

Cybersecurity Capstone Netcat Project Presentation for 10ALYTICS-DC

JUDE CHIDUBEM ANYAEGBU

- **Title:** Strengthening Security Monitoring at 10ALYTICS-DC
- **Subtitle:** Detecting Unauthorized Netcat Processes with Wazuh
- **Details:**

Presented by: Jude Chidubem Anyaegbu

Date: June 18, 2025

Capstone Netcat Project for
10ALYTICS-DC



PROJECT PROCEDURE

Project Overview

This project addresses critical security gaps at 10ALYTICS-DC by leveraging Wazuh's capabilities to monitor and respond to unauthorized Netcat usage, a common tool for data exfiltration and backdoors."

Content:

- **Problem:** Threat intelligence reports increased attempts to exploit systems via unauthorized tools, particularly Netcat.
- **Goal:** Enhance security monitoring using Wazuh to detect and block malicious processes in real-time.

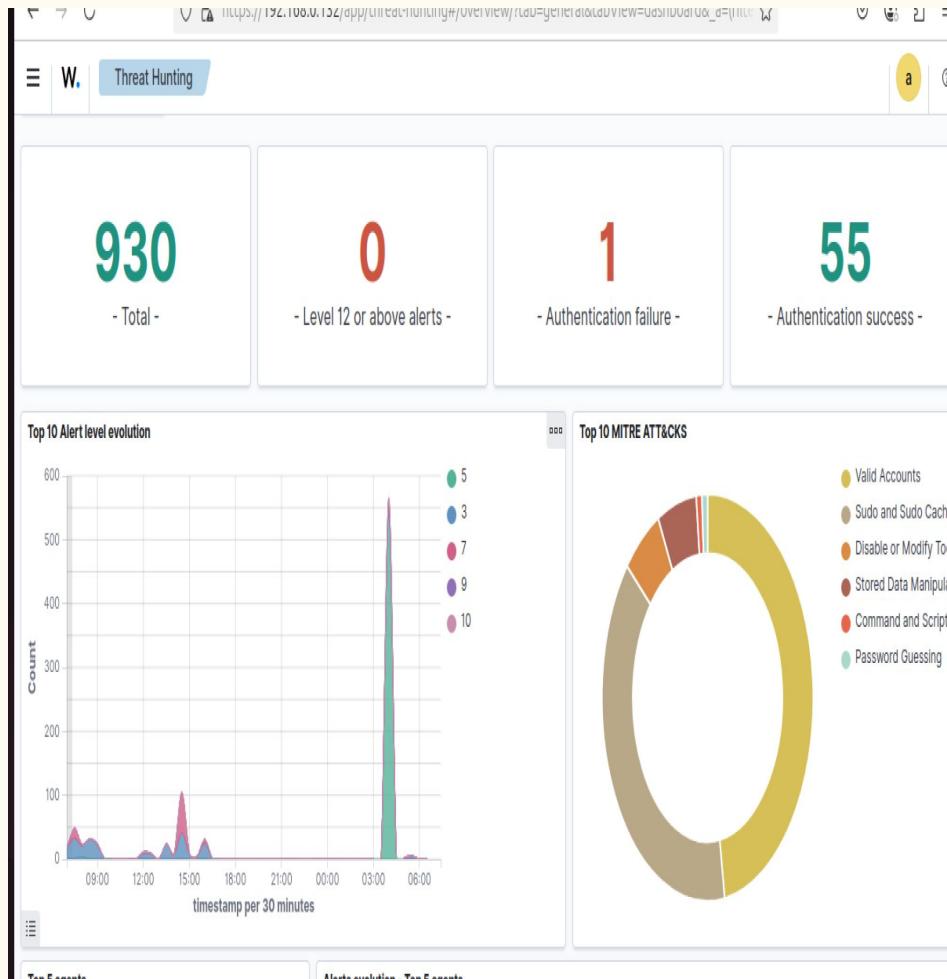
Materials

The project was carried out with virtual machine tools listed

- Laptop
 - Ubuntu VM
 - Kali VM
 - Wazuh VM
 - Slack App
 - Netcat VM
-

Objectives

- Detect unauthorized Netcat processes, especially in listening mode.
- Generate real-time security alerts for suspicious activity.
- Implement active response to terminate malicious processes.
- Document findings and provide mitigation strategies.



