**Evading IDS, Firewalls, and Honeypots**

**Intrusion detection system (IDS):**

An Intrusion Detection System (IDS) is a security tool that monitors network traffic and devices for malicious activity or policy violations. It helps detect unauthorized access, potential threats, and abnormal activities by analysing traffic and alerting administrators to take action.

IDS is crucial for maintaining network security and protecting sensitive data from cyber-attacks.

**How an IDS works?**

An Intrusion Detection System (IDS) works by monitoring network traffic and system logs for suspicious activity. It typically uses three main detection methods:

**Signature-based detection:** This method compares network traffic to a database of known attack signatures. If a match is found, the IDS raises an alert.

**Anomaly-based detection:** This method establishes a baseline of normal network behaviour and flags any significant deviations as potential threats. It uses statistical analysis or machine learning techniques to identify anomalies.

**Protocol Anomaly Detection:** Here the models are built to explore anomalies in the way in which vendors deploy the TCP/IP specification.

Here's a simplified breakdown of how an IDS works:

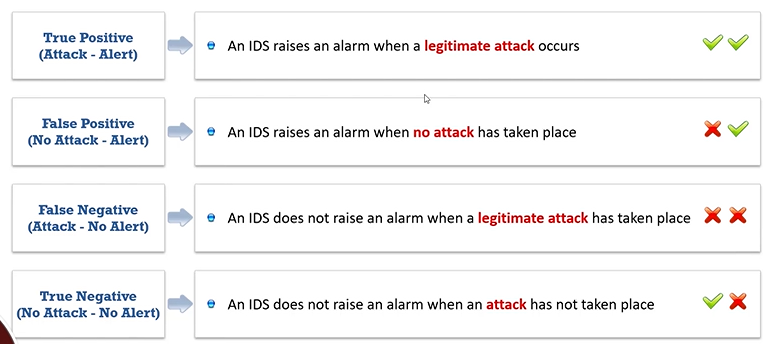
1. **Monitoring:** The IDS continuously monitors network traffic and system logs.
2. **Analysis:** It analyzes the collected data using signature-based or anomaly-based techniques.
3. **Detection:** If suspicious activity is detected, the IDS generates an alert.
4. **Alerting:** Alerts can be sent to security administrators via email, SMS, or other notification methods.

Some advanced IDS systems can also take automated actions, such as blocking malicious traffic or isolating compromised systems.

**Types of IDS:**

1. **Network-Based Intrusion Detection Systems**: These systems typically consist of a black box that is placed on the network in a promiscuous mode, listening for patterns indicative of an intrusion. It detects malicious activity such as Denial-of-Service attacks, port scans, or even attempts to crack into computers by monitoring network traffic.
2. **Host-Based Intrusion Detection Systems**: These systems usually include auditing for events that occur on a specific host. These are not as common, due to the overhead they incur by having to monitor each system event.

**Types of IDS Alerts:**

****

**Intrusion prevention system:**

An IPS is also considered as an active IDS since it is capable of not only detecting the intrusions but also preventing them. These are continuous monitoring system that often sits behind the firewalls as an additional layer of protection.

**IDS vs IPS:**

**Response to Threats:**

* **IDS:** Detects and alerts about potential threats but does not take any action to block or mitigate them.
* **IPS:** Detects threats and actively blocks or mitigates them in real-time, preventing malicious traffic from reaching its intended target.

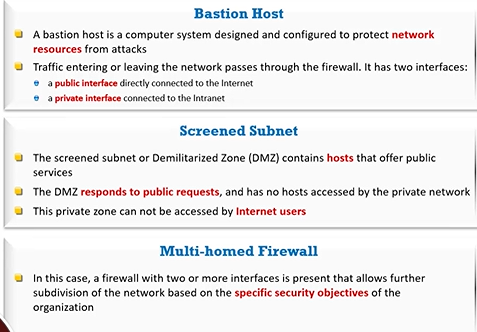
**Impact on Network Performance:**

* **IDS:** Has minimal impact on network performance as it only monitors traffic.
* **IPS:** Can significantly impact network performance due to its active inspection and blocking of traffic.

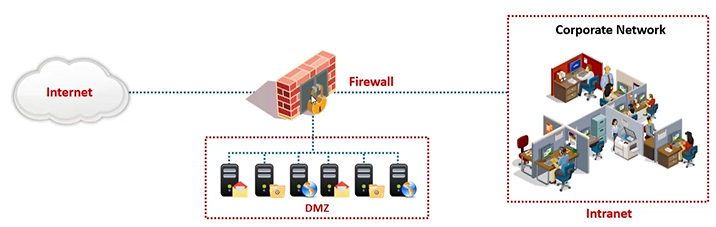
**Firewall:**

* Firewalls are hardware and/or software designed to prevent unauthorized access to or from a private network.
* They are placed at the junction or gateway between two networks, which is usually between a private network and a public network such as the Internet.
* Firewalls examine all messages entering or leaving the Intranet (or private network) and block those that do not meet the specified security criteria.

