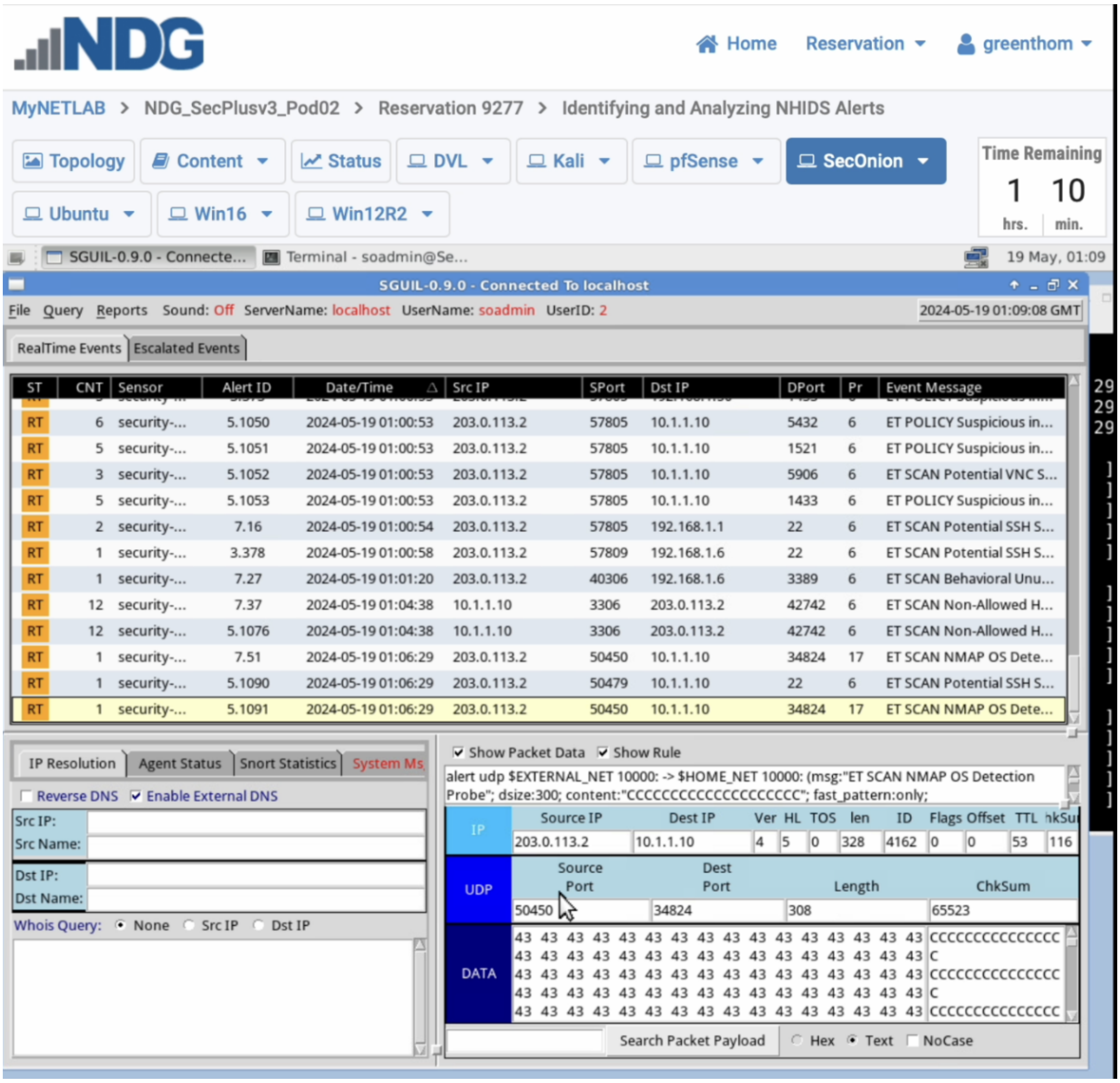
CYBR371 Lab 5

greenthom – 300536064

PART 1: IDS alerts

1. **Describe the columns in the Sguil. Do this by choosing one event log (of your choice), i.e., one row, explain the information in each column, along with the value for that example event.**



Sound: Off ServerName: localhost UserName: soadmin UserID: 2 2024-05-19 01:09:08 GMT

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	6	security-...	5.1050	2024-05-19 01:00:53	203.0.113.2	57805	10.1.1.10	5432	6	ET POLICY Suspicious in...
RT	5	security-...	5.1051	2024-05-19 01:00:53	203.0.113.2	57805	10.1.1.10	1521	6	ET POLICY Suspicious in...
RT	3	security-...	5.1052	2024-05-19 01:00:53	203.0.113.2	57805	10.1.1.10	5906	6	ET SCAN Potential VNC S...
RT	5	security-...	5.1053	2024-05-19 01:00:53	203.0.113.2	57805	10.1.1.10	1433	6	ET POLICY Suspicious in...
RT	2	security-...	7.16	2024-05-19 01:00:54	203.0.113.2	57805	192.168.1.1	22	6	ET SCAN Potential SSH S...
RT	1	security-...	3.378	2024-05-19 01:00:58	203.0.113.2	57809	192.168.1.6	22	6	ET SCAN Potential SSH S...
RT	1	security-...	7.27	2024-05-19 01:01:20	203.0.113.2	40306	192.168.1.6	3389	6	ET SCAN Behavioral Unu...
RT	12	security-...	7.37	2024-05-19 01:04:38	10.1.1.10	3306	203.0.113.2	42742	6	ET SCAN Non-Allowed H...
RT	12	security-...	5.1076	2024-05-19 01:04:38	10.1.1.10	3306	203.0.113.2	42742	6	ET SCAN Non-Allowed H...
RT	1	security-...	7.51	2024-05-19 01:06:29	203.0.113.2	50450	10.1.1.10	34824	17	ET SCAN NMAP OS Dete...
RT	1	security-...	5.1090	2024-05-19 01:06:29	203.0.113.2	50479	10.1.1.10	22	6	ET SCAN Potential SSH S...
RT	1	security-...	5.1091	2024-05-19 01:06:29	203.0.113.2	50450	10.1.1.10	34824	17	ET SCAN NMAP OS Dete...

☐ Reverse DNS ☑ Enable External DNS

Src IP:
Src Name:
Dst IP:
Dst Name:

Whois Query: ● None ○ Src IP ○ Dst IP

☑ Show Packet Data ☑ Show Rule

```
alert udp $EXTERNAL_NET 10000: -> $HOME_NET 10000: (msg:"ET SCAN NMAP OS Detection
Probe"; dsize:300; content:"CCCCCCCCCCCCCCCCCCC"; fast_pattern:only;
```

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	hkSu
	203.0.113.2	10.1.1.10	4	5	0	328	4162	0	0	53	116

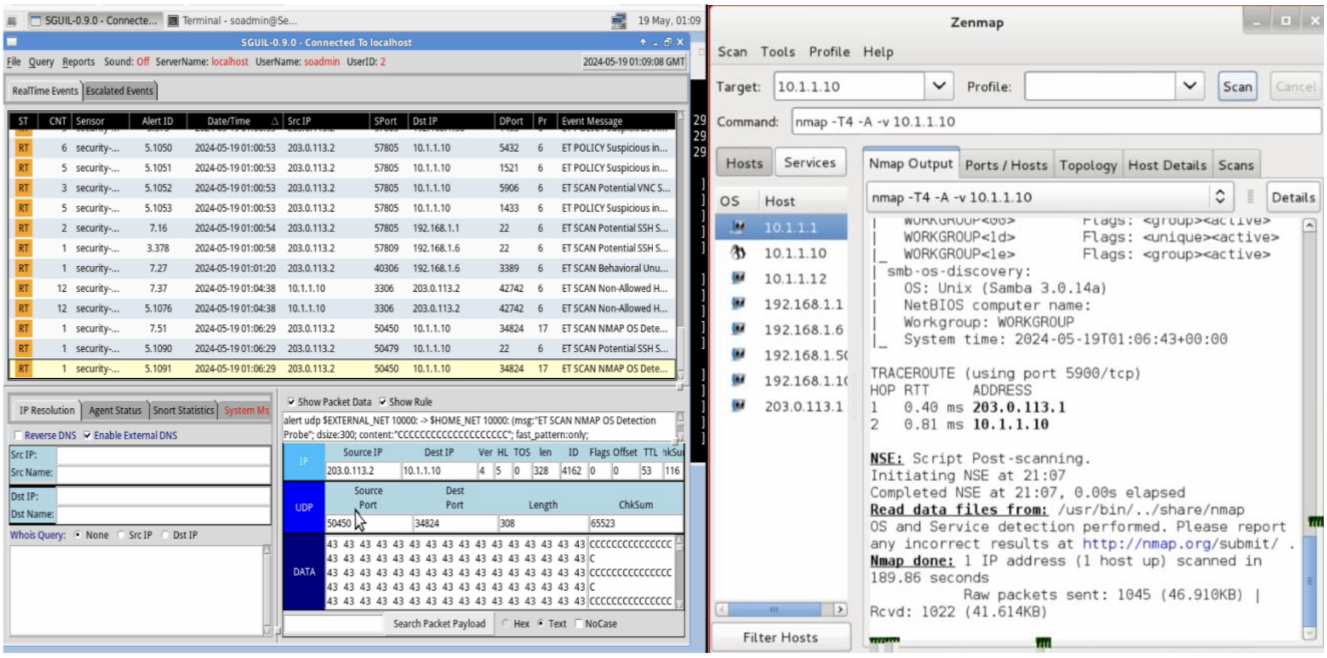
UDP	Source Port	Dest Port	Length	ChkSum
	50450	34824	308	65523

```
DATA
43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 CCCCCCCCCCCCCCCC
43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 C
43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 CCCCCCCCCCCCCCCC
43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 C
43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 CCCCCCCCCCCCCCCC
```