Methodology

1. Deploy Wazuh manager and agents on Linux servers.
2. Configure process monitoring for Netcat detection.
3. Create custom Wazuh rules for alerting.
4. Set up active response to terminate unauthorized processes.
5. Archive results and document findings.



ACTIVE STEP

SET UP WAZUH :

- Start wazuh manager, dashboard, and Indexer, with {sudo systemctl start wazuh- ...}
- Run wazuh-manager status {sudo systemctl status wazuh-manager}
- Run {ifconfig} to confirm my ip address
- Integrate my slack app on wazuh for real time monitoring by running {sudo nano /var/ossec/etc/ossec.conf} this action came after creating app in in slack platform
- I create Netcatcat rule after set up my wazuh agent in ubuntu {sudo nano /var/ossec/etc/rules/local_rules.xml}

```
Loaded: loaded (/usr/lib/systemd/system/wazuh-manager.service; enabled; pri-  
Active: active (running) since Thu 2025-06-12 09:05:06 UTC; 4min 24s ago  
Process: 1032 ExecStart=/usr/bin/wazuh-control start --  
Tasks: 111 (limit: 350)  
Memory: 456 kB  
CPU: 26.51ms  
CGroup: /system.slice/wazuh-manager.service  
└─[2471] /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/  
  [2473] /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/  
  [2474] /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/  
  [2476] /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/  
  [2480] /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/  
  [2533] /var/ossec/bin/wazuh-integrator  
  [2556] /var/ossec/bin/wazuh-attal  
  [2579] /var/ossec/bin/wazuh-db  
  [2587] /var/ossec/bin/wazuh-execd  
  [2600] /var/ossec/bin/wazuh-syscheckd  
  [2608] /var/ossec/bin/wazuh-syscheckd  
  [2729] /var/ossec/bin/wazuh-remoted  
  [2728] /var/ossec/bin/wazuh-logger  
  [2821] /var/ossec/bin/wazuh-monitored  
  
Jun 12 09:05:01 wazuh-server em[2243]: wazuh-syscheckd: Process 2603 not used  
Jun 12 09:05:02 wazuh-server em[2243]: Started wazuh-syscheckd...  
Jun 12 09:05:02 wazuh-server em[2243]: wazuh-remoted: Process 2704 not used by  
Jun 12 09:05:02 wazuh-server em[2243]: Started wazuh-remoted...  
Jun 12 09:05:02 wazuh-server em[2243]: wazuh-logger: Process 2743 not used by  
Jun 12 09:05:03 wazuh-server em[2243]: Started wazuh-logger...  
[wazuh-user@wazuh-server ~]
```

```
GNU nano 8.3          /var/ossec/etc/rules/local_rules.xml  
<group name="local,syslog,sshd,">  
  <!--  
  Dec 10 01:02:02 host sshd[1234]: Failed none for root from 1.1.1.1 port 1066 >  
  -->  
  <rule id="100001" level="5">  
    <if_sid>5716</if_sid>  
    <srcip>1.1.1.1</srcip>  
    <description>sshd: authentication failed from IP 1.1.1.1.</description>  
    <group>authentication_failed,pci_dss_10.2.4,pci_dss_10.2.5,</group>  
  </rule>  
</group>  
  
<group name="local,netcat">  
  <rule id="100010" level="10">  
    <if_sid>530</if_sid>  
    <match>nclnetcat|ncat,</match>  
    <description>Unauthorized Netcat usage detected</description>  
    <mitre>  
      <id>T1059</id>  
    </mitre>  
    <group>Process_monitoring,unauthorized_process,</group>  
  </rule>  
</group>  
  
^G Help      ^O Write Out   ^F Where Is   ^X Cut        ^T Execute   ^C Location  
^X Exit      ^R Read File  ^P Replace   ^U Paste      ^J Justify  ^L Go To Line
```

CONTINUE ACTIVE STEP

SLACK APP SET UP

- I login to <https://api.slack.com/app>
- I click create a new app {from scratch}
- I selected a slack channels {cyber eagle}
- I was taken to app {besic information},
- I selected {incoming webhook} on the side bar.
- I copy webhook url of {all cyber eagle}.

