

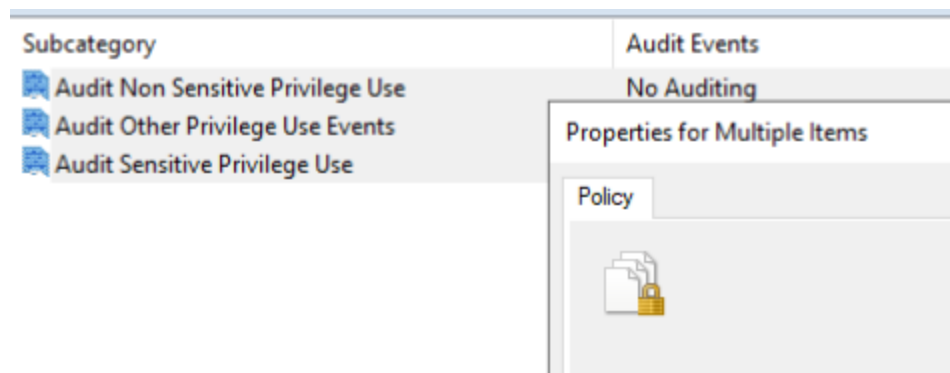
Colby Heilner
Professor Torres
11/12
IT 120
Lab 11

Part A: NETLAB Security+ v4: Identify and Analyze Network/Host NDS/IDS Alerts

NETLAB IDS

- Using the websites below, configure 10 logs against WinOSDomainController
 - [Windows Audit Policies](#)
- [Links to an external site.](#)
- [Windows Event IDs](#)
- - [Links to an external site.](#)
- Configure a shared folder Called Justice and add Superman, Batman, and Wonderwoman to the WinOS
 - Grant Wonderwoman access to the folder.
- Test the below activity to ensure logs are generated
 - Log in with an invalid password on Superman and Batman
 - Attempt to access the Justice folder as Batman
 - Verify that logs are generated with Screenshots

While enabling these policies, I learned that you could configure multiple at once



```
C:\Windows\system32>net user













User accounts for \\WINOS

-----
Administrator          batman                Guest
krbtgt                  lab2-user             lab-user
lab-user-id             superman              wonderwoman
The command completed successfully.
```

Audit for my File share with wonderwoman

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	11/13/2024 2:07:20 AM	Microsoft Windows sec...	5145	Detailed File Share
Audit Success	11/13/2024 2:07:20 AM	Microsoft Windows sec...	5145	Detailed File Share
Audit Success	11/13/2024 2:07:20 AM	Microsoft Windows sec...	5140	File Share

Here is a audit log for incorrect login.

 Audit Failure	11/13/2024 2:09:16 AM	Microsoft Wind
 Audit Success	11/13/2024 2:09:15 AM	Microsoft Wind
 Audit Success	11/13/2024 2:09:04 AM	Microsoft Wind
 Audit Success	11/13/2024 2:09:04 AM	Microsoft Wind
 Audit Success	11/13/2024 2:09:04 AM	Microsoft Wind
 Audit Success	11/13/2024 2:09:04 AM	Microsoft Wind
 Audit Success	11/13/2024 2:09:04 AM	Microsoft Wind
 Audit Success	11/13/2024 2:09:04 AM	Microsoft Wind
 Audit Success	11/13/2024 2:09:04 AM	Microsoft Wind
 Audit Success	11/13/2024 2:09:04 AM	Microsoft Wind
 Audit Success	11/13/2024 2:09:04 AM	Microsoft Wind
 Audit Success	11/13/2024 2:09:04 AM	Microsoft Wind