○ Hex ● Text ☐ NoCase

Screenshot from the lab. Shows the Sguil network security monitor. Displays various events related to network security. ST: shows the status. In this particular column, the status is RT which stands for “Real Time” -> event appeared in Sguil and is waiting for validation. CNT: shows the count/frequency of the specific event type. In this event, the count is 1 -> only appeared once. Sensor: identifies the sensor detected in the event -> sensor generating the event. In this case, the sensor is security-onion. Alert ID: event identifier to keep track of incident. This event identifier is 5.1091. Date/Time: indicates time event was detected -> 2024-05-19 01:00:58”. Src IP: is the source IP from where the event originated -> 203.0.113.2. Sport: source port from which the connection was made -> 50450. Dst IP: is the destination IP where the event was directed -> 10.1.1.10. DPort: destination port used in connection -> Pr: protocol used during the event -> 17 -> UDP. Event Message: description about nature of the event -> ET SCAN NMAP OS Detection Probe.

2. **In Sguil, choose one event of your choice, find out the rule responsible for creating that alert, then explain why that rule was triggered for that event.**


SGUIL-0.9.0 - Connecte...
Terminal - soadmin@Se...
19 May, 01:09
SGUIL-0.9.0 - Connected To localhost
File Query Reports Sound: Off ServerName: localhost UserName: soadmin UserID: 2
2024-05-19 01:09:08 GMT
RealTime Events
Escalated Events

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	6	security-...	5.1050	2024-05-19 01:00:53	203.0.113.2	57805	10.1.1.10	5432	6	ET POLICY Suspicious in...
RT	5	security-...	5.1051	2024-05-19 01:00:53	203.0.113.2	57805	10.1.1.10	1521	6	ET POLICY Suspicious in...
RT	3	security-...	5.1052	2024-05-19 01:00:53	203.0.113.2	57805	10.1.1.10	5906	6	ET SCAN Potential VNC S...
RT	5	security-...	5.1053	2024-05-19 01:00:53	203.0.113.2	57805	10.1.1.10	1433	6	ET POLICY Suspicious in...
RT	2	security-...	7.16	2024-05-19 01:00:54	203.0.113.2	57805	192.168.1.1	22	6	ET SCAN Potential SSH S...
RT	1	security-...	3.378	2024-05-19 01:00:58	203.0.113.2	57809	192.168.1.6	22	6	ET SCAN Potential SSH S...
RT	1	security-...	7.27	2024-05-19 01:01:20	203.0.113.2	40306	192.168.1.6	3389	6	ET SCAN Behavioral Unu...
RT	12	security-...	7.37	2024-05-19 01:04:38	10.1.1.10	3306	203.0.113.2	42742	6	ET SCAN Non-Allowed H...
RT	12	security-...	5.1076	2024-05-19 01:04:38	10.1.1.10	3306	203.0.113.2	42742	6	ET SCAN Non-Allowed H...
RT	1	security-...	7.51	2024-05-19 01:06:29	203.0.113.2	50450	10.1.1.10	34824	17	ET SCAN NMAP OS Dete...
RT	1	security-...	5.1090	2024-05-19 01:06:29	203.0.113.2	50479	10.1.1.10	22	6	ET SCAN Potential SSH S...
RT	1	security-...	5.1091	2024-05-19 01:06:29	203.0.113.2	50450	10.1.1.10	34824	17	ET SCAN NMAP OS Dete...

IP Resolution
Agent Status
Snort Statistics
System Ms
☐ Reverse DNS ☑ Enable External DNS
Src IP:
Src Name:
Dst IP:
Dst Name:
Whois Query: ● None ○ Src IP ○ Dst IP
☑ Show Packet Data ☑ Show Rule

```
alert udp $EXTERNAL_NET 10000: -> $HOME_NET 10000: (msg:"ET SCAN NMAP OS Detection Probe"; dsize:300; content:"CCCCCCCCCCCCCCCCCCCC"; fast_pattern:only;
```

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	hkSu
	203.0.113.2	10.1.1.10	4	5	0	328	4162	0	0	53	116

UDP	Source Port	Dest Port	Length	ChkSum
	50450	34824	308	65523

```
DATA
43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 CCCCCCCCCCCCCCC
43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 C
43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 CCCCCCCCCCCCCCC
43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 C
43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 CCCCCCCCCCCCCCC
```

Target: 10.1.1.10 Profile:

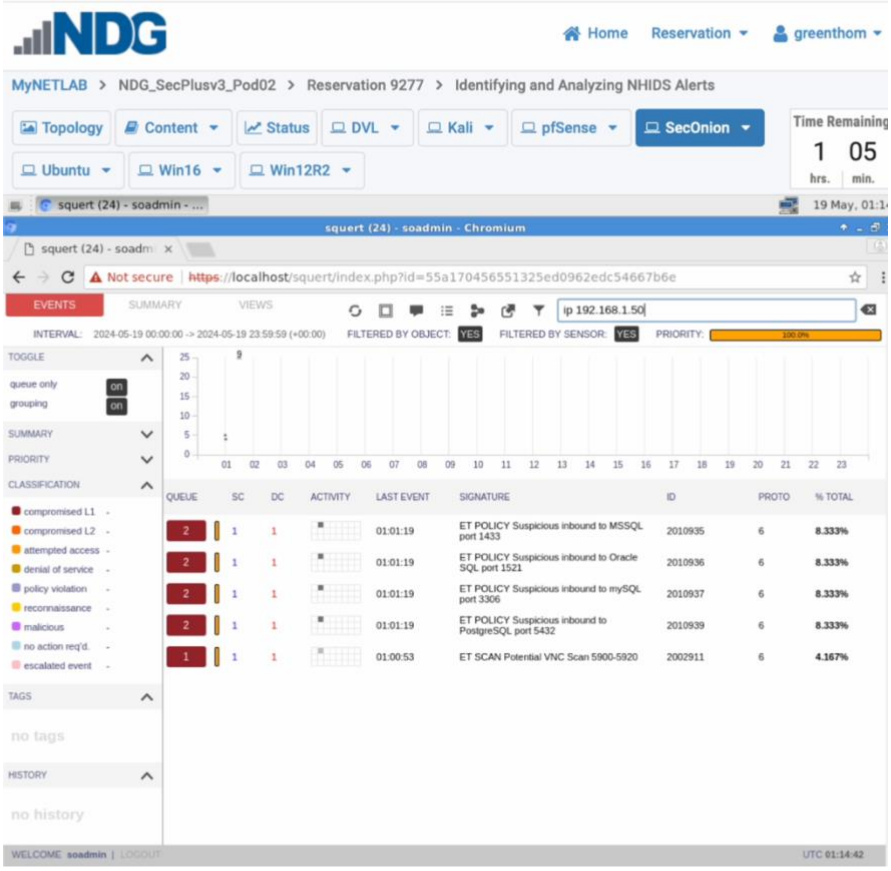
Command: nmap -T4 -A -v 10.1.1.10

OS	Host
	10.1.1.1
	10.1.1.10
	10.1.1.12
	192.168.1.1
	192.168.1.6
	192.168.1.5(
	192.168.1.1(
	203.0.113.1

```
nmap -T4 -A -v 10.1.1.10
|   WORKGROUP<00>          Flags: <group><active>
|   WORKGROUP<1d>          Flags: <unique><active>
|_  WORKGROUP<1e>          Flags: <group><active>
| smb-os-discovery:
|   OS: Unix (Samba 3.0.14a)
|   NetBIOS computer name:
|   Workgroup: WORKGROUP
|_  System time: 2024-05-19T01:06:43+00:00

TRACEROUTE (using port 5900/tcp)
HOP RTT     ADDRESS
1   0.40 ms 203.0.113.1
2   0.81 ms 10.1.1.10

NSE: Script Post-scanning.
Initiating NSE at 21:07
Completed NSE at 21:07, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report
any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in
189.86 seconds
           Raw packets sent: 1045 (46.910KB) |
Rcvd: 1022 (41.614KB)
```

Event I picked -> rule responsible for triggering the alert: ET SCAN NMAP OS Detection Probe”. Triggered by a rule designed to detect network activities typical of an OS detection probe used by Nmap. The Nmap scan used in making this event happen was through the command ‘nmap -T4 -A -v 10.1.1.10’ -> -A enables OS detection, where it attempts to determine what operating system, the target is using, detects versions of services running on open ports, traces the path packets take to target. This is targeted at 10.1.1.10 IP which the Sguil picked up. The specific packet characteristics that we captured (Show Packet Data), as well as the Zenmap, would match the pattern expected by the intrusion detection system(IDS) rule for Nmap OS detection probes. The rule was triggered because a UDP packet met the criteria of; originating from external and going for internal with src. ports being <10000+. Packet size 300 bytes (dsize), payload with string “CCCC…C”. These characteristics are an indicator of an Nmap OS detection probe which resulted in the rule and alert being triggered. By using these characteristics, identification of malicious scanning activity through IDS systems in place helps network admins secure the network.