**Firewall Architecture:**

****

**Demilitarized Zone:**

****

It is a network that serves as a buffer between the internal secure network and the insecure network. It can be created using a firewall with three or more network interfaces, assigned with specific roles such as the internal trusted network, the DMZ network, and the external un-trusted network.

**Types of Firewalls:**

1. **Hardware Firewalls**: These are physical devices that sit between a network and its external connections. They filter incoming and outgoing traffic based on predefined security rules. Hardware firewalls provide robust protection for larger networks, offering features like NAT, VPN support, and more, typically managed by IT professionals.
2. **Software Firewalls**: These are programs installed on individual devices to monitor and control network traffic. They provide customizable protection for computers or servers, blocking harmful traffic based on rules set by the user. Software firewalls are commonly used for personal security on endpoints, offering flexibility and ease of use.

**Honeypot:**

1. **What is a honeypot?** A honeypot is a decoy system or network designed to attract cyberattacks, mimicking real systems to deceive attackers. It acts as a trap, collecting data on attack methods, providing insight into vulnerabilities, and luring malicious activity away from actual targets, enhancing cybersecurity monitoring.
2. **How it works?** Honeypots work by simulating vulnerable systems, attracting attackers with seemingly unprotected services. When an attacker interacts with the honeypot, it records their actions, enabling security teams to analyse attack patterns and learn about new threats. It can also isolate the attacker, preventing harm to real systems.
3. **Advantages**  
   Honeypots provide valuable insights into attack methods, helping organizations understand evolving threats. They can divert attackers from critical systems, enhance threat detection, and improve incident response strategies. By simulating vulnerabilities, they allow for proactive security measures without compromising real assets.
4. **Disadvantages**  
   Honeypots can be resource-intensive, requiring maintenance and monitoring. If not properly isolated, they risk becoming a launchpad for further attacks. Skilled attackers may recognize honeypots and avoid them. Additionally, their presence can potentially attract unwanted attention or increased targeting of an organization's infrastructure.

**Intrusion Detection:**

**Intrusion Detection** refers to the process of monitoring network or system activities for malicious activities or security breaches. It involves identifying unauthorized access, misuse, or violations of security policies. Intrusion detection systems (IDS) analyse traffic patterns, logs, and system behaviour to detect potential threats and alert administrators for further investigation.

**Intrusion Detection Tools: Snort**

It is an open-source network intrusion detection system, capable of performing real-time traffic analysis and packet logging on IP networks.

Uses:

* Straight packet sniffer like tcpdump
* Packet logger
* Network intrusion prevention system

**Snort Rules:**

1. Snort's rule engine allows custom rules to be established to meet the needs of the network
2. Snort rules help in differentiating between normal Internet activities and malicious activities
3. Snort rules must be contained on a single line; the Snort rule parser does not handle rules on multiple lines
4. Snort rules come with two logical parts:
   * Rule header: Identifies the rule's actions, such as alert, log, pass, activate, and dynamic
   * Rule options: Identifies the rule's alert messages

**IDS Evasion Techniques:**

1. **Packet Fragmentation**: Attackers break malicious data into smaller packets to bypass IDS detection, which may not reassemble fragmented packets for inspection.
2. **Encryption/Obfuscation**: Malicious traffic is encrypted or obfuscated to hide its true nature, making it difficult for IDS to analyze content.
3. **Polymorphic/Metamorphic Malware**: Malware is altered in form or structure with each attack, making it harder for signature-based IDS to detect it.
4. **Tunneling**: Attackers encapsulate malicious traffic within a legitimate protocol (e.g., HTTP or DNS) to bypass IDS filters.
5. **Session Splicing**: Malicious traffic is split across multiple sessions to evade detection, preventing IDS from recognizing patterns indicative of an attack.
6. **Traffic Padding**: Attackers insert irrelevant or padded data into packets to confuse IDS systems and mask malicious activities.
7. **Spoofing**: Attacker impersonates a trusted source (IP address or MAC address), bypassing IDS checks that rely on identifying source authenticity.
8. **Denial of Service (DoS) Flooding**: Attackers overwhelm an IDS with excessive traffic, causing it to miss or fail to process malicious packets.
9. **Timing Attacks**: Malicious payloads are sent in bursts or with delays, aiming to evade detection by confusing IDS monitoring intervals or thresholds.
10. **Protocol Abuse**: Attackers exploit weaknesses in certain protocols (e.g., HTTP, DNS) to disguise their attack and evade IDS detection.