The image shows two screenshots of the Slack API interface. The top screenshot is a list of apps under 'Your Apps', showing one entry: 'NETAPP' in 'CYBEREAGLE' workspace, App ID 'A091LR73FUL', Modern type, and Not distributed status. The bottom screenshot is a modal dialog titled 'Name app & choose workspace'. It has fields for 'App Name' (set to 'Net APP') and 'Pick a workspace to develop your app in' (set to 'CYBEREAGLE'). Below these are instructions about workspace permanence and a link to sign into a different workspace. At the bottom are 'Cancel' and 'Create App' buttons. To the right of the modal is a sidebar for creating an app, showing sections for 'From a manifest' (using a manifest file to add basic info, scopes, settings, & features), 'From scratch' (using a configuration UI to manually add basic info, scopes, settings, & features), and a curl command example for activating a webhook. The curl command is:

```
curl -X POST -H "Content-type: application/json" --data '{"text': 'Hello, world!'}' https://hooks.slack.com/services/T085C620URK/B914T239R/UKYCmpG2wRXG1kypd83n
```

Buttons for 'Copy' and 'Paste' are shown next to the curl command. Below the curl section is a table for 'Webhook URL', 'Channel', and 'Added By', showing two entries: '#all-cyber-eagle-soc' added by 'Dubem.' on Jun 16, 2025, and another entry for '#all-cyber-eagle-soc' added by 'Dubem.' on Jun 16, 2025. A 'Copy' button is also present here. At the bottom right is a 'Add New Webhook' button.

CONTINUE ACTIVE STEP

UBUNTU SET UP

- I open ubuntu web browser to confirm my agent deployment
- I run the ubuntu terminal
- Restart my wazuh agent by {sudo systemctl restart wazuh agent}
- Install netcat { sudo apt install ncat nmap -y},
- {sudo apt install netcat-traditional} , {sudo ufw enable}, {sudo apt status ufw}
- I open up listening port in ubuntu by running { sudo nc -lvp /bin/bash/}

The image shows two terminal windows side-by-side. Both windows have a title bar 'vboxuser@Ubuntu:~' and a close button 'x'. The left window shows the command history and output of the user's actions:

```
vboxuser@Ubuntu:~$ sudo systemctl start wazuh-agent
[sudo] password for vboxuser:
vboxuser@Ubuntu:~$ sudo systemctl start wazuh-agent
vboxuser@Ubuntu:~$ sudo systemctl restart wazuh-agent
vboxuser@Ubuntu:~$ sudo nano /var/ossec/etc/ossec.conf
vboxuser@Ubuntu:~$ sudo apt install ncat nmap -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
ncat is already the newest version (7.94+git20230807.3be01efb1+dfsg-3build2).
nmap is already the newest version (7.94+git20230807.3be01efb1+dfsg-3build2).
0 upgraded, 0 newly installed, 0 to remove and 104 not upgraded.
vboxuser@Ubuntu:~$ nc -lvp 4444
[listening on 0.0.0.0 4444
^C
vboxuser@Ubuntu:~$ sudo nano /var/ossec/etc/ossec.conf
[sudo] password for vboxuser:
vboxuser@Ubuntu:~$ sudo systemctl restart wazuh-agent
[sudo] password for vboxuser:
vboxuser@Ubuntu:~$ sudo apt uninstall open-ssh
E: Invalid operation uninstall
vboxuser@Ubuntu:~$ sudo apt uninstall ssh
E: Invalid operation uninstall
vboxuser@Ubuntu:~$ sudo systemctl restart wazuh-agent
See 'snap info <snapname>' for additional versions.
vboxuser@Ubuntu:~$ sudo apt install net-tools
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
net-tools
0 upgraded, 1 newly installed, 0 to remove and 104 not upgraded.
Need to get 204 kB of archives.
After this operation, 811 kB of additional disk space will be used.
Get:1 http://gb.archive.ubuntu.com/ubuntu noble-updates/main amd64 net-tools amd64 2.10-0.1ubuntu4.4 [204 kB]
Fetched 204 kB in 0s (567 kB/s)
Selecting previously unselected package net-tools.
(Reading database ... 155508 files and directories currently installed.)
Preparing to unpack .../net-tools_2.10-0.1ubuntu4.4_amd64.deb ...
Unpacking net-tools (2.10-0.1ubuntu4.4) ...
Setting up net-tools (2.10-0.1ubuntu4.4) ...
Processing triggers for man-db (1.12.0-1ubuntu4.2) ...
vboxuser@Ubuntu:~$ run nc -lvp 4444
Command 'run' not found, did you mean:
  command 'rue' from snap darkdimension-rue (1.0.7)
  command 'bun' from snap bun-js (1.2.15)
  command 'grun' from deb grun (0.9.3+git20200303-3)
```