3. **(a) Repeat the first question now with Squert. (b) Compare and contrast the kind of information that Squert provides versus Sguil. In particular, is there any information that one provides and not the other?**



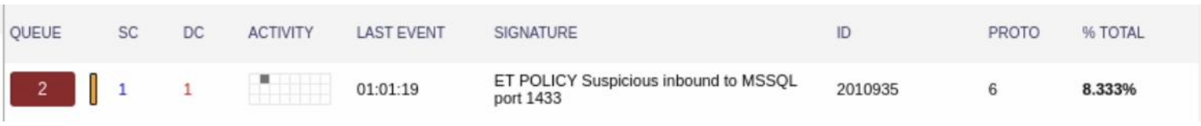
https://localhost/squert/index.php?id=55a170456551325ed0962edc54667b6e

ip 192.168.1.50

INTERVAL: 2024-05-19 00:00:00 -> 2024-05-19 23:59:59 (+00:00) FILTERED BY OBJECT: YES FILTERED BY SENSOR: YES PRIORITY: 100.0%

QUEUE	SC	DC	ACTIVITY	LAST EVENT	SIGNATURE	ID	PROTO	% TOTAL
2	1	1		01:01:19	ET POLICY Suspicious inbound to MSSQL port 1433	2010935	6	8.333%
2	1	1		01:01:19	ET POLICY Suspicious inbound to Oracle SQL port 1521	2010936	6	8.333%
2	1	1		01:01:19	ET POLICY Suspicious inbound to mySQL port 3306	2010937	6	8.333%
2	1	1		01:01:19	ET POLICY Suspicious inbound to PostgreSQL port 5432	2010939	6	8.333%
1	1	1		01:00:53	ET SCAN Potential VNC Scan 5900-5920	2002911	6	4.167%

a. Screenshot from the lab. Shows the Squert web application. Used to query and view event data stored in the Sguil database (IDS). QUEUE: refers to the number of grouped events in the queue -> 2. SC: number of distinct source IPs for the given alert -> 1. DC: number of distinct destination Ips for the given alert -> 1. ACTIVITY: number of events for a given alert on a per-hour basis -> top column above. LAST EVENT: time event last occurred -> 01:01:19. SIGNATURE: event IDS signature -> ET POLICY Suspicious inbound to MSSQL port 1433. ID: event signature ID -> 2010935. PROTO: protocol relative/recognized within/in regard to event -> 6, TCP. % TOTAL: percentage of event grouping/entire event count -> 8.333%.



QUEUE	SC	DC	ACTIVITY	LAST EVENT	SIGNATURE	ID	PROTO	% TOTAL
2	1	1		01:01:19	ET POLICY Suspicious inbound to MSSQL port 1433	2010935	6	8.333%

THOUGHT WE HAD TO REDO QUESTION TWO (JUST LEAVING IT HERE JUST IGNORE): Rule (MSSQL port 1433) looks for traffic directed at port 1433 which is the default port for Microsoft SQL. The IP address that is filtered for this event is 192.168.1.50 which does not run MSSQL, so the presence of traffic directed at this port on Ubuntu can be flagged as suspicious because it is unusual and potentially indicates an attempt to probe network services that might be misconfigured or incorrectly reported. The rule may have been triggered due to characteristics of the inbound traffic that may match malicious scanning. The Ubuntu VM, located behind the pfSense firewall on the internal network (192.168.1.0) suggests that this traffic passed through network security measures and was still deemed suspicious.

b. **Compare and contrast the kind of information that Squert provides versus Sguil. In particular, is there any information that one provides and not the other?**

SGUIL specializes in real-time data monitoring for immediate response capabilities which is vital for detecting and mitigating security incidents effectively. SGUIL also shows the alerts for the attacks by providing investigation tools for deep analysis which allows security admins to investigate packet captures as well as session data which helps in examining potential threats as they occur.

SQUERT prioritises its UI as well as reviewing historical data which helps users who do not have extensive technical expertise to understand data. SQUERT uses metadata and time series representations to help provide further context to each event. Its interface and visualization of data make it easier for non-technical users to understand complex security information. Analysis of historical data also enables users to identify long-term patterns and trends in the system.

PART 2: IDS evasion

4. **There are 3 IDS evasion techniques presented in this lab:**
   - **Low MTU Scan**
   - **Decoy Scan**
   - **Spoofed MAC scan**

a. **Provide the nmap command that corresponds to the first technique(low MTU scan – hint: remember what happens to packets that are bigger in size than the MTU! – Describe the command in simple words (what does it do). Finally, explain in simple terms how this achieves the IDS evasion.**

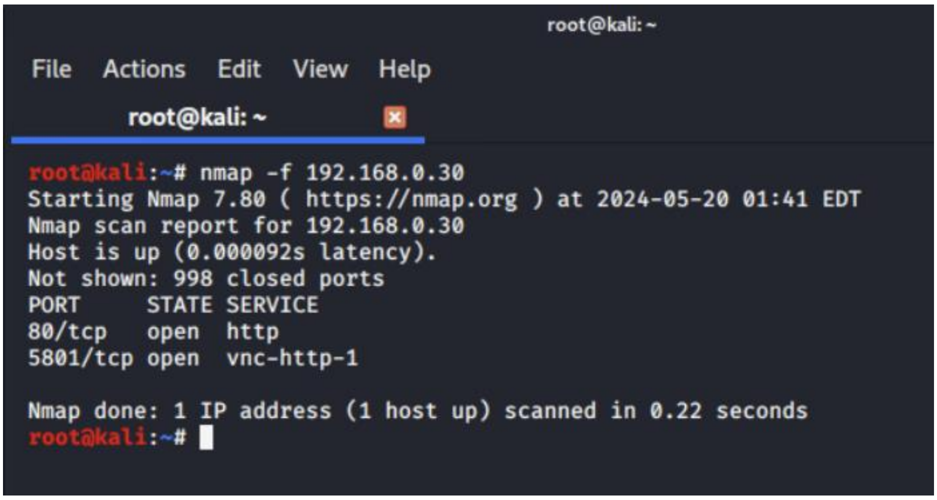
Command: nmap –f 192.168.0.30 (low mtu), nmap 192.168.0.30(standard)

Description of command: Configures Nmap to perform a network scan with packets fragmented. This Nmap scan is directed at IP address 192.168.0.30. This size ensures that each packet sent during the scan is much smaller than usual.

How it achieves IDS evasion: Fragmenting packets makes it harder for IDS to recognize harmful patterns, as key elements might be spread across multiple packets. Smaller packets often avoid detection because they don't fit the typical profiles for scanning activity monitored by many IDS configurations. Additionally, some IDS tools might not effectively reassemble fragmented packets, missing out on detecting the full content. This technique helps to sneak past network defenses by mimicking normal, fragmented network traffic, reducing the likelihood of triggering alerts.

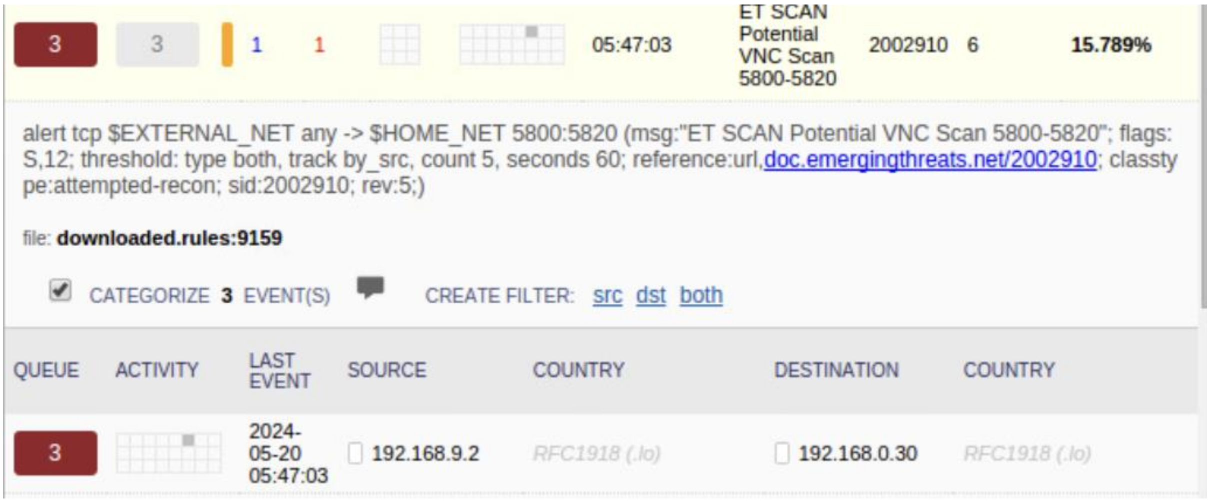
b. **Evaluate the success of the "Low MTU scan" (in the previous part) in evading the NIDs by comparing its effect on the NIDS logs compared with the simple nmap scan.**

Low MTU Scan:



```
root@kali:~# nmap -f 192.168.0.30
Starting Nmap 7.80 ( https://nmap.org ) at 2024-05-20 01:41 EDT
Nmap scan report for 192.168.0.30
Host is up (0.000092s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
80/tcp   open  http
5801/tcp open  vnc-http-1

Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
root@kali:~# 
```

Scanned 5801 (vnc-http-1).