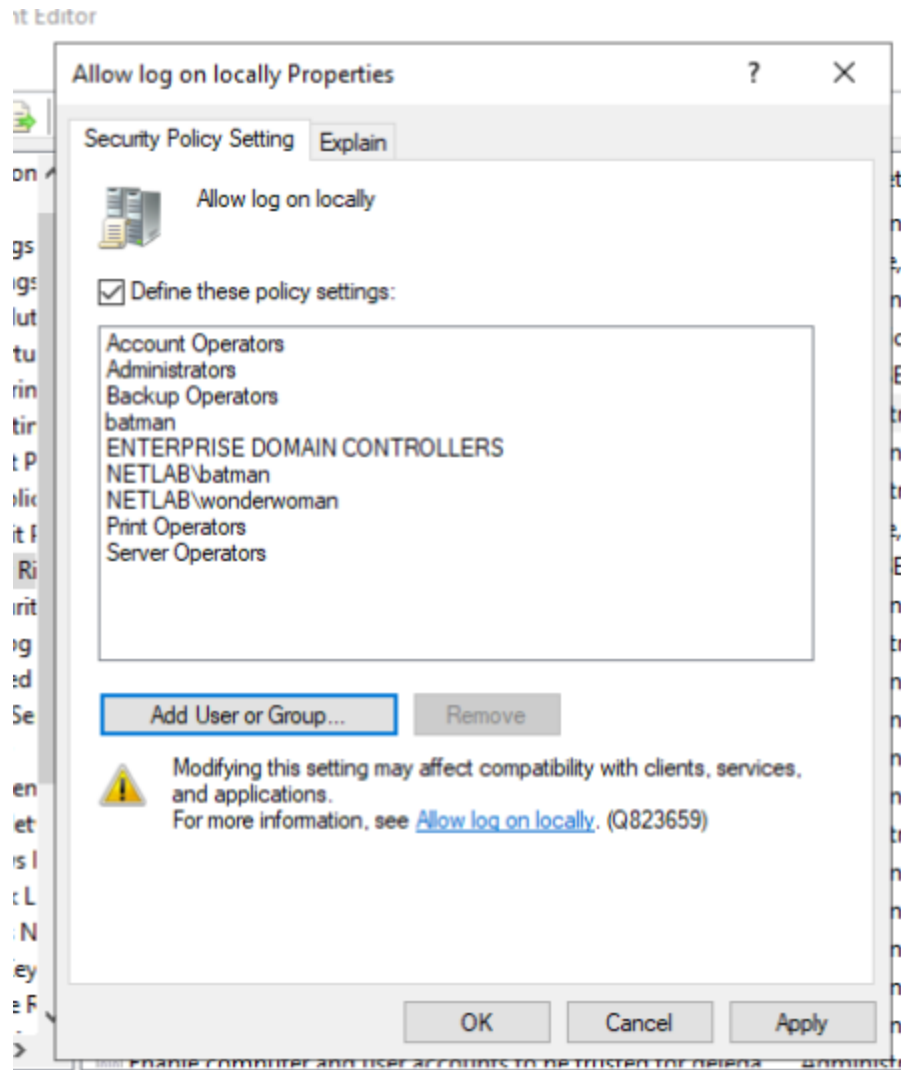
Event 4625, Microsoft Windows security auditing.

General Details

☒ Friendly View ☐ XML View

SubjectUserName administrator
SubjectDomainName NETLAB
SubjectLogonId 0x98aa6
TargetUserSid S-1-0-0
TargetUserName batman
TargetDomainName NETLAB
Status 0xc000006d
FailureReason %%2313
SubStatus 0xc000006a

Worth noting that you must configure this setting to allow new accounts to logon locally to a DC

