NIST-Based Security Requirements

## Introduction

This document outlines the security requirements for a honeypot hosting environment. The security measures are based on guidelines provided by the National Institute of Standards and Technology to ensure the confidentiality, integrity, and availability of the honeypot and its data.

# System Overview

## **The honeypot hosting environment comprises the following components:**

Honeypot Systems: Simulated vulnerable systems or services designed to attract malicious actors.

## **Network Infrastructure:**

Networking components are responsible for directing and monitoring traffic to and from the honeypot systems.

## **Security Tools:**

Intrusion detection and prevention systems, logging mechanisms, and other security tools for monitoring and analyzing activity within the honeypot environment.

# Network Security

## **Traffic Monitoring:** NIST SP 800-41 (Guidelines on Firewalls and Firewall Policy) and SP 800-83 (Guide to Malware Incident Prevention and Handling).

Monitor all network traffic to and from the honeypot environment using intrusion detection systems (IDS) and intrusion prevention systems (IPS).

Analyze network traffic patterns to detect and respond to malicious activity.

## **Data Protection:** (NIST SP 800-53 requirements: DS-2 (Data-at-Rest Encryption) and DS-5 (Denial of Service Protection))

Use dummy data within the honeypot environment to simulate real systems and services without risking actual sensitive data.

Protect any sensitive data stored within the honeypot systems to prevent unauthorized access.

## **Data Logging:** (NIST SP 800-92 (Guide to Computer Security Log Management))

Comprehensive logging of all activity within the honeypot environment, including network traffic, system events, and user interactions.

Store logs securely and analyze them regularly to identify suspicious behaviour.

## **Isolation:** (NIST SP 800-53 requirement AC-17 (Remote Access) and AC-20 (Use of External Information Systems).

Isolate the honeypot environment to prevent unauthorised access to critical infrastructure hosting the honeypot.

Implement network segmentation to restrict communication between the honeypot environment and other network segments.

## **Configuration Management**:(NIST SP 800-53 requirement CM-2 (Baseline Configuration) and CM-6 (Configuration Settings))

Harden the configuration of honeypot systems to minimize potential attack surfaces outside the scope.

Disable unnecessary services and protocols to reduce the risk of abuse outside the scope.

## **Event Logging:** (NIST SP 800-53 requirement AU-2 (Auditable Events) and AU-6 (Audit Review, Analysis, and Reporting))

Implement logging to capture all security events within the honeypot environment.

Centralised log collection and analysis using a Security Information and Event Management (SIEM) system.

## **Incident Response:** (NIST SP 800-61 (Computer Security Incident Handling Guide))

Develop an incident response plan for the honeypot environment.

Create procedures for responding to security incidents detected within the honeypot.

# Software and applications

HoneyPot Software:

**Cowrie**: An SSH/Telnet honeypot designed to log brute force attacks and the shell interaction performed by the attacker.

**Honeypot-ftp:** An FTP honeypot that can catch used credentials, and malware files.

**Webserver:** A web serverhoneypot we will setup that allows webpage attacks such as SQL injection or XSS attacks which we will monitor and catch

Networking Tools:

**Suricata:** An open-source network intrusion detection system that can be configured to detect specific types of attacks or behaviours.

**Wazuh:** An open-source network intrusion detection system that can be configured to detect specific types of attacks or behaviours. It combines the functionality of intrusion detection, log management, file integrity monitoring, and security information and event management.

**Pfsense:** pfSense is an open-source firewall and router software distribution based on FreeBSD. It provides advanced features typically found in expensive, commercial firewall solutions, making it a popular choice for both home and enterprise environments.

**Logging and Analysis Tools:**

**Log-stash:** an open-source data processing pipeline that ingests, processes, and forwards logs and other event data from various sources to a centralized repository or analytics platform.

**Wazuh-agent:** part of wazuh it allows system information to be shipped to a wazuh server, where the data can be processed to give a graphical overview it is mainly used in HIDS

**Operating Systems:**

**FreeBSD:** This is a free and open source OS that is mainly used by our pfsense routers and will allow us to control the flow of traffic through our Network.