3	3	1	1	05:47:03	ET SCAN Potential VNC Scan 5800-5820	2002910	6	15.789%

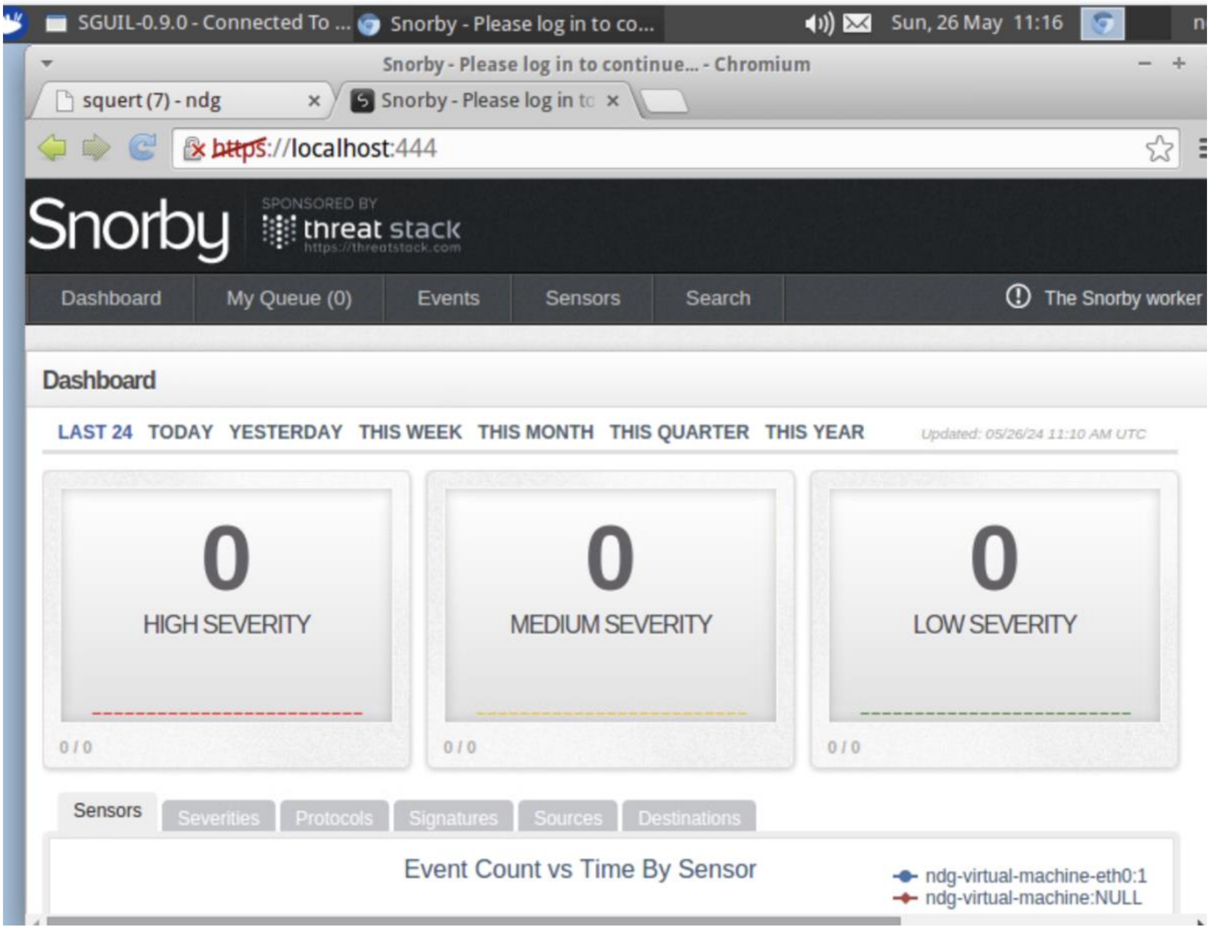
```
alert tcp $EXTERNAL_NET any -> $HOME_NET 5800:5820 (msg:"ET SCAN Potential VNC Scan 5800-5820"; flags: S,12; threshold: type both, track by_src, count 5, seconds 60; reference:url,doc.emergingthreats.net/2002910; classty pe:attempted-recon; sid:2002910; rev:5;)
```

file: **downloaded.rules:9159**

☑ CATEGORIZE **3** EVENT(S) CREATE FILTER: src dst both

QUEUE	ACTIVITY	LAST EVENT	SOURCE	COUNTRY	DESTINATION	COUNTRY
3		2024-05-20 05:47:03	□ 192.168.9.2	RFC1918 (.lo)	□ 192.168.0.30	RFC1918 (.lo)

Getting potential scan at 5800-5820 which relates to the port scanned. Snorby which is a network monitoring tool does not pick up on the fragmented packet -> successfully evading IDS.

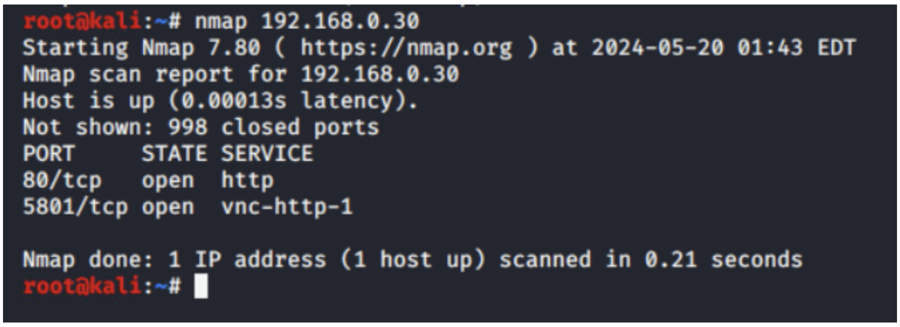

SGUIL-0.9.0 - Connected To ...
Snorby - Please log in to co...
Sun, 26 May 11:16
Snorby - Please log in to continue... - Chromium
squert (7) - ndg
Snorby - Please log in to
~~https~~://localhost:444
Snorby
SPONSORED BY
threat stack
https://threatstack.com
Dashboard
My Queue (0)
Events
Sensors
Search
The Snorby worker

Dashboard

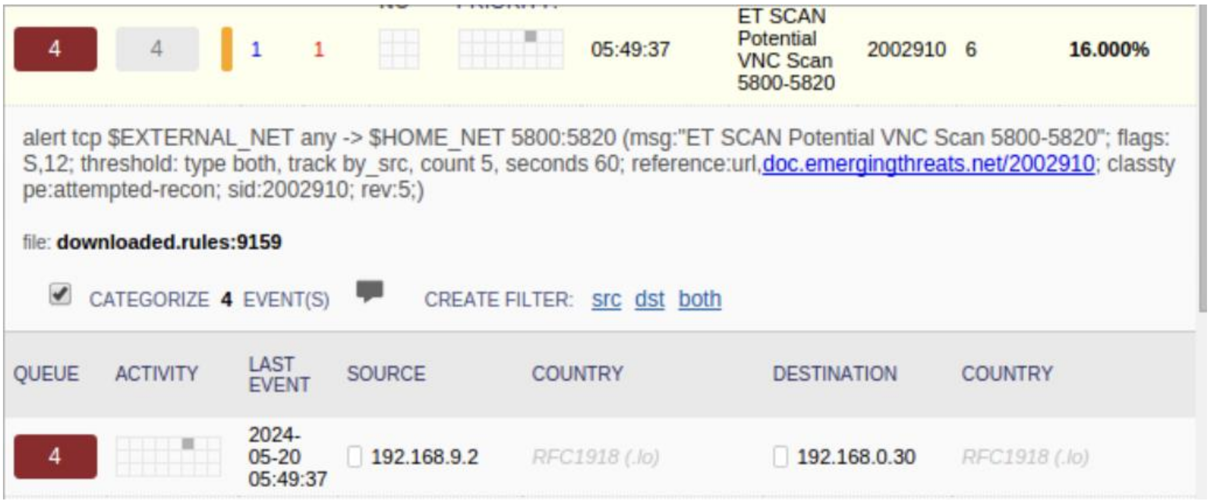
LAST 24 TODAY YESTERDAY THIS WEEK THIS MONTH THIS QUARTER THIS YEAR Updated: 05/26/24 11:10 AM UTC