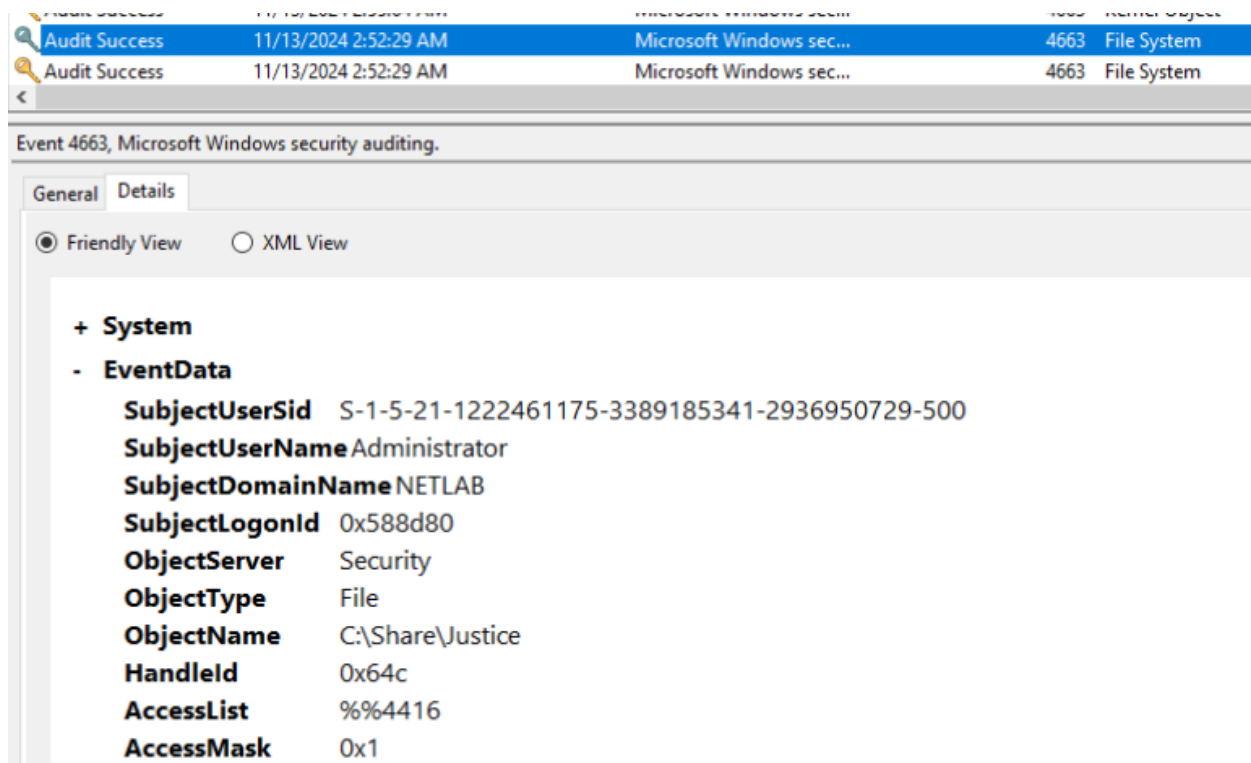


Batman failing to access folder

I was unable to generate failed to access object on the folder.

Not sure why but it has something to do with every time I try to access it also gives me a popup to login with admin to access it.

But could get these



Part B:

- Log on to Security Onion
 - open terminal, and become root
 - run the command so-allow
 - Port Forward the pfSense logs to Security Onion (This is done on pfSense Gui)
 - Add the rules in Security Onion to allow access to the agents and the firewall
 - so-allow (three Windows agents, 2 Linux agents)
- Log on to the WindowsOS
 - open the browser to 192.168.0.6, log on to Security Onion
 - Download and install Windows tools
- Log on to UbuntuSRV
 - open the browser to 192.168.0.6, log on to Security Onion
 - Download and install Linux tools
- Due to an issue with Netlab, there is no way to test this environment.

- **Please provide enough screenshots and notes to show that you did the work**

I copied the ips of the win and Linux machine onto a note pad and started opening all ports for the agents

File	Edit	View	Search	Terminal	Help
<pre> Started: 04:26:31.659990 Duration: 951.415 ms Changes: Summary for local ----- Succeeded: 93 (changed=2) Failed: 0 ----- Total states run: 93 Total run time: 10.147 s [root@seconion sysadmin]# so-allow This program allows you to add a firewall rule to allow connections from a new IP address. Choose the role for the IP or Range you would like to add [a] - Analyst - ports 80/tcp and 443/tcp [b] - Logstash Beat - port 5044/tcp [e] - Elasticsearch REST API - port 9200/tcp [f] - Strelka frontend - port 57314/tcp [o] - Osquery endpoint - port 8090/tcp [s] - Syslog device - 514/tcp/udp [w] - Wazuh agent - port 1514/tcp/udp [p] - Wazuh API - port 55000/tcp [r] - Wazuh registration service - 1515/tcp Please enter your selection: 0 Enter a single ip address or range to allow (example: 10.10.10.10 or 10.10.0.0/16): 172.16.1.10 Adding 172.16.1.10 to the osquery_endpoint role. This can take a few seconds </pre>					<pre> ubuntu 172.16.1.10 win 192.168.0.50 </pre>