**Insertion attack and Evasion:**

| **Point** | **Insertion Attack** | **Evasion Attack** |
| --- | --- | --- |
| **Definition** | Insertion attacks involve adding malicious data into the communication flow, targeting the IDS or security system. | Evasion attacks aim to bypass or deceive security systems, such as IDS, without triggering alarms. |
| **Objective** | The goal is to insert malicious data that will be detected by security mechanisms. | The goal is to avoid detection by manipulating or disguising the malicious traffic. |
| **Method** | Involves inserting harmful payloads, like false traffic or malicious packets, into legitimate traffic. | Involves manipulating traffic to evade detection, often by using fragmentation or encryption. |
| **Impact on IDS** | IDS might detect and flag the inserted malicious data as a threat. | IDS fails to detect the attack, as the malicious traffic is disguised or fragmented. |
| **Common Example** | Sending malicious payloads in HTTP headers or network packets. | Using encryption, fragmentation, or obfuscation to hide malicious activity within legitimate traffic. |

**Obfuscating and False positive generation:**

| **Point** | **Session Splicing** | **Unicode Evasion** |
| --- | --- | --- |
| **Definition** | Session splicing involves breaking an attack into smaller parts across multiple sessions to bypass IDS detection. | Unicode evasion uses Unicode encoding to obscure malicious payloads, making them harder to detect by security systems. |
| **Objective** | The goal is to evade detection by splitting malicious data over several packets or sessions, making it less recognizable as an attack. | The goal is to obfuscate the payload by using Unicode characters to hide malicious content within seemingly harmless text. |
| **Method** | Attackers fragment a single attack into smaller pieces and send them across multiple sessions, often exploiting protocol weaknesses. | Malicious payloads are encoded using Unicode characters (e.g., UTF-8 or UTF-16) to mask harmful content within legitimate-looking data. |
| **Impact on IDS** | IDS may fail to detect the attack as it spans multiple sessions, lacking enough context to identify it as malicious. | IDS may fail to decode the Unicode characters properly, leading it to miss the malicious payload hidden within the encoded data. |
| **Example** | An attacker sends parts of an exploit over different HTTP requests, preventing the IDS from recognizing it as a complete attack. | An attacker uses Unicode encoding to represent SQL keywords (e.g., "SELECT" or "DROP") in a way that avoids detection by IDS/IPS systems. |

**Overlapping Fragments:**

**Overlapping Fragments** refer to a technique used in network attacks where malicious data is fragmented into smaller packets, and the fragments overlap with one another. This means that parts of the same data are included in multiple fragments, which can confuse or bypass network security systems like Intrusion Detection Systems (IDS) or firewalls.

**How It Works:**

* When an attacker sends fragmented packets, each fragment contains part of the malicious payload.
* In the case of overlapping fragments, the data from one fragment might overlap with the data from the next, creating ambiguity.
* This can trick security devices into not properly reconstructing the entire packet or interpreting the payload incorrectly.

**Why It’s Used:**

* **Evasion**: Overlapping fragments can be used to evade detection, as security systems might fail to reassemble the fragments correctly or identify the malicious payload.
* **Bypassing Security Filters**: Some firewalls and IDS systems may not handle overlapping fragments properly, allowing the attack to bypass defences.

**TTL attacks:**

Time-to-Live (TTL) attacks exploit the TTL value in network packets, which determines how long a packet can exist in a network before being discarded. Attackers manipulate TTL values to evade detection, cause network congestion, or redirect traffic. TTL attacks can disrupt routing, perform denial-of-service (DoS) attacks, or bypass security filters by masking the packet's origin.

**Application-layer Attacks:**

Applications accessing media files (audio, video and images) compress them to a smaller size for maximizing the data transfer rate

* The IDS cannot verify the signature of the compressed file format
* This enables an attacker to exploit the vulnerabilities in compressed data
* The IDS can recognize conditions favourable for attack, but alternative forms of attack are also possible, for example, various integer values can be used to exploit integer overflow vulnerabilities
* This makes the detection of attack traffic extremely difficult at the IDS

**Other types of Evasion:**

1. Encryption: When the attacker has already established an encrypted session with the victim, it results in the most effective evasion attack.
2. Flooding: The attacker sends loads of unnecessary traffic to produce noise, and if the IDS does not analyze the noise traffic well, then the true attack traffic may go undetected.

**Detecting Honeypots:**

**Honeypots** are decoy systems or networks designed to attract cyber attackers and divert them from valuable targets. They simulate vulnerabilities to gather intelligence about attack methods, tactics, and tools.

**Why they are used:**

* To monitor and study attacker behavior.
* To distract and delay attackers from real systems.
* To gather evidence for improving cybersecurity defenses.

**Advantages:**

* **Threat intelligence:** Provides insight into attack methods and vulnerabilities.
* **Early detection:** Helps identify new exploits and threats.
* **Distraction:** Diverts attackers from real systems, reducing risks.
* **Resource optimization:** Can be set up as low-cost, high-value research tools.

**Disadvantages:**

* **Resource-intensive:** Requires management and maintenance.
* **False sense of security:** May lead to overconfidence in defenses.
* **Attracts attackers:** If discovered, a honeypot might increase targeted attacks on the network.
* **Risk of compromise:** Can be used as a launch point for further attacks if misconfigured.