0 HIGH SEVERITY	0 MEDIUM SEVERITY	0 LOW SEVERITY
0 / 0	0 / 0	0 / 0

Simple Nmap Scan:



```
root@kali:~# nmap 192.168.0.30
Starting Nmap 7.80 ( https://nmap.org ) at 2024-05-20 01:43 EDT
Nmap scan report for 192.168.0.30
Host is up (0.00013s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
80/tcp   open  http
5801/tcp open  vnc-http-1

Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds
root@kali:~# 
```



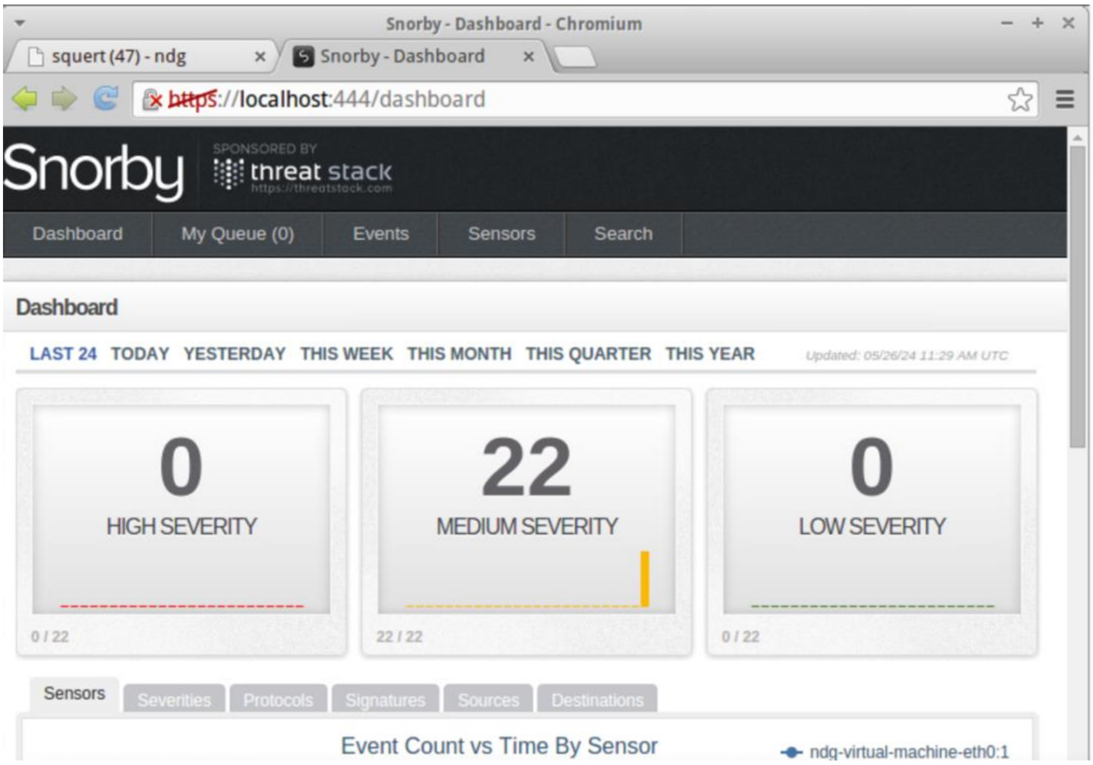
4	4	1	1			05:49:37	ET SCAN Potential VNC Scan 5800-5820	2002910	6	16.000%

alert tcp $EXTERNAL_NET any -> $HOME_NET 5800:5820 (msg:"ET SCAN Potential VNC Scan 5800-5820"; flags: S,12; threshold: type both, track by_src, count 5, seconds 60; reference:url,doc.emergingthreats.net/2002910; classtype:attempted-recon; sid:2002910; rev:5;)

file: **downloaded.rules:9159**

☑ CATEGORIZE **4** EVENT(S) CREATE FILTER: src dst both

QUEUE	ACTIVITY	LAST EVENT	SOURCE	COUNTRY	DESTINATION	COUNTRY
4		2024-05-20 05:49:37	□ 192.168.9.2	RFC1918 (.lo)	□ 192.168.0.30	RFC1918 (.lo)



Picked up on a normal Nmap scan.

c. **Describe the nmap command that was used for the “Decoy scan” method in simple words, i.e., explain what the command does in simple English.**

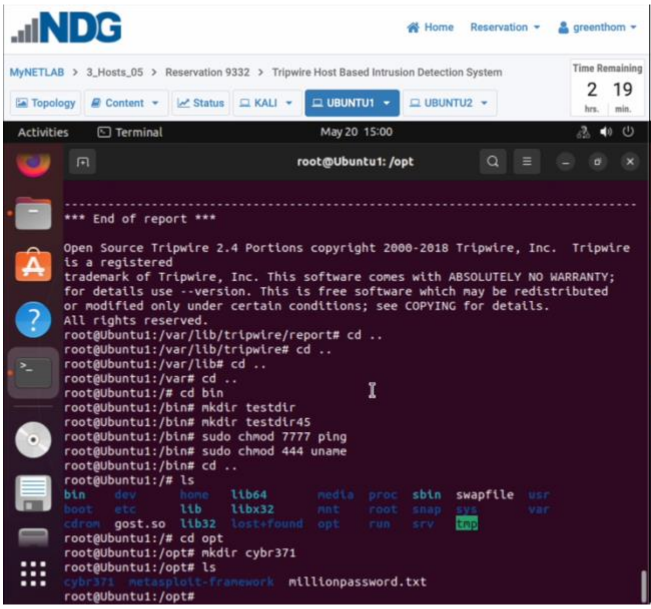
Command: nmap -D 192.168.9.20 192.168.9.30 192.168.9.40 192.168.0.30

Explanation: This command tells Nmap to scan the target IP address 192.168.0.30, but it also includes a decoy feature (‘-D’). The decoy feature makes the scan appear as if it is coming from multiple other IP addresses (‘192.168.9.20 192.168.9.30 192.168.9.40 192.168.0.30’) in addition to the real scanning machine. This tactic is used to confuse and mislead the network’s IDS, making it harder to identify where the scan is actually coming from and potentially disguising the real IP of the attacker.

PART 3: Tripwire HIDS

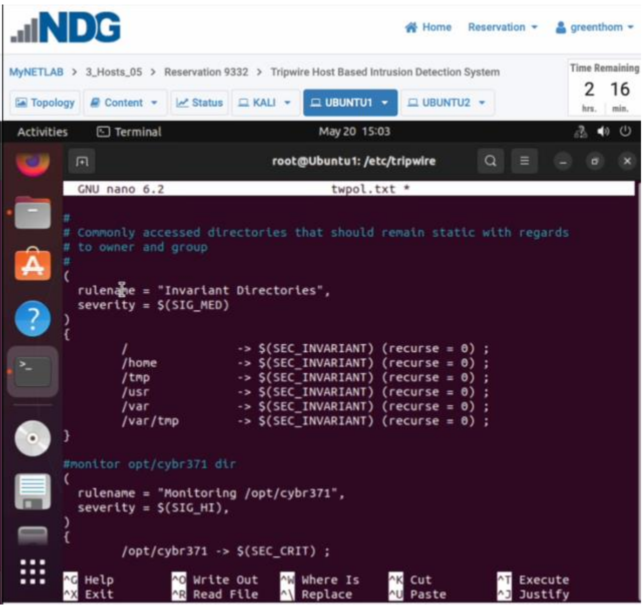
5. **Do the following:**

a. **Create a directory /opt/cybr371. Then add a rule to the tripwire’s policy file that watches the integrity of this directory, i.e., generates an alert if something is changed in that directory. Provide the rule here.**



NDG
Home
Reservation
greenthom
MyNETLAB > 3_Hosts_05 > Reservation 9332 > Tripwire Host Based Intrusion Detection System
Time Remaining 2 hrs. 19 min.
Topology
Content
Status
KALI
UBUNTU1
UBUNTU2
Activities
Terminal
May 20 15:00
root@Ubuntu1: /opt