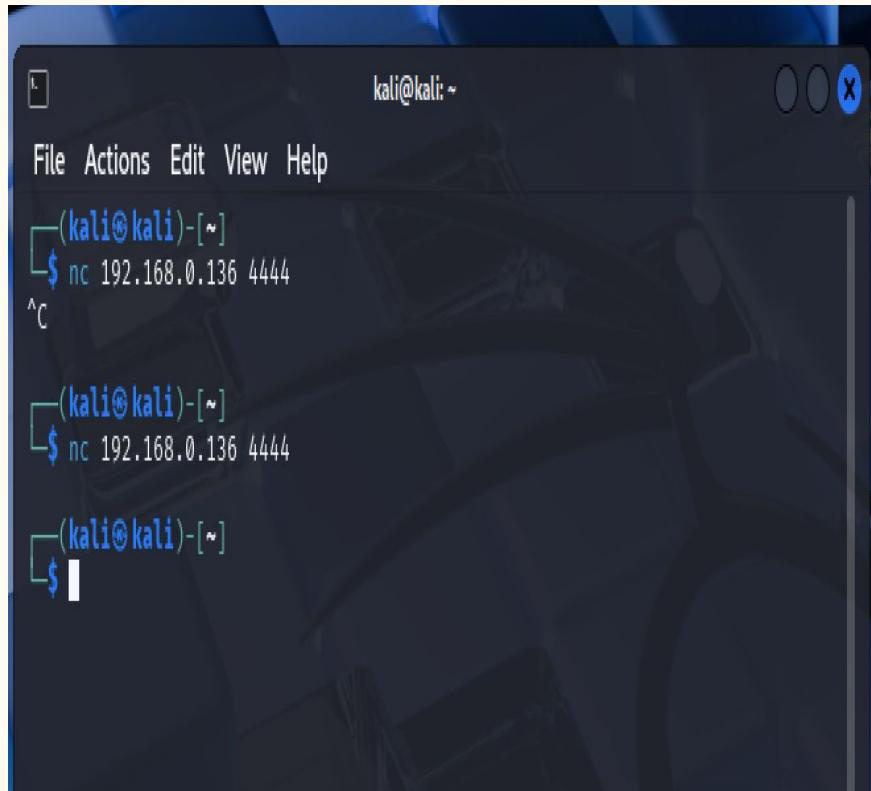
The right window shows the netcat listener being established and receiving a connection:

```
lines 1-9/9 (END)
vboxuser@Ubuntu:~$ sudo systemctl allow 4444
Unknown command verb 'allow', did you mean 'show'?
vboxuser@Ubuntu:~$ sudo ufw allow 4444
Rules updated
Rules updated (v6)
vboxuser@Ubuntu:~$ sudo ufw reload
Firewall not enabled (skipping reload)
vboxuser@Ubuntu:~$ sudo ufw status
Status: inactive
vboxuser@Ubuntu:~$ sudo ufw allow 4444
Skipping adding existing rule
Skipping adding existing rule (v6)
vboxuser@Ubuntu:~$ sudo ufw enable
Firewall is active and enabled on system startup
vboxuser@Ubuntu:~$ sudo nc -lvp 4444
[sudo] password for vboxuser:
Listening on 0.0.0.0 4444
^C
vboxuser@Ubuntu:~$ nc -lvp 4444
Listening on 0.0.0.0 4444
^C
vboxuser@Ubuntu:~$ netstat-tuln | grep 4444
Command 'grep' not found, but can be installed with:
vboxuser@Ubuntu:~$ nc -lvp 4444 /bin/bash
usage: nc [-46CdfhklNnrStuvZz] [-l length] [-i interval] [-M ttl]
          [-m minttl] [-O length] [-P proxy_username] [-p source_port]
          [-q seconds] [-s sourceaddr] [-T keyword] [-V rtable] [-W recvlimit]
          [-w timeout] [-X proxy_protocol] [-x proxy_address[:port]]
          [-destination] [port]
vboxuser@Ubuntu:~$ sudo nc -lvp 4444
Listening on 0.0.0.0 4444
Connection received on 192.168.0.127 50162
vboxuser@Ubuntu:~$ sudo nc -lvp 4444
[sudo] password for vboxuser:
Listening on 0.0.0.0 4444
Connection received on 192.168.0.127 50372
^C
vboxuser@Ubuntu:~$ sudo nc -lvp 4444
[sudo] password for vboxuser:
Listening on 0.0.0.0 4444
Connection received on 192.168.0.127 50959
vboxuser@Ubuntu:~$ sudo nc -lvp 4444
[sudo] password for vboxuser:
Listening on 0.0.0.0 4444
Connection received on 192.168.0.127 51160
^C
vboxuser@Ubuntu:~$
```

