Internship Project 1

Title of the project: Detection of the harassment through email communication and the data exchanged within it using the memory dump.

Description of the project:

If the system gets compromised and the Hacker stole a lot of information but he/she also deleted a very important file of the victim. The data should be recovered using the memory dump of victim machine.
Also perform the network forensics to get analysis the email.

Domain of the project: Digital forensics (Memory)

Expected Outcome: Clearly define the outcome of the project such as, POC of the problem stated, desired documents (One detailed document of step-by-step execution process, ppt and project report).

Note: **Format for the documents to be provided to the interns will be prepared and shared with you.**

Suggested tools/techniques to be used:

Volatility

Wireshark

Ram Capturer

FTK Imager

Email Tracer

Learning resources/links for understanding the problem and solution:

https://mmox.me/posts/writeups/memlabs-lab4/

Internship Project 2

Title of the project: Detection of the data theft and recovery of the data using the memory dump.

Description of the project:

Received this memory dump from the victim. Evidence might hold some secrets of the malicious activity. Your job is to go through the memory
Dump and find out the information about the stolen data from the machine. If there was any malware installed to steal the data or manually steal project should find out both.
The project should also detect the anti-forensics techniques such as password protected files, signature mismatch, encrypted files, stegnographed files, signature mismatched files, overwritten files etc. and able to recover them successfully using the set of open source tools and techniques.

Domain of the project: Digital forensics (Disk Forensics)

Expected Outcome: Clearly define the outcome of the project such as, POC of the problem stated, desired documents (One detailed document of step-by-step execution process, ppt and project report).

Note: **Format for the documents to be provided to the interns will be prepared and shared with you.**

Suggested tools/techniques to be used:

Volatility

Autopsy

FTK Imager

CyberCheckSuite

Win-Lift

Win Hex

Learning resources/links for understanding the problem and solution:

https://github.com/shadawck/awesome-anti-forensic

http://www.cyberforensics.in/

Internship Project 3

Title of the project: DNS Performance Measurement Tool with record Lookups

Description of the project: This project aims to develop a tool that measures the performance of Domain Name System (DNS) lookups for various record types, supporting both single and multiple domain name inputs.

Domain of the project: Networking

Expected Outcome: A functional tool that performs DNS lookups for user-specified domain names and record types (e.g., A, MX, CNAME).

* Measurement and display of key performance metrics like lookup time, response time, and server location for each record type.
* Ability to handle both single and multiple domain name inputs for efficient batch analysis.
* (Optional) Visualization of results for easier interpretation (e.g., bar charts).

Suggested tools/techniques to be used:

*DNS Lookup Libraries: Utilize libraries specifically designed for DNS interactions.
*Command-Line Interface (CLI) - ZDNS Tool
or Graphical User Interface (GUI):

Learning resources/links for understanding the problem and solution:

1.https://mxtoolbox.com

2.https://www.nslookup.io

3. https://github.com/zmap/zdns#GeneratedCaptionsTabForHeroSec

4.https://blog.apnic.net/2023/03/22/zdns-a-fast-dns-toolkit-for-internet-measurement

Internship Project 4

Title of the project: Unveiling the Cracks: Exploring Data Leaks in Mobile and Desktop Applications

Description of the project: This project delves into the critical issue of data leaks in mobile and desktop applications. You'll explore the various ways data leaks occur, their potential consequences, and techniques for identifying and mitigating these vulnerabilities.

Domain of the project: Application Security

Expected Outcome:

*Enhanced Awareness: Gain a comprehensive understanding of common data leaks in mobile and desktop applications.

*Risk Assessment:Identify potential data leaks within applications you use and develop strategies to minimize risks.

*Security Advocacy: Develop communication skills to raise awareness about data leaks among mobile and desktop application users.

*Technical Understanding (Optional): Explore techniques for static and dynamic analysis of mobile and desktop applications to identify vulnerabilities (requires some programming knowledge).

Suggested tools/techniques to be used:

*Mobile App Analysis Tools: Utilize tools like Androguard (Android) or Hopper (iOS) to analyze mobile applications for potential data leaks (requires some technical expertise).

* Desktop Application Analysis Tools:Consider tools like IDA Pro or Ghidra to analyze desktop applications for vulnerabilities (advanced technical knowledge required).

* Open-Source Code Review: If applications are open-source, contribute to code reviews to identify potential data leaks in the source code.

* Privacy Policy Review Analyze the privacy policies of applications to understand their data collection practices and potential leak risks.
*Penetration Testing Techniques (Optional): For advanced users, explore penetration testing methodologies to simulate real-world attacks and identify data leakage vulnerabilities.