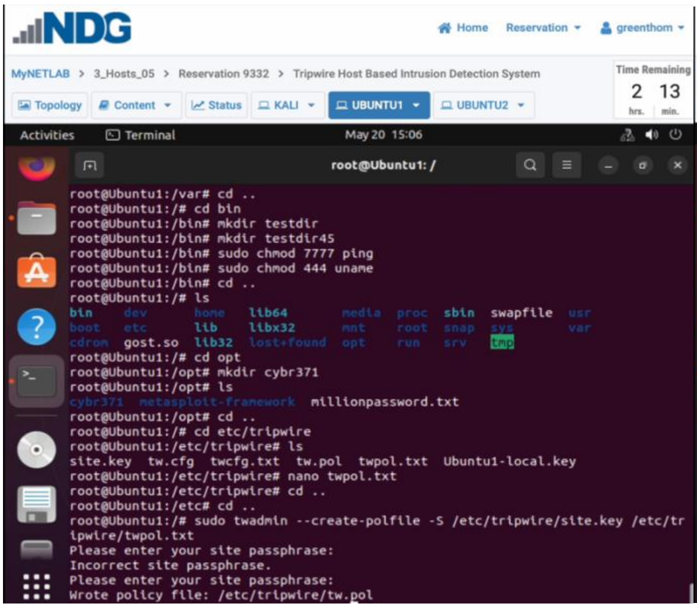
```
-------------------------------------------------------------------------------
*** End of report ***

Open Source Tripwire 2.4 Portions copyright 2000-2018 Tripwire, Inc.  Tripwire
is a registered
trademark of Tripwire, Inc. This software comes with ABSOLUTELY NO WARRANTY;
for details use --version. This is free software which may be redistributed
or modified only under certain conditions; see COPYING for details.
All rights reserved.
root@Ubuntu1:/var/lib/tripwire/report# cd ..
root@Ubuntu1:/var/lib/tripwire# cd ..
root@Ubuntu1:/var/lib# cd ..
root@Ubuntu1:/var# cd ..
root@Ubuntu1:/# cd bin
root@Ubuntu1:/bin# mkdir testdir
root@Ubuntu1:/bin# mkdir testdir45
root@Ubuntu1:/bin# sudo chmod 7777 ping
root@Ubuntu1:/bin# sudo chmod 444 uname
root@Ubuntu1:/bin# cd ..
root@Ubuntu1:/# ls
bin    dev      home   lib64       media  proc  sbin  swapfile  usr
boot   etc      lib    libx32      mnt    root  snap  sys       var
cdrom  gost.so  lib32  lost+found  opt    run   srv   tmp
root@Ubuntu1:/# cd opt
root@Ubuntu1:/opt# mkdir cybr371
root@Ubuntu1:/opt# ls
cybr371  metasploit-framework  millionpassword.txt
root@Ubuntu1:/opt#
```



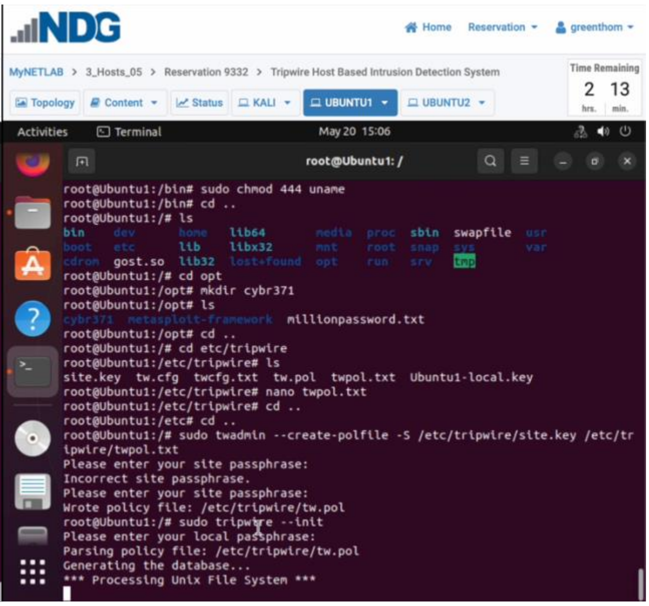
NDG
Home
Reservation
greenthom
MyNETLAB > 3_Hosts_05 > Reservation 9332 > Tripwire Host Based Intrusion Detection System
Time Remaining 2 hrs. 16 min.
Topology
Content
Status
KALI
UBUNTU1
UBUNTU2
Activities
Terminal
May 20 15:03
root@Ubuntu1: /etc/tripwire

```
  GNU nano 6.2                     twpol.txt *

#
# Commonly accessed directories that should remain static with regards
# to owner and group
#
(
  rulename = "Invariant Directories",
  severity = $(SIG_MED)
)
{
        /                    -> $(SEC_INVARIANT) (recurse = 0) ;
        /home                -> $(SEC_INVARIANT) (recurse = 0) ;
        /tmp                 -> $(SEC_INVARIANT) (recurse = 0) ;
        /usr                 -> $(SEC_INVARIANT) (recurse = 0) ;
        /var                 -> $(SEC_INVARIANT) (recurse = 0) ;
        /var/tmp             -> $(SEC_INVARIANT) (recurse = 0) ;
}

#monitor opt/cybr371 dir
(
  rulename = "Monitoring /opt/cybr371",
  severity = $(SIG_HI),
)
{
        /opt/cybr371 -> $(SEC_CRIT) ;
^G Help       ^O Write Out  ^W Where Is   ^K Cut        ^T Execute
^X Exit       ^R Read File  ^\ Replace    ^U Paste      ^J Justify
```

Created cybr371 directory inside of opt/. Added rule inside of the twpol.txt directory to generate an alert if something has changed inside of the directory. From here, update the policy information file. We then update the tripwire database:

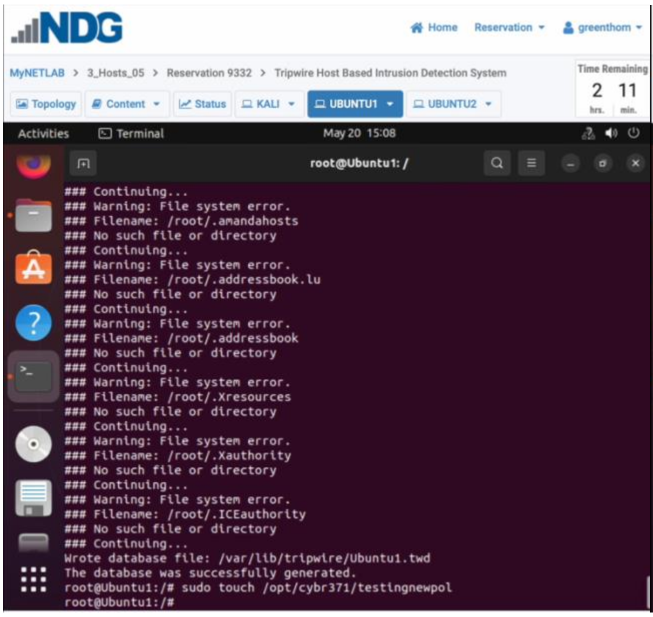


```
root@Ubuntu1:/var# cd ..
root@Ubuntu1:/# cd bin
root@Ubuntu1:/bin# mkdir testdir
root@Ubuntu1:/bin# mkdir testdir45
root@Ubuntu1:/bin# sudo chmod 7777 ping
root@Ubuntu1:/bin# sudo chmod 444 uname
root@Ubuntu1:/bin# cd ..
root@Ubuntu1:/# ls
bin    dev      home   lib64       media  proc  sbin  swapfile  usr
boot   etc      lib    libx32      mnt    root  snap  sys       var
cdrom  gost.so  lib32  lost+found  opt    run   srv   tmp
root@Ubuntu1:/# cd opt
root@Ubuntu1:/opt# mkdir cybr371
root@Ubuntu1:/opt# ls
cybr371  metasploit-framework  millionpassword.txt
root@Ubuntu1:/opt# cd ..
root@Ubuntu1:/# cd etc/tripwire
root@Ubuntu1:/etc/tripwire# ls
site.key  tw.cfg  twcfg.txt  tw.pol  twpol.txt  Ubuntu1-local.key
root@Ubuntu1:/etc/tripwire# nano twpol.txt
root@Ubuntu1:/etc/tripwire# cd ..
root@Ubuntu1:/etc# cd ..
root@Ubuntu1:/# sudo twadmin --create-polfile -S /etc/tripwire/site.key /etc/tr
ipwire/twpol.txt
Please enter your site passphrase:
Incorrect site passphrase.
Please enter your site passphrase:
Wrote policy file: /etc/tripwire/tw.pol
```

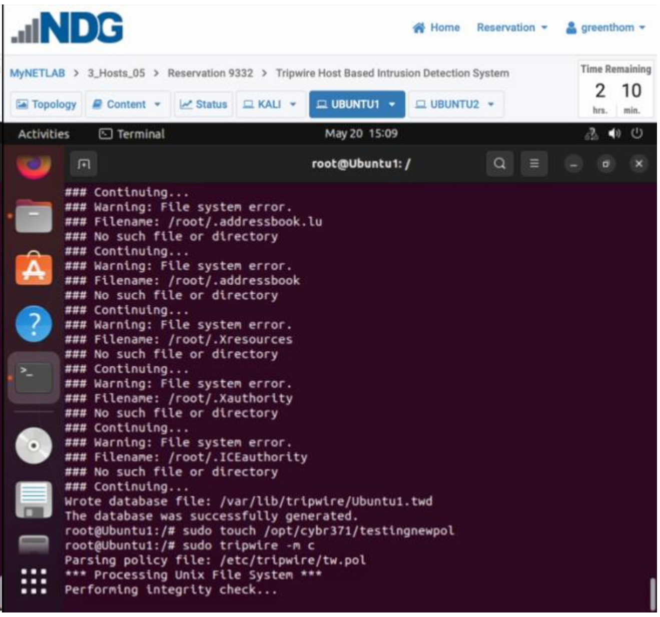


```
root@Ubuntu1:/bin# sudo chmod 444 uname
root@Ubuntu1:/bin# cd ..
root@Ubuntu1:/# ls
bin    dev      home   lib64       media  proc  sbin  swapfile  usr
boot   etc      lib    libx32      mnt    root  snap  sys       var
cdrom  gost.so  lib32  lost+found  opt    run   srv   tmp
root@Ubuntu1:/# cd opt
root@Ubuntu1:/opt# mkdir cybr371
root@Ubuntu1:/opt# ls
cybr371  metasploit-framework  millionpassword.txt
root@Ubuntu1:/opt# cd ..
root@Ubuntu1:/# cd etc/tripwire
root@Ubuntu1:/etc/tripwire# ls
site.key  tw.cfg  twcfg.txt  tw.pol  twpol.txt  Ubuntu1-local.key
root@Ubuntu1:/etc/tripwire# nano twpol.txt
root@Ubuntu1:/etc/tripwire# cd ..
root@Ubuntu1:/etc# cd ..
root@Ubuntu1:/# sudo twadmin --create-polfile -S /etc/tripwire/site.key /etc/tr
ipwire/twpol.txt
Please enter your site passphrase:
Incorrect site passphrase.
Please enter your site passphrase:
Wrote policy file: /etc/tripwire/tw.pol
root@Ubuntu1:/# sudo tripwire --init
Please enter your local passphrase:
Parsing policy file: /etc/tripwire/tw.pol
Generating the database...
*** Processing Unix File System ***
```