**Linux:** this is also a free and open-source OS that we will use as the backbone to host all of our applications such as all the Honey Pot software and be the backbone of the docker environment that we will be hosting.

# Threats

**Scanning and Reconnaissance:**

Attackers tend to perform scanning and other reconnaissance techniques to identify targets and vulnerabilities. They can scan the entire network and find open ports and services or vulnerabilities. Now of course this is a honeypot and the point is that we expect them to do this but a misconfiguration in the honeypot or not fully secured could result in unexpected exploitation from the attackers

**Command and Control (C2) Communication:**

If the honeypot is configured to emulate vulnerable services or systems, attackers may attempt to establish command and control communication with it. This could involve sending commands to the honeypot to perform actions or exfiltrate data.

**Distributed Denial of Service (DDoS) Attacks:**

Attackers could target the honeypot with DDoS attacks to disrupt its operations by flooding the honeypot with excessive traffic or exploiting vulnerabilities to overwhelm its resources.

**Evasion Techniques:**

Attackers could use techniques to avoid detection by the honeypot. This could include obfuscating their actions or using other tactics to evade detection mechanisms implemented in the honeypot.

**Exploitation:**

Once attackers identify potential vulnerabilities through scanning, they may try to exploit them. This could involve launching exploits against known vulnerabilities in services running on the honeypot, such as web servers, FTP servers, or database servers.

# CIA threat table

Confidentiality, Integrity, and Availability are rated from 1 (low) to 3 (high) based on the impact each threat has on these aspects of security.

Likelihood and Impact are rated from 1 (low) to 3 (high) based on the probability of the threat occurring and the severity of its consequences.

Risk Rating is calculated by multiplying the Likelihood and Impact scores. A score of 3 indicates the highest risk.

Scanning and Reconnaissance:

Confidentiality (2): Moderate risk as attackers may gain insights into network topology and potential vulnerabilities.

Integrity (2): Moderate risk as attackers may exploit vulnerabilities, leading to unauthorized modifications.

Availability (1): Relatively low risk as scanning activities typically do not directly impact service availability.

Command and Control (C2) Communication:

Confidentiality (2): Moderate risk as interception or compromise of C2 traffic could reveal sensitive information.

Integrity (3): Higher risk as unauthorized modification of C2 communication could lead to unintended actions on compromised systems.

Availability (3): Significant risk as disruption of C2 communication channels can impede attackers' control over compromised systems.

Distributed Denial of Service (DDoS) Attacks:

Confidentiality (1): Relatively low risk as DDoS attacks primarily target availability rather than confidentiality.

Integrity (2): Moderate risk as DDoS attacks can indirectly impact data integrity by disrupting system operation.

Availability (3): Significant risk as DDoS attacks aim to disrupt or degrade service availability for legitimate users.

Evasion Techniques:

Confidentiality (1): Relatively low risk as evasion techniques generally do not directly target confidentiality.

Integrity (2): Moderate risk as evasion techniques may attempt to manipulate system configurations or traffic, leading to unauthorized modifications.

Availability (2): Moderate risk as certain evasion techniques may consume system resources or disrupt network communication, impacting service availability.

Exploitation:

Confidentiality (2): Moderate risk as successful exploitation of vulnerabilities may lead to unauthorized access to sensitive information.

Integrity (3): Higher risk as exploitation may result in unauthorized modifications or compromise of system integrity.

Availability (2): Moderate risk as exploitation may lead to system crashes or service interruptions, impacting availability.

| Threat | Confidentiality | Integrity | Availability | Likelihood | Impact | Risk  Rating |
| --- | --- | --- | --- | --- | --- | --- |
| Scanning and Reconnaissance | 2 | 2 | 1 | 3 | 2 | 3 |
| Command and Control (C2) Communication | 2 | 3 | 2 | 2 | 3 | 3 |
| Distributed Denial of Service (DDoS) Attacks | 1 | 2 | 3 | 2 | 3 | 3 |
| Evasion Techniques | 1 | 2 | 2 | 2 | 2 | 2 |
| Exploitation | 2 | 3 | 2 | 3 | 3 | 3 |