CONTINUE ACTIVE STEP

KALI LINUX SETUP

- I open my kali linux
- I signup
- I goto terminal
- Run this command {nc ‘my ubuntu ip address’ 4444} to connect to the my ubuntu that is actively listening.



A screenshot of a Kali Linux terminal window titled '(kali㉿kali)-[~]'. The window has a dark blue background with white text. It shows three separate instances of the 'nc' command running in parallel:

```
$ nc 192.168.0.136 4444
^C
$ nc 192.168.0.136 4444
$ |
```

EXPECTED RESULT

SOME OF THE SLACK MESSAGE RECEIVE.

NET APP APP 13:34
WAZUH Alert

Listened ports status (netstat) changed (new port opened or closed).
ossec: output: 'netstat listening ports':
tcp 0.0.0.0:22 0.0.0.0:* /usr
tcp6 ::22 ::* /usr
udp 10.0.3.15:68 0.0.0.0:* 2178/
systemd-networ
udp 192.168.0.132:68 0.0.0.0:
2178/systemd-networ
Agent
(000) - wazuh-server
Location
netstat listening ports
Rule ID
533 _(Level 7)_
Today at 13:34

Show more

NET APP APP 15:11
WAZUH Alert

Listened ports status (netstat) changed (new port opened or closed).
ossec: output: 'netstat listening ports':
tcp 0.0.0.0:22 0.0.0.0:* /usr
tcp6 ::22 ::* /usr
udp 10.0.3.15:68 0.0.0.0:* 2178/
systemd-networ
udp 192.168.0.132:68 0.0.0.0:
2178/systemd-networ
Agent
(000) - wazuh-server
Location
netstat listening ports
Rule ID
533 _(Level 7)_
Today at 15:11

Show more

Message in #all-cybereagle-soc

NET APP APP Today at 17:27
WAZUH Alert

Unauthorized Netcat usage detected
ossec: output: 'netstat listening ports':
tcp6 ::22 ::* 1/init
tcp 127.0.0.53:53 0.0.0.0:* 429/
systemd-resolve
tcp 127.0.0.54:53 0.0.0.0:* 429/
systemd-resolve
udp 127.0.0.53:53 0.0.0.0:* 429/
systemd-resolve
Agent
(000) - wazuh-server
Location
netstat listening ports
Rule ID
533 _(Level 7)_
Today at 08:16

Show more

NET APP APP Today at 08:16
WAZUH Alert

Listened ports status (netstat) changed (new port opened or closed).
ossec: output: 'netstat listening ports':
tcp 0.0.0.0:22 0.0.0.0:* /usr
tcp6 ::22 ::* /usr
udp 10.0.3.15:68 0.0.0.0:* 2178/
systemd-networ
udp 192.168.0.132:68 0.0.0.0:* 2178/
systemd-networ
Agent
(000) - wazuh-server
Location
netstat listening ports
Rule ID
533 _(Level 7)_
Today at 08:16

Show more

+ Add a reply

EXPECTED RESULT

MY WAZUS THREAT HUNTING EVENT AND DASHBOARD.