From here we want to add a modification to the /opt/cybr371 directory. We do this by creating a file ('testingnewpol'). From here we want to check if it has been identified by the IDS that we created a modification(file) inside of the opt/cybr371 directory.

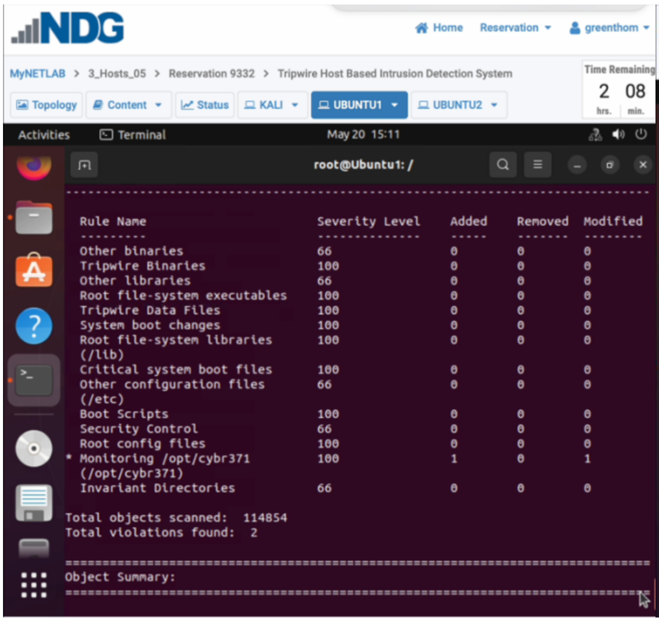


```
### Continuing...
### Warning: File system error.
### Filename: /root/.amandahosts
### No such file or directory
### Continuing...
### Warning: File system error.
### Filename: /root/.addressbook.lu
### No such file or directory
### Continuing...
### Warning: File system error.
### Filename: /root/.addressbook
### No such file or directory
### Continuing...
### Warning: File system error.
### Filename: /root/.Xresources
### No such file or directory
### Continuing...
### Warning: File system error.
### Filename: /root/.Xauthority
### No such file or directory
### Continuing...
### Warning: File system error.
### Filename: /root/.ICEauthority
### No such file or directory
### Continuing...
Wrote database file: /var/lib/tripwire/Ubuntu1.twd
The database was successfully generated.
root@Ubuntu1:/# sudo touch /opt/cybr371/testingnewpol
root@Ubuntu1:/#
```

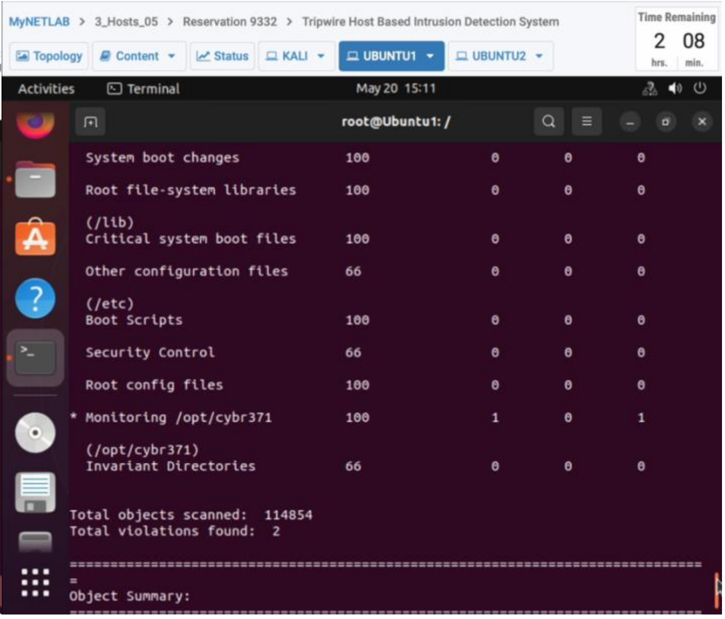


```
### Continuing...
### Warning: File system error.
### Filename: /root/.addressbook.lu
### No such file or directory
### Continuing...
### Warning: File system error.
### Filename: /root/.addressbook
### No such file or directory
### Continuing...
### Warning: File system error.
### Filename: /root/.Xresources
### No such file or directory
### Continuing...
### Warning: File system error.
### Filename: /root/.Xauthority
### No such file or directory
### Continuing...
### Warning: File system error.
### Filename: /root/.ICEauthority
### No such file or directory
### Continuing...
Wrote database file: /var/lib/tripwire/Ubuntu1.twd
The database was successfully generated.
root@Ubuntu1:/# sudo touch /opt/cybr371/testingnewpol
root@Ubuntu1:/# sudo tripwire -m c
Parsing policy file: /etc/tripwire/tw.pol
*** Processing Unix File System ***
Performing integrity check...
```

We then want to observe the report to see if the rule change to the policy has worked. Here we can see that the rule had an effect on the report with it picking up on the changes (added: 1, modifications: 1).



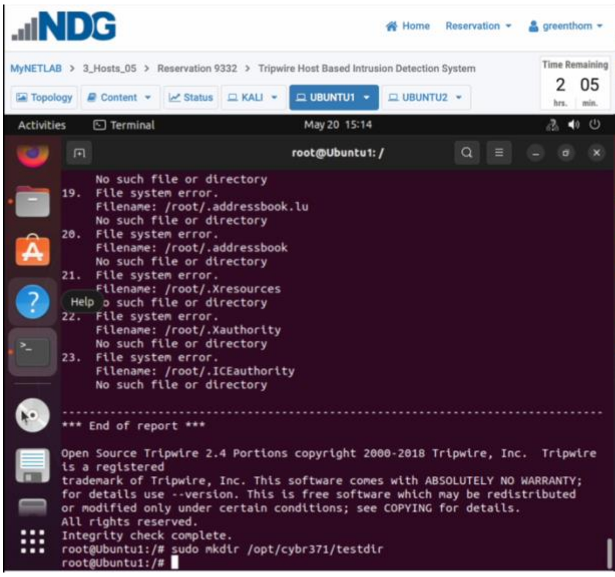
```
-----------------------------------------------------------------------------

  Rule Name                       Severity Level    Added    Removed  Modified
  ---------                       --------------    -----    -------  --------
  Other binaries                  66                0        0        0
  Tripwire Binaries               100               0        0        0
  Other libraries                 66                0        0        0
  Root file-system executables    100               0        0        0
  Tripwire Data Files             100               0        0        0
  System boot changes             100               0        0        0
  Root file-system libraries      100               0        0        0
  (/lib)
  Critical system boot files      100               0        0        0
  Other configuration files       66                0        0        0
  (/etc)
  Boot Scripts                    100               0        0        0
  Security Control                66                0        0        0
  Root config files               100               0        0        0
* Monitoring /opt/cybr371         100               1        0        1
  (/opt/cybr371)
  Invariant Directories           66                0        0        0

Total objects scanned:  114854
Total violations found:  2

=============================================================================
Object Summary:
=============================================================================
```



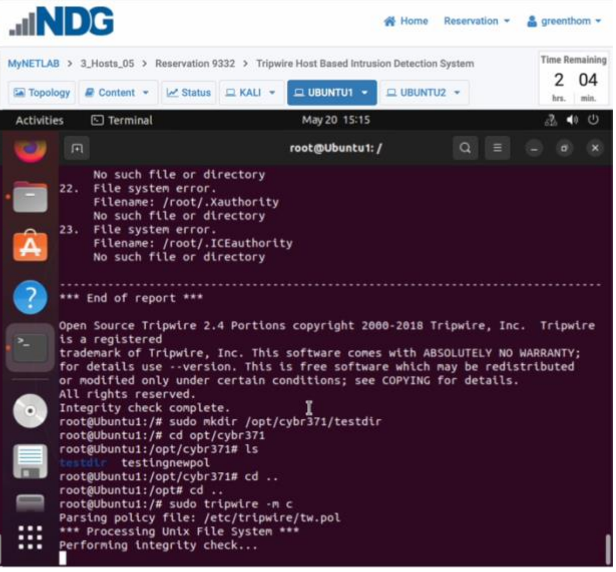
```
  System boot changes             100               0        0        0

  Root file-system libraries      100               0        0        0

  (/lib)
  Critical system boot files      100               0        0        0

  Other configuration files       66                0        0        0

  (/etc)
  Boot Scripts                    100               0        0        0

  Security Control                66                0        0        0

  Root config files               100               0        0        0

* Monitoring /opt/cybr371         100               1        0        1

  (/opt/cybr371)
  Invariant Directories           66                0        0        0


Total objects scanned:  114854
Total violations found:  2

===============================================================================
=
Object Summary:
===============================================================================
```

b. **Violate the integrity of the directory by creating a sub-directory inside it. Did tripwire produce an alert? If so, provide the report here. If not, explain why it was not generated.**

To test if the rule change that we added to the policy was effective against the creation of a sub-directory, we want to create a directory inside of opt/cybr371. From here we want to check if it has been identified by the IDS that we created a modification(directory) inside of the opt/cybr371 directory.