Windows agents

s

Enter a single ip address or range to allow (example: 10.10.10.10 or 10.10.0.0/16):

192.168.0.50

Adding 192.168.0.50 to the syslog role. This can take a few seconds

■

Adding 192.168.0.50 to the wazuh_agent role. This can take a few seconds

Already exists

^C

Exiting gracefully on Ctrl-c

[root@seconion sysadmin]# so-allow

This program allows you to add a firewall rule to allow connections from a new IP address.

Choose the role for the IP or Range you would like to add

- [a] - Analyst - ports 80/tcp and 443/tcp
- [b] - Logstash Beat - port 5044/tcp
- [e] - Elasticsearch REST API - port 9200/tcp
- [f] - Strelka frontend - port 57314/tcp
- [o] - Osquery endpoint - port 8090/tcp
- [s] - Syslog device - 514/tcp/udp
- [w] - Wazuh agent - port 1514/tcp/udp
- [p] - Wazuh API - port 55000/tcp
- [r] - Wazuh registration service - 1515/tcp

Please enter your selection:

o

Enter a single ip address or range to allow (example: 10.10.10.10 or 10.10.0.0/16):

192.168.0.50

Adding 192.168.0.50 to the osquery_endpoint role. This can take a few seconds

■

Pfsense Forward

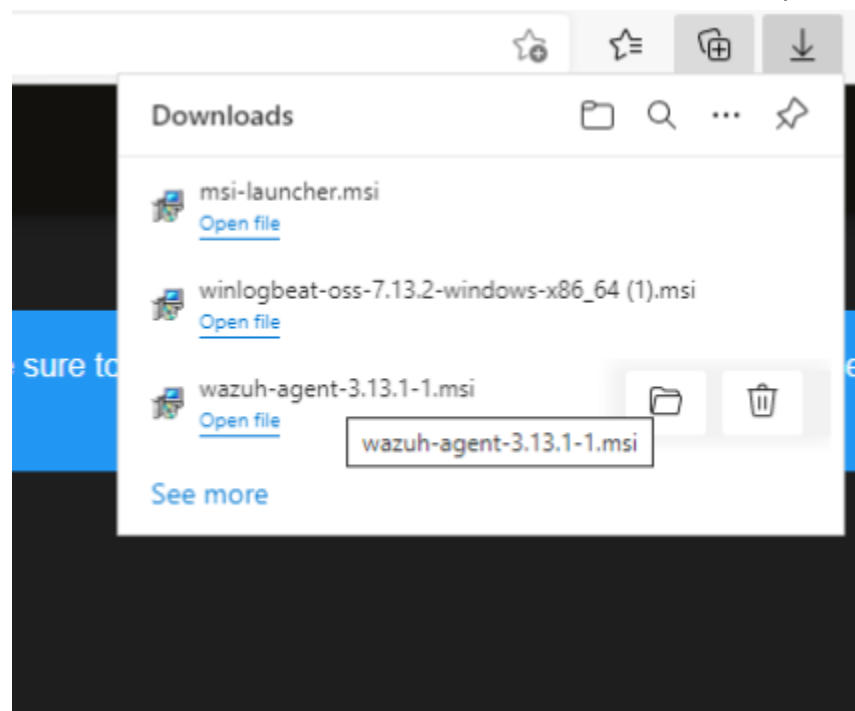
selected type is not found on the chosen interface, the other type

Remote log servers

Remote Syslog Contents

- ☒ Everything
- ☐ System Events
- ☐ Firewall Events
- ☒ DNS Events (Resolver/unbound, Forwarder/dnsmasq, filterdn
- ☐ DHCP Events (DHCP Daemon, DHCP Relay, DHCP Client)
- ☐ PPP Events (PPPoE WAN Client, L2TP WAN Client, PPTP WAN
- ☐ General Authentication Events
- ☐ Captive Portal Events
- ☐ VPN Events (IPsec, OpenVPN, L2TP, PPPoE Server)
- ☐ Gateway Monitor Events
- ☐ Routing Daemon Events (RADVD, IPnP, RIP, OSPF, BGP)

Here are the windows files that I was able to install, and press KEEP.