Learning resources/links for understanding the problem and solution:
*OWASP Mobile Top 10:
https://owasp.org/www-project-mobile-app-security/](https://owasp.org/www-project-mobile-app-security/

*OWASP Top 10:
https://owasp.org/www-project-top-ten/

*National Institute of Standards and Technology (NIST)Cybersecurity Framework: https://www.nist.gov/cyberframework

*Androguard (Android App Analysis Tool):
https://github.com/androguard/androguard

*Hopper (iOS App Analysis Tool): https://www.hopperapp.com/)

*IDA Pro (Reversing Tool):** https://hex-rays.com/

*Ghidra (Reversing Tool): https://ghidra-sre.org/

*Additional Considerations:

*Contextualize Data Leaks: Consider the type of data leaked (personal information, financial data, etc.) and its potential impact on users.

*Responsible Reporting: If you identify a data leak in a third-party application, report it responsibly to the developers following their vulnerability disclosure policy.
* User Education:* Develop educational materials or presentations to raise awareness about data leaks and encourage users to be more cautious about the applications they install and the data they share.

By delving into this project, you'll gain valuable knowledge about data leaks in mobile and desktop applications. This knowledge empowers you to protect

your own data, advocate for secure application development practices, and contribute to a more secure digital environment. Remember, continuous learning and adaptation are crucial in the ever-evolving landscape of cybersecurity.

Internship Project 5

Title of the project: Linux Guardian: Nagios-Powered Host Monitoring

Description of the project: The purpose is to provide comprehensive monitoring and management of Linux hosts using Nagios. This includes real-time monitoring of system metrics, services, and applications running on Linux servers to ensure optimal performance, availability, and security. Nagios facilitates proactive detection of issues and helps administrators respond promptly to potential problems, thereby enhancing the stability and reliability of Linux-based infrastructure.

Domain of the project: It comes under the domain of **Security Operations** in cybersecurity. It related to monitoring, detection, analysis, and response to security incidents and threats in order to maintain the security posture of systems and networks.

Expected Outcome: Nagios provides real-time monitoring. Monitoring Publicly Available Services like:

- Monitoring HTTP
- Monitoring SSH
- Monitor agent version
- Monitor/Check NCPA agent version

Suggested tools/techniques to be used: Nagios in linux

Learning resources/links for understanding the problem and solution:

- https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/4/en/quickstart.html
- https://support.nagios.com/forum/viewtopic.php?t=8866
- https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/4/en/monitoring-publicservices.html

Internship Project 7

Title of the project: Optimizing Web Server Performance: Implementing Reverse Proxy with Nginx for Apache Integration.

Description of the project: Nginx as a reverse proxy server in front of Apache, a popular web server. Nginx acts as an intermediary, receiving client requests and then forwarding them to Apache for processing. This setup offers several benefits, including improved performance, enhanced security, and efficient resource utilization. For example, Nginx can handle static content delivery and caching, offloading these tasks from Apache and reducing its workload.

Domain of the project: It will mention the security domain, such as Web Security or Web Server Security etc.

Expected Outcome: When accessing Nginx through a web browser, the content displayed originates from Apache, as Nginx acts as a reverse proxy, seamlessly serving Apache's web content.

Suggested tools/techniques to be used: Nginx and Apache2

Learning resources/links for understanding the problem and solution:

- https://ioflood.com/blog/how-to-set-up-nginx-as-a-reverse-proxy-for-apache/#Benefits_of_Using_Nginx_Reverse_Proxy_with_Apache
- https://www.techrepublic.com/article/how-to-use-nginx-as-a-reverse-proxy-for-apache/

Internship Project 8

Title of the project: Securing Windows Networks: Harnessing the Power of Snort for Intrusion Detection.

Description of the project: Snort on Windows works like a digital watchdog for your network. It watches the traffic flowing through your Windows system's network card. When it sees something suspicious, like a hacker trying to break in or a virus spreading, it raises an alert.

First, it examines the incoming and outgoing data packets, looking for patterns that match known threats. Then, if it detects something fishy, it can either log the event for review or take immediate action to block the suspicious traffic.

It uses a set of rules, like a set of instructions, to decide what's normal and what's not. These rules can be customized to fit the specific needs of your network.

Overall, Snort helps keep your Windows network safe from intruders and malware by acting as a vigilant guardian, always on the lookout for anything out of the ordinary.

Domain of the project: The project focusing on the implementation and utilization of Snort on Windows systems falls under the domain of **Network Security**. Specifically, it relates to the field of **Intrusion Detection and Prevention Systems (IDPS)**.

Expected Outcome: Analyse network traffic, identifies and alerts on suspicious activity or potential security threats, helping to protect Windows-based systems from cyber-attacks and unauthorized access.

Suggested tools/techniques to be used: Snort in Window

Learning resources/links for understanding the problem and solution:

- https://www.snort.org/
- https://zaeemjaved10.medium.com/installing-configuring-snort-2-9-17-on-windows-10-26f73e342780

Internship Project 9

Title of the project: Exploring Cyber Deception: Implementing Cowrie Honeypots to emulate a vulnerable source shell.

Description of the project: Cowrie is a high-interaction honeypot designed to log SSH by attackers. This allows the collection of comprehensive information about an attacker's activities. By design, honeypots are meant to be probed, attacked, and potentially compromised. Their primary purpose is not to provide real services, but to gather information about the behaviour of attackers.