The dashboard displays the following key metrics:

- Total alerts: 930
- Level 12 or above alerts: 0
- Authentication failure: 1
- Authentication success: 55

Below these metrics are two charts:

- Top 10 Alert level evolution:** A line chart showing alert counts over time. The Y-axis is "Count" from 0 to 600, and the X-axis is "timestamp per 30 minutes" from 09:00 to 06:00. A legend indicates alert levels: 5 (green), 3 (blue), 7 (red), 9 (purple), and 10 (pink).
- Top 10 MITRE ATT&CKS:** A donut chart showing the distribution of attack techniques. The largest segment is "Valid Accounts" (yellow).

On the right side of the dashboard, there is a detailed log table:

Jun 16, 2025 @ 07:20:22.750 - Jun 17, 2025 @ 07:20:22.750	Export Formatted	645 available fields	Columns	Density	1 fields sorted	Full screen
timestamp	agent.name	rule.description	rule.level	rule.id		
Jun 17, 2025 @ 08:30:57.4...	Ubuntu	Systemd: Service exited due to a failure.	5	40704		
Jun 17, 2025 @ 05:50:01.3...	wazuh-server	Successful sudo to ROOT executed.	3	5402		
Jun 17, 2025 @ 05:50:01.3...	wazuh-server	PAM: Login session opened.	3	5501		
Jun 17, 2025 @ 05:49:53.3...	wazuh-server	PAM: Login session closed.	3	5502		
Jun 17, 2025 @ 05:46:24.9...	wazuh-server	Successful sudo to ROOT executed.	3	5402		
Jun 17, 2025 @ 05:46:24.9...	wazuh-server	PAM: Login session opened.	3	5501		
Jun 17, 2025 @ 05:26:04.2...		Listened ports status (netstat) changed (new port opened or clo...	7	533		
Jun 17, 2025 @ 05:20:08.4...	Ubuntu	Listened ports status (netstat) changed (new port opened or clo...	7	533		
Jun 17, 2025 @ 05:05:33.0...	Ubuntu	Listened ports status (netstat) changed (new port opened or clo...	7	533		
Jun 17, 2025 @ 04:59:32.3...	Ubuntu	Listened ports status (netstat) changed (new port opened or clo...	7	533		
Jun 17, 2025 @ 04:47:31.3...	Ubuntu	Listened ports status (netstat) changed (new port opened or clo...	7	533		
Jun 17, 2025 @ 04:46:57.2...	Ubuntu	Systemd: Service exited due to a failure.	5	40704		
Jun 17, 2025 @ 04:41:35.2...	Ubuntu	Listened ports status (netstat) changed (new port opened or clo...	7	533		
Jun 17, 2025 @ 04:26:50.9...	wazuh-server	SCA summary: CIS Benchmark for Amazon Linux 2023 Benchmark...	7	19004		
Jun 17, 2025 @ 04:26:47.9...	wazuh-server	CIS Benchmark for Amazon Linux 2023 Benchmark v1.0.0: Ensur...	5	19012		

Mitigation Strategies

- **Restrict Netcat:** Remove from non-essential systems (apt-get remove netcat).
- **AppArmor/SELinux:** Restrict execution to authorized users.
- **Network Monitoring:** Add netstat monitoring in ossec.conf.
- **User Training:** Promote secure alternatives (e.g., tcpdump).
- **Incident Response:** Develop playbook for Netcat alerts.

Conclusion

- Enhanced detection and response capabilities for 10ALYTICS-DC.
- Reduced risk of unauthorized access and data breaches.
- Blueprint for future security enhancements.
- Next Steps: Expand monitoring to other tools, integrate with SIEM.