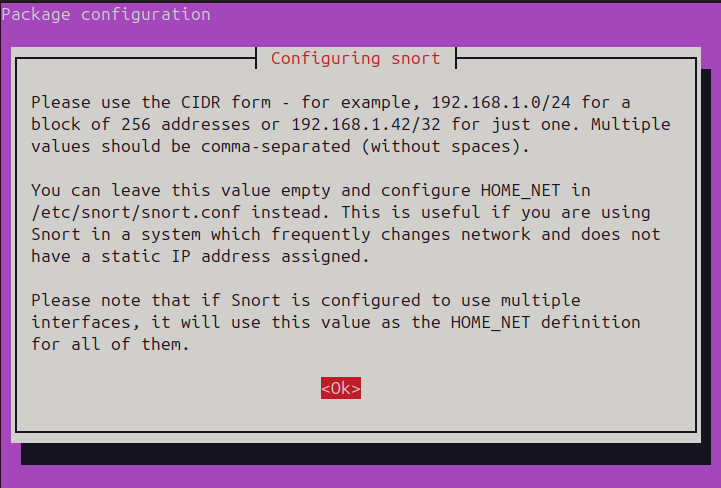
**How they can be detected:**

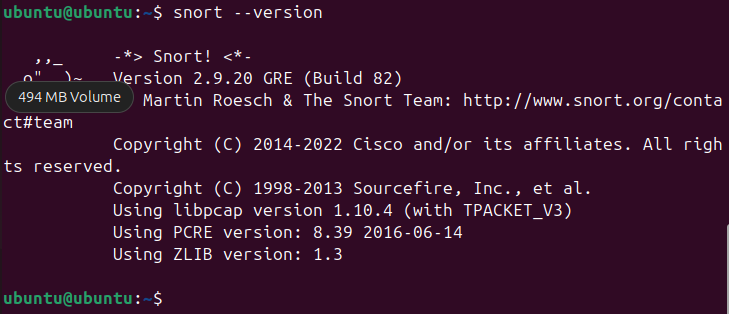
* **Traffic analysis:** Sophisticated attackers may analyze traffic patterns to spot anomalies associated with honeypots.
* **Fingerprinting:** Advanced techniques can detect the unique characteristics of honeypots (e.g., operating system or software inconsistencies).
* **Behavior analysis:** A lack of real users interacting with the system or abnormal interaction patterns may reveal the presence of a honeypot.

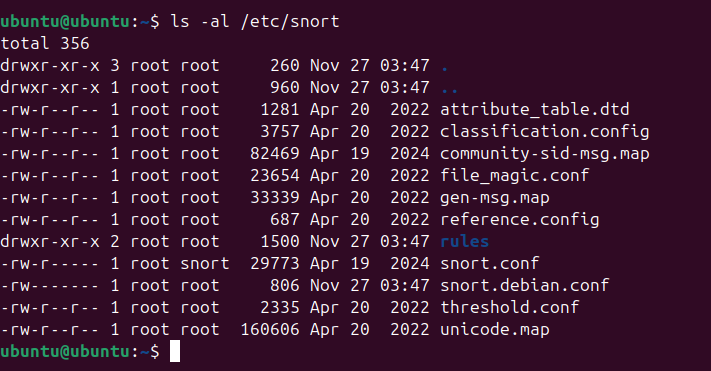
**Tools to detect:**

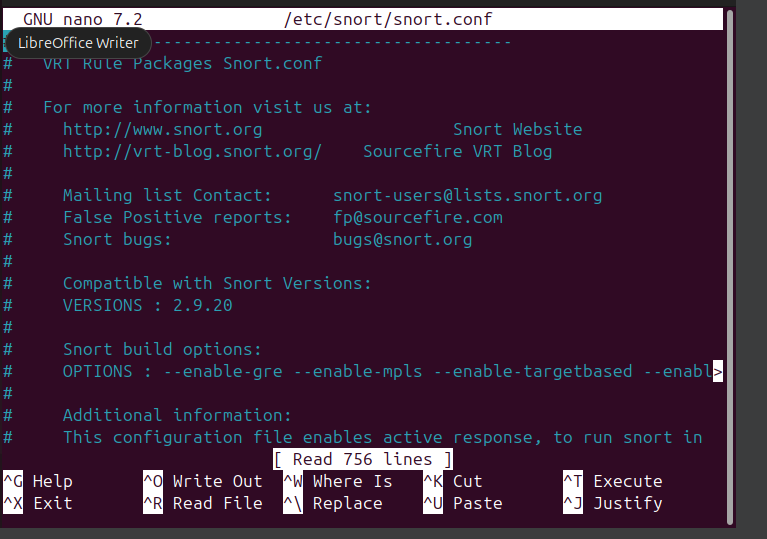
1. **Kippo\_detect**
2. **Send-safe Honeypot Hunter**