Now Linux files,

```
sysadmin@ubuntu:~$ ls
Desktop  http.js      package.json.1  Public  Videos
Documents Music        package-lock.json snap
Downloads node_modules Pictures      Templates

sysadmin@ubuntu:~$ cd Downloads/
sysadmin@ubuntu:~/Downloads$ ls
deb-launcher.deb  javascripts  wazuh-agent_3.13.1-1_amd64.deb
sysadmin@ubuntu:~/Downloads$ dpkg -i wazuh-agent_3.13.1-1_amd64.deb
dpkg: error: requested operation requires superuser privilege
sysadmin@ubuntu:~/Downloads$ sudo dpkg -i wazuh-agent_3.13.1-1_amd64.deb
[sudo] password for sysadmin:
Selecting previously unselected package wazuh-agent.
(Reading database ... 170237 files and directories currently installed.)
Preparing to unpack wazuh-agent_3.13.1-1_amd64.deb ...
Unpacking wazuh-agent (3.13.1-1) ...
```

Part C:

- [Review the videos on this link. The times and titles are listed below:](#)
- [Links to an external site.](#)
- Intro to Security Onion (12:32)
- Installation part 1 (6:34)
- Installation part 2 (10:28)
- Intro to Analysis Tools (20:20)
- Updating (8:11)
- Alert Triage and Case Creation (16:11)
- Threat Hunting (17:20)
- Detection Engineering (16:19)
- Course Wrapup (5:01)
- About three and a half hours of Video
- **After viewing the videos**, review Netlab --> Security+v4-->Lab 08:
Identifying and Analyzing Network/Host Intrusion Detection System (NIDS/HIDS) Alerts:
- Within this lab, kali scanned some targets, ran Wireshark, saved the pcap (packet data), and imported it into Security Onion for analysis.
- Does the analysis make sense? Can you follow along with the handout?

Yes, I am going to run my own nmap scan and capture it with wireshark. I will the import it and check it out on sec onion.

I copied over the pcap file to sec onion and had a permission error I fixed.

```
13/11/2024 16:01:55 /home/mobaxterm scp /drives/c/Users/colby/Documents/nmap2.pcap admin@192.168.4.99:/home/admin/SecurityOnion/pcaps
#####
###
###  UNAUTHORIZED ACCESS PROHIBITED  ###
###
#####
nmap2.pcap
```

```
root@seconion pcaps1# mv nmap.pcap
mv: missing destination file operand
Try 'mv --help' for more information
root@seconion pcaps1# mv nmap.pcap
mv: missing destination file operand
Try 'mv --help' for more information
root@seconion pcaps1# ls
nmap.pcapng test
root@seconion pcaps1# ls
nmap2.pcap nmap.pcapng test
root@seconion pcaps1# _
```