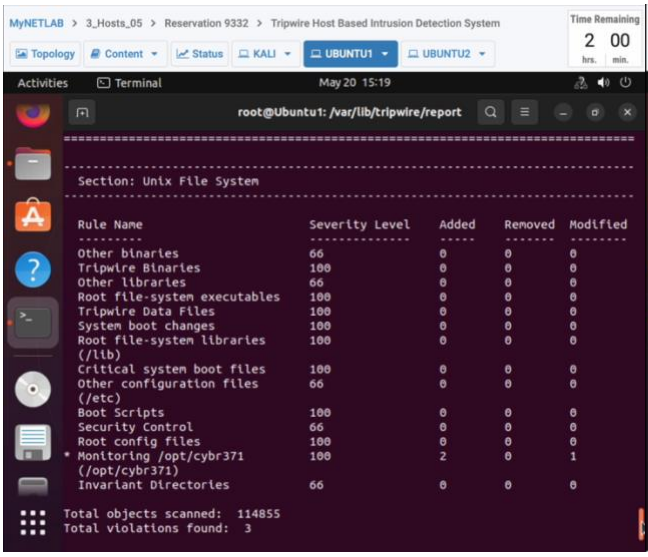


```
     No such file or directory
19.  File system error.
     Filename: /root/.addressbook.lu
     No such file or directory
20.  File system error.
     Filename: /root/.addressbook
     No such file or directory
21.  File system error.
     Filename: /root/.Xresources
     No such file or directory
22.  File system error.
     Filename: /root/.Xauthority
     No such file or directory
23.  File system error.
     Filename: /root/.ICEauthority
     No such file or directory

-------------------------------------------------------------------------------
*** End of report ***

Open Source Tripwire 2.4 Portions copyright 2000-2018 Tripwire, Inc.  Tripwire
is a registered
trademark of Tripwire, Inc. This software comes with ABSOLUTELY NO WARRANTY;
for details use --version. This is free software which may be redistributed
or modified only under certain conditions; see COPYING for details.
All rights reserved.
Integrity check complete.
root@Ubuntu1:/# sudo mkdir /opt/cybr371/testdir
root@Ubuntu1:/# 
```

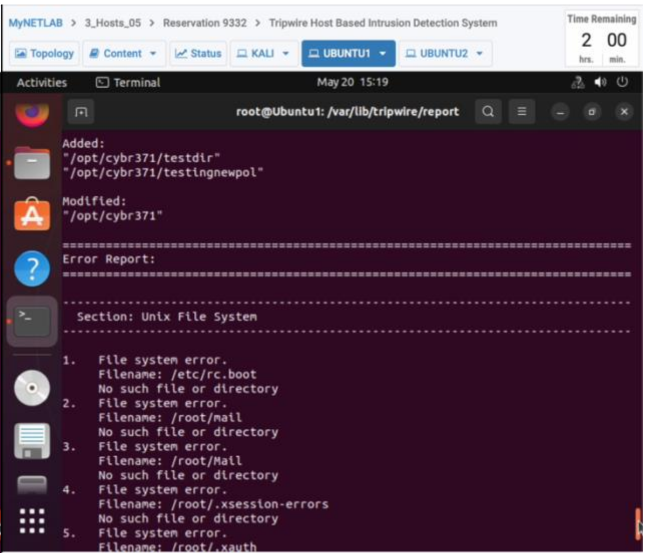


```
     No such file or directory
22.  File system error.
     Filename: /root/.Xauthority
     No such file or directory
23.  File system error.
     Filename: /root/.ICEauthority
     No such file or directory

-------------------------------------------------------------------------------
*** End of report ***

Open Source Tripwire 2.4 Portions copyright 2000-2018 Tripwire, Inc.  Tripwire
is a registered
trademark of Tripwire, Inc. This software comes with ABSOLUTELY NO WARRANTY;
for details use --version. This is free software which may be redistributed
or modified only under certain conditions; see COPYING for details.
All rights reserved.
Integrity check complete.
root@Ubuntu1:/# sudo mkdir /opt/cybr371/testdir
root@Ubuntu1:/# cd opt/cybr371
root@Ubuntu1:/opt/cybr371# ls
testdir  testingnewpol
root@Ubuntu1:/opt/cybr371# cd ..
root@Ubuntu1:/opt# cd ..
root@Ubuntu1:/# sudo tripwire -m c
Parsing policy file: /etc/tripwire/tw.pol
*** Processing Unix File System ***
Performing integrity check...
```

We then want to observe the report to see if the rule change to the policy has worked. Here we can see that the rule had an effect in the report with it picking up on the changes of adding a sub-directory inside of /opt/cybr371. It specifies the added files also. We can see that added is at 2 meaning the file created before in a. as well as the directory. Also signifies the latest modifications (directory).


MyNETLAB > 3_Hosts_05 > Reservation 9332 > Tripwire Host Based Intrusion Detection System
Topology
Content
Status
KALI
UBUNTU1
UBUNTU2
Time Remaining
2 00
hrs. min.
Activities
Terminal
May 20 15:19
root@Ubuntu1: /var/lib/tripwire/report

```
===============================================================================

-------------------------------------------------------------------------------
  Section: Unix File System
-------------------------------------------------------------------------------

  Rule Name                       Severity Level    Added    Removed  Modified
  ---------                       --------------    -----    -------  --------
  Other binaries                  66                0        0        0
  Tripwire Binaries               100               0        0        0
  Other libraries                 66                0        0        0
  Root file-system executables    100               0        0        0
  Tripwire Data Files             100               0        0        0
  System boot changes             100               0        0        0
  Root file-system libraries      100               0        0        0
  (/lib)
  Critical system boot files      100               0        0        0
  Other configuration files       66                0        0        0
  (/etc)
  Boot Scripts                    100               0        0        0
  Security Control                66                0        0        0
  Root config files               100               0        0        0
* Monitoring /opt/cybr371         100               2        0        1
  (/opt/cybr371)
  Invariant Directories           66                0        0        0

Total objects scanned:  114855
Total violations found:  3
```


MyNETLAB > 3_Hosts_05 > Reservation 9332 > Tripwire Host Based Intrusion Detection System
Topology
Content
Status
KALI
UBUNTU1
UBUNTU2
Time Remaining
2 00
hrs. min.
Activities
Terminal
May 20 15:19
root@Ubuntu1: /var/lib/tripwire/report

```
Added:
"/opt/cybr371/testdir"
"/opt/cybr371/testingnewpol"

Modified:
"/opt/cybr371"

===============================================================================
Error Report:
===============================================================================

-------------------------------------------------------------------------------
  Section: Unix File System
-------------------------------------------------------------------------------

1.    File system error.
      Filename: /etc/rc.boot
      No such file or directory
2.    File system error.
      Filename: /root/mail
      No such file or directory
3.    File system error.
      Filename: /root/Mail
      No such file or directory
4.    File system error.
      Filename: /root/.xsession-errors
      No such file or directory
5.    File system error.
      Filename: /root/.xauth
```

6. **Can tripwire be used to create alerts when a file or directory is only accessed (is read) but not modified? If the answer is affirmative, provide an example rule, if the answer is negative, discuss an alternative.**

Tripwire is used to detect changes in file systems based on attributes like file content, permissions, timestamps, and other properties that indicate modifications. It does not monitor or log simple read accesses (not modifying contents) to files or directories because this kind of monitoring does not alter any attributes that Tripwire checks.

Tripwire uses cryptographic hashes to check the integrity of files and directories. When a file or directory is only read and not modified, its hash remains unchanged. Therefore, Tripwire does not generate alerts for read-only accesses since its primary function is to detect modifications that could signify unauthorized changes, corruption, or other security threats.

An alternative solution is using kernels such as SELinux (Security-Enhanced Linux), which is a Linux kernel security module that provides mandatory access controls and other access control security policies to directories. It provides mandatory access control architecture to its subsystems which enforces the separation of information within the system based on confidentiality and integrity requirements. Provides alert system (SELinux access control errors section) which is provided in a table -> provides access control errors.