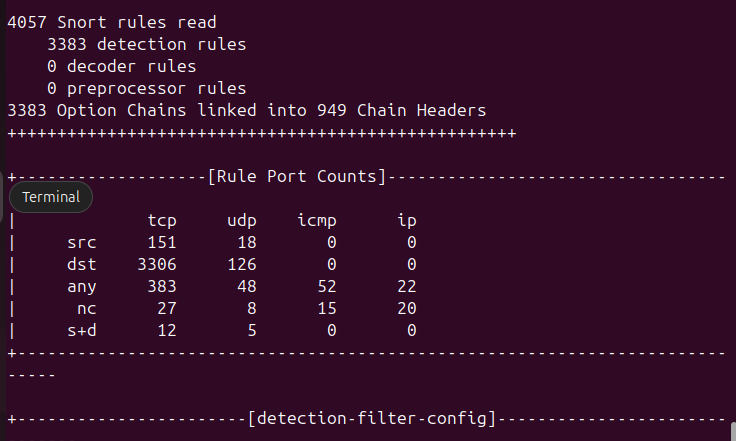
**Detect Intrusions using Snort:**

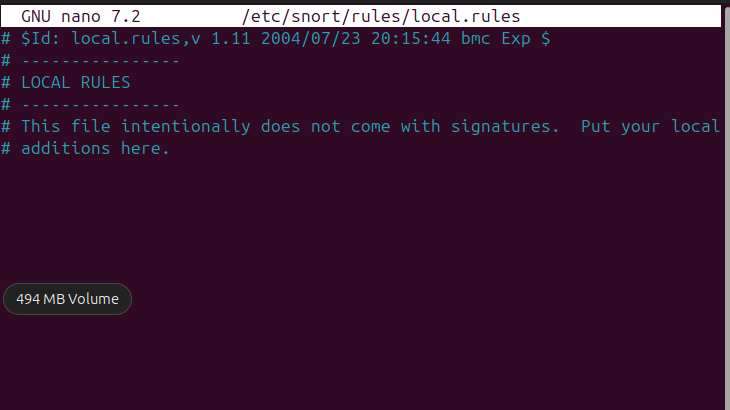


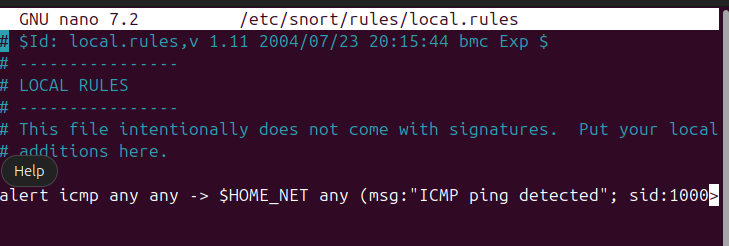


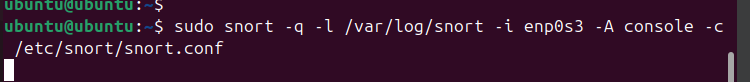


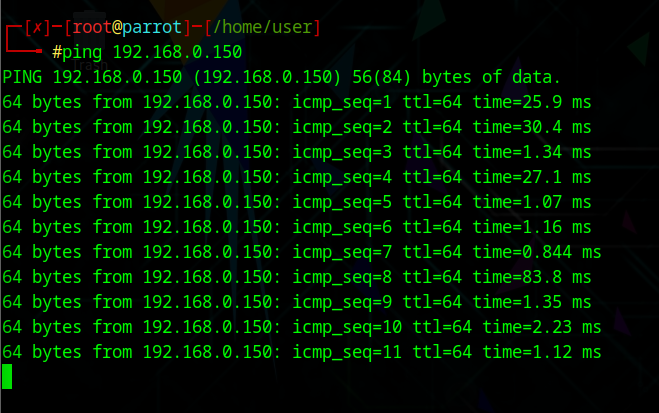


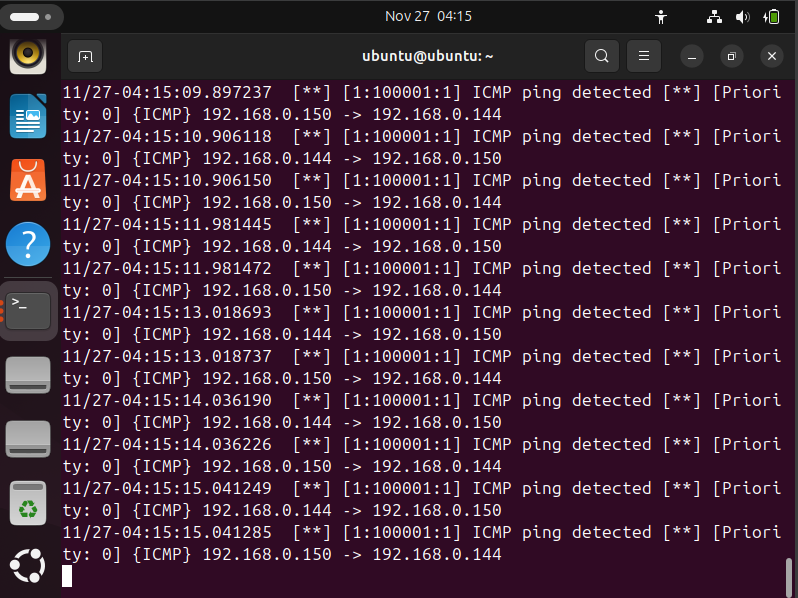








