FTP Brute-Force attempt response	high	192.168.189.129	21	192.168.189.130	34768
2024-12-03 09:37:29.191 -05:00	suricata.alert	ET SCAN Potential FTP Brute-Force attempt response	high	192.168.189.129	21	192.168.189.130	34712
2024-12-03 09:37:29.182 -05:00	suricata.alert	ET SCAN Potential FTP Brute-Force attempt response	high	192.168.189.129	21	192.168.189.130	34754
2024-12-03 09:37:26.285 -05:00	suricata.alert	ET SCAN Potential FTP Brute-Force attempt response	high	192.168.189.129	21	192.168.189.130	34666
2024-12-03 09:37:26.284 -05:00	suricata.alert	ET SCAN Potential FTP Brute-Force attempt response	high	192.168.189.129	21	192.168.189.130	34696
2024-12-03 09:37:26.284 -05:00	suricata.alert	ET SCAN Potential FTP Brute-Force attempt response	high	192.168.189.129	21	192.168.189.130	34658
2024-12-03 09:37:22.945 -05:00	suricata.alert	ET SCAN Potential FTP Brute-Force attempt response	high	192.168.189.129	21	192.168.189.130	34754
2024-12-03 09:37:22.944 -05:00	suricata.alert	ET SCAN Potential FTP Brute-Force attempt response	high	192.168.189.129	21	192.168.189.130	34748

Version: 2.4.110 © 2024 Security Onion Solutions, LLC License: ELv2

Conclusion

This project demonstrated the effectiveness of Security Onion as a NIDS for monitoring and detecting intrusions in a simulated lab environment.

References

- Security Onion Documentation