Here is my confirmation

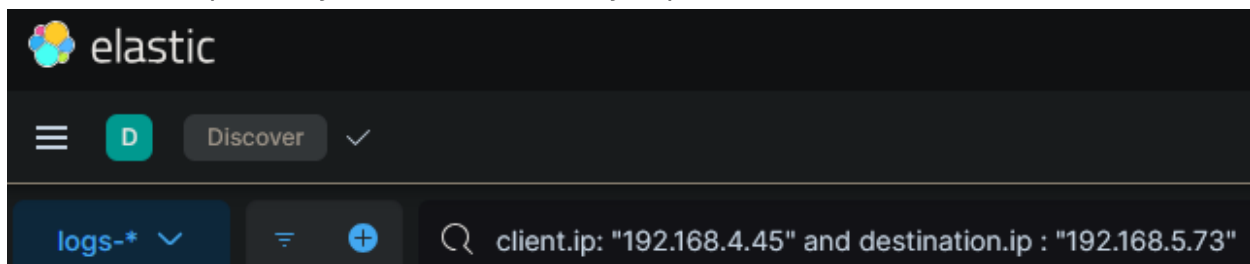
```
Import complete!

Use the following hyperlink to view the imported data. Triple-click to quickly highlight the entire
hyperlink and then copy it into a browser:
https://192.168.4.99/#/dashboards?q=import.id:60921a845fd5ddffc3bf0d51474020c7:20:7C:20groupby:20event.module:20:7C:20groupby:20-sankey:20event.module:20event.dataset:20:7C:20groupby:20event.dataset:20:7C:20groupby:20source.ip:20:7C:20groupby:20destination.ip:20:7C:20groupby:20destination.port:20:7C:20groupby:20network.protocol:20:7C:20groupby:20rule.name:20rule.category:20event.severity_label:20:7C:20groupby:20dns.query.name:20:7C:20groupby:20file.mime_type:20:7C:20groupby:20http.virtual_host:20http.uri:20:7C:20groupby:20notice.message:20notice.sub_message:20:7C:20groupby:20ssl.server_name:20:7C:20groupby:20source_geo.organization_name:20source_geo.country_name:20:7C:20groupby:20destination_geo.organization_name:20destination_geo.country_name&t=2024:2F11:2F13:2000:3A00:3A00:20AM&z=UTC

or, manually set the Time Range to be (in UTC):
From: 2024-11-13 To: 2024-11-14

Note: It can take 30 seconds or more for events to appear in Security Onion Console.
root@seconion pcaps1# _
```

I did a scan with 192.168.4.45, against 192.168.5.73 After importing and setting my filter to scr and dst respectively. I was able to see my imported traffic.



With a little learning of the filters, I was able to then view my port 80 Nmap connections

Edit filter

=

destination.port

▼

is one of

▼

80 ×

Preview

destination.port: is one of 80

Custom label (optional)

Add a custom label here

3

17:0018:0019:0020:0021:0022:0023:0000:0001:0002:0003:0004:0005:00

November 12, 2024November 13, 2024

Nov 12, 2024 @ 16:37:58.671 - Nov 13, 2024 @ 16:37:58.671 (Inte

Documents (45)

Field statistics

@timestamp ⌚ ↑

Document

🔗

☐

Nov 13, 2024 @ 15:55:36.982

@timestamp Nov 13, 2024 @ 15:55:36.982 @version 1 client.bytes 12 client.ip 192.168.4.45 c
connection.bytes.missed 0 connection.history ShADaFf connection.local.originator true conn
completion.container.id conn.log data_stream.dataset zeek data_stream.namespace so data_str
elastic_agent.id 1aebc270-94dd-4317-ace6-39a884394905 elastic_agent.snapshot false elastic
event.ingested Nov 13, 2024 @ 15:55:48.281 event.module zeek input.type log log.file.path
{\"ts\":1731542136.982259,\"uid\":\"CvzSS1NnxjBduXJ45\",\"id.orig_h\":\"192.168.4.45\",\"id.orig_p\":4
ig_bytes\":12,\"resp_bytes\":0,\"conn_state\":\"SF\",\"local_orig\":true,\"local_resp\":true,\"missed_b
32,\"community_id\":\"1:coAz6ZJnfB8SGbF4Q/dYb8Eor5w=\",\"orig_mac_oui\":\"HP Inc.\"} metadata.beat
metadata.pipeline zeek.conn metadata.raw_index logs-zeek-so metadata.stream_id logfile-log
network.community_id 1:coAz6ZJnfB8SGbF4Q/dYb8Eor5w= network.transport tcp observer.name se
3 server.port 80 source.ip 192.168.4.45 source.port 47043 tags [elastic-agent, input-secc
eek-so-2024.11.08-000001 _score -