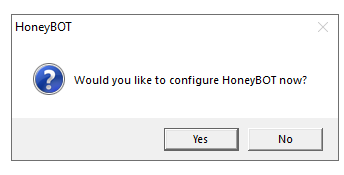


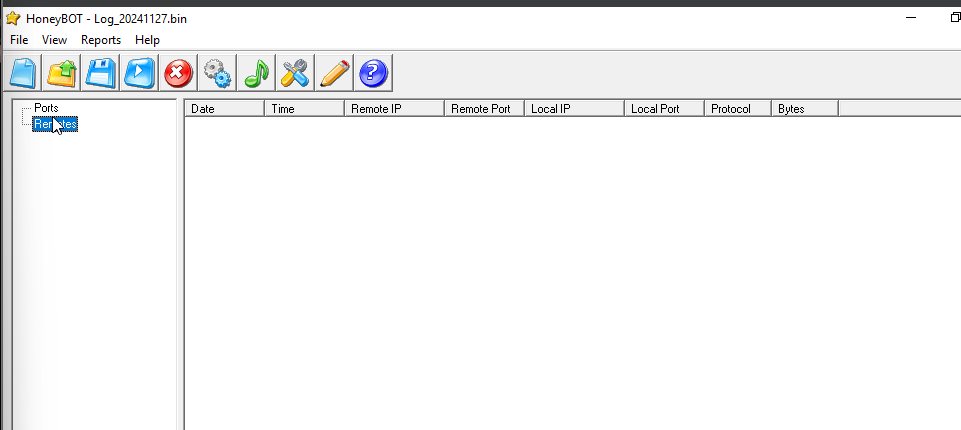


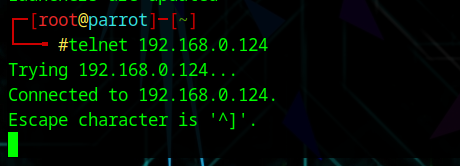
**Detect malicious network traffic using zone alarm free firewall:**

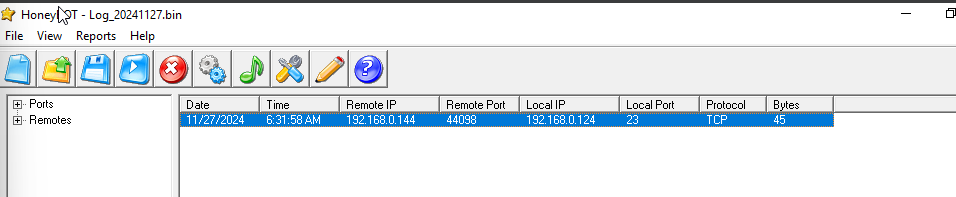
N.A.

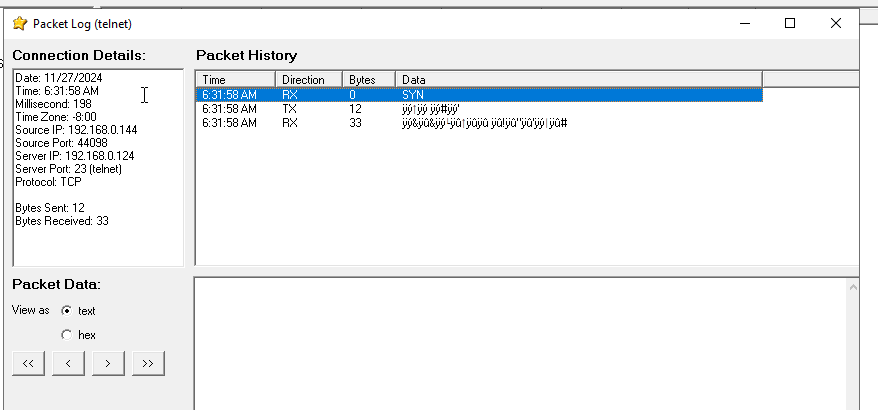
**Detect Malicious Network Traffic Using Honeybot:**

****

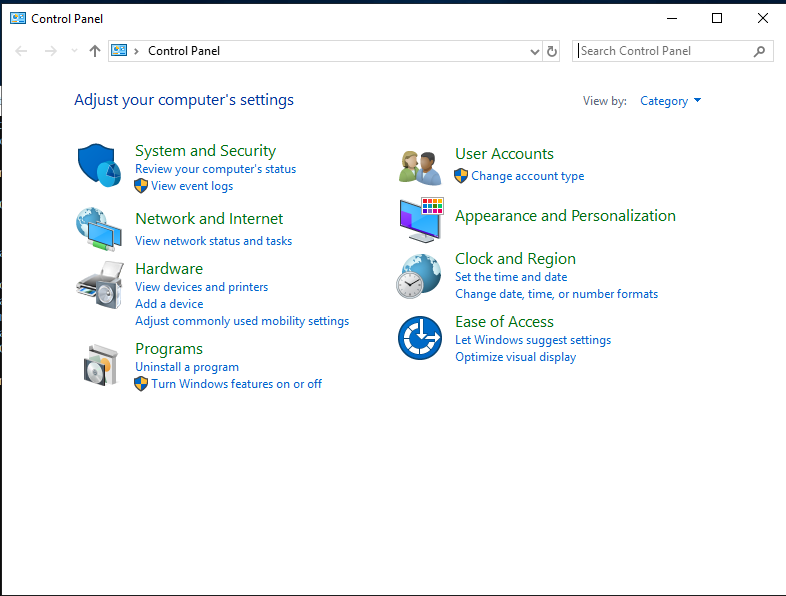
****

****

****

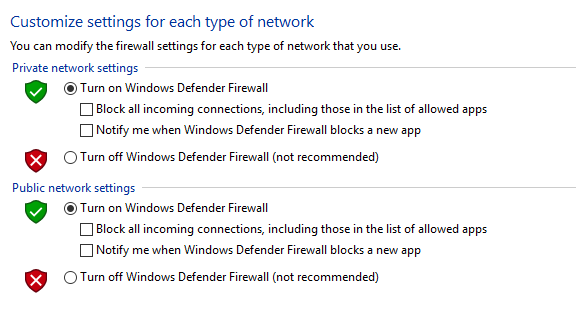
****

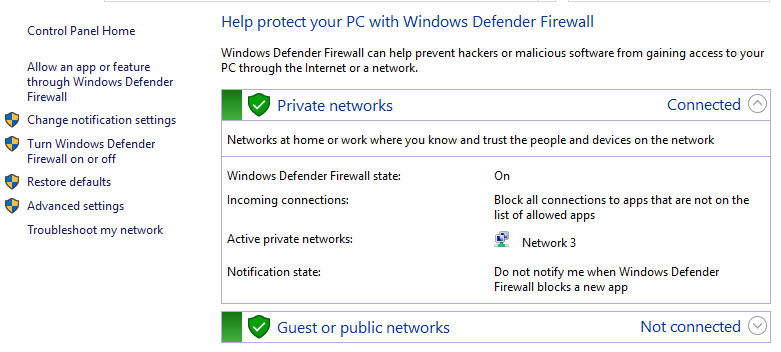
**Bypass Firewall through windows BitsAdmin:**

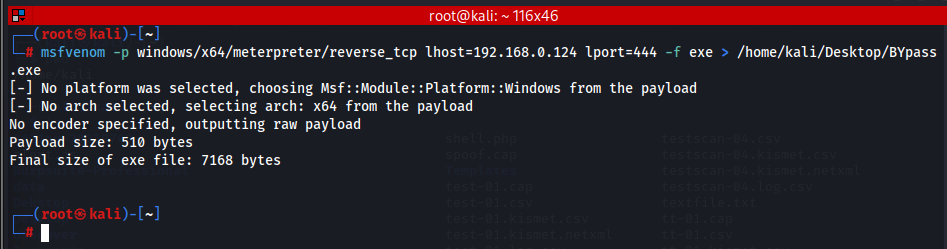


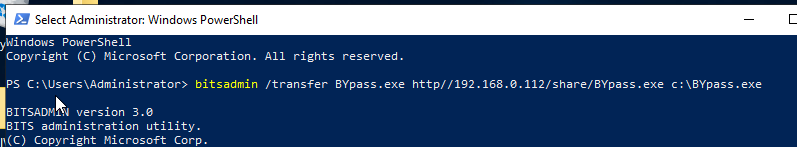


****

****

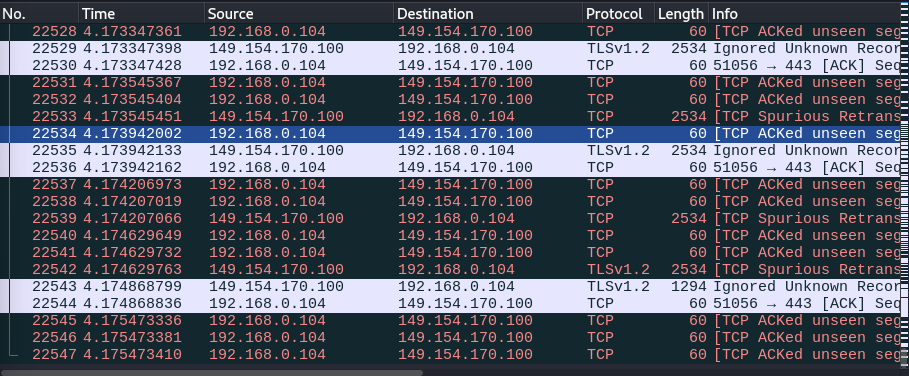
****

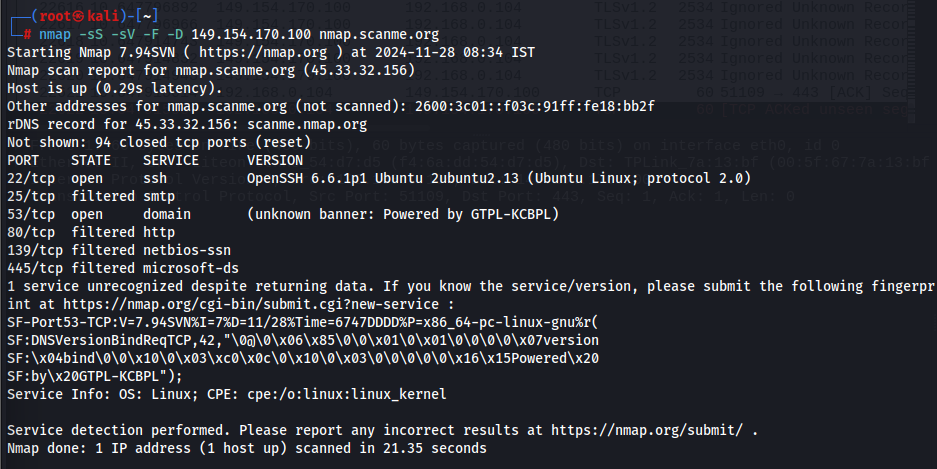
****

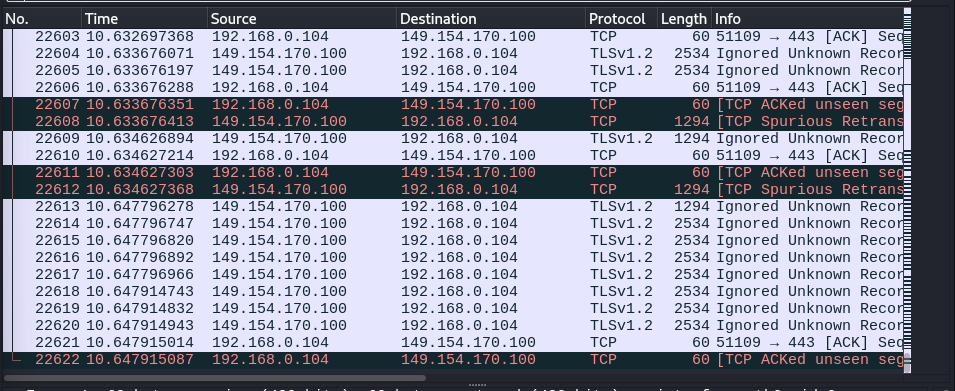
****

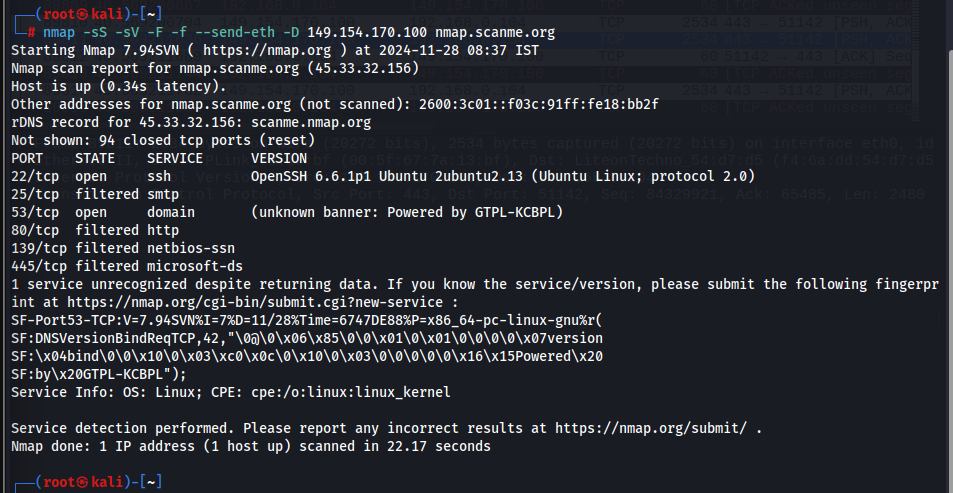
**Bypass Windows Firewall using Nmap Evasion Techniques:**