Domain of the project: It will mention the security domain, Cyber Defense and Deception in cybersecurity and etc.

Expected Outcome: Cowrie honeypot design to emulate a vulnerable SSH(source shell).

Suggested tools/techniques to be used: Cowrie honeypot

Learning resources/links for understanding the problem and solution:

- https://medium.com/@jeremiedaniel48/install-and-setup-cowrie-honeypot-on-ubuntu-linux-5d64552c31dc

Internship Project 10

Title of the project: Securing Apache Server Using ModSecurity open source web application firewall.

Description of the project: Securing Apache Server with ModSecurity involves deploying an open-source web application firewall (WAF) to protect against various online threats. ModSecurity works as a shield between the server and the internet, inspecting incoming traffic and filtering out malicious requests or payloads. Through customizable rulesets, it helps to mitigate common web-based attacks such as SQL injection, cross-site scripting (XSS), and remote file inclusion (RFI), bolstering the overall security posture of Apache servers.

Domain of the project: It will mention the security domain, such as web application security, network security, end point security, etc.

Expected Outcome: Using ModSecurity WAF with the OWASP core rule set helps protect your server from common cyber threats like local file inclusion attacks, SQL injection attacks/ cross-site scripting attacks.

Suggested tools/techniques to be used: ModeSecurity open source web application firewall

Learning resources/links for understanding the problem and solution:

- https://medium.com/codelogicx/securing-apache-server-using-modsecurity-oswaf-d29664179a05

Internship Project 11

Title of the project: Domain name analysis of an organisation and an email address using Information gathering OSINT tools.

Description of the project: This project is centered around gathering information about domain names. In today's digital landscape, where fraudulent websites abound, it's imperative to discern between genuine and counterfeit ones. Additionally, we aim to ascertain the various platforms where our email address is registered, enhancing our understanding of its digital footprint.

Domain of the project: It will mention the security domain and Digital footprint and Reconnaissance.

Expected Outcome:

- Grab some information regarding the domain name. Identify that this is real or fake. If not then grab information with valid proof using Spiderfoot and Netlas. Example: cdacgujarat.com (or use any domain name as per your choice.)
- Retrieve platform usage information associated with any given email address using spiderfoot.
- Also use other features of spiderfoot to grab some information. Like IPv4 address, Human name, username etc.

Suggested tools/techniques to be used: Spiderfoot, Netlas and use some other tools for domain name analysis(as per of your choice).

Learning resources/links for understanding the problem and solution:

- https://github.com/smicallef/spiderfoot
- https://netlas.io/

Internship Project 12

Title of the project: Information gathering of user's phone number using open source intelligence tools.

Description of the project: In today's landscape, we receive numerous unknown calls daily, disrupting workflow and occasionally posing as scams. To address this challenge, we employ the reconnaissance process, focusing on gathering information through phone numbers. By leveraging this approach, we aim to identify and mitigate potential risks associated with these calls, ensuring a more secure and uninterrupted work environment.

Domain of the project: It falls under the category of reconnaissance and OSINT tools, specifically associated with digital footprint.

Expected Outcome:

- The primary objective is to accurately identify user information, including name, gender, profile picture, city, email address, and the associated company name linked to the user's phone number registration. This aims to provide comprehensive caller identification and enhance user experience by offering valuable insights into incoming calls.
- Now that all the above information has been gathered, utilize it to acquire further details about the user. Like using the email address find the other digital footprint of user like geo-location and more.

Suggested tools/techniques to be used: Truecallerjs (phone number information gathering tool), phoneinfoga (phone number information gathering tool), epieos (give information related to email address and phone numbers) and use other tools also as per your requirements.

Learning resources/links for understanding the problem and solution:

- https://github.com/sumithemmadi/truecallerjs
- https://epieos.com/

Internship Project 13

Title of the project: Intrusion Detection System using open source HIDS and monitored with open source monitoring tool.

Description of the project: This project will focus on log analysis. Organizations require robust solutions to safeguard against unauthorized access, malware infections, and other malicious activities. By providing real-time alerts, log analysis, and file integrity monitoring, OSSEC strengthens security postures and fortifies defences against cyberattacks.

Domain of the project: It will be related to the network security domain, such as Security Information and Event Management (SIEM), Host-based Intrusion Detection Systems (HIDS), application performance monitoring (APM).

Expected Outcome: The main goal is log analysis of File Integrity Management and Detection SSH brute-force attack through Ossec. The outcomes will show in Splunk precisely.

Suggested tools/techniques to be used: Ossec (open source HIDS) and Splunk (open source monitoring tool).

Learning resources/links for understanding the problem and solution:

- https://www.digitalocean.com/community/tutorials/how-to-monitor-ossec-agents-using-an-ossec-server-on-ubuntu-14-04
- https://www.splunk.com/en_us/resources/videos/installing-splunk-enterprise-on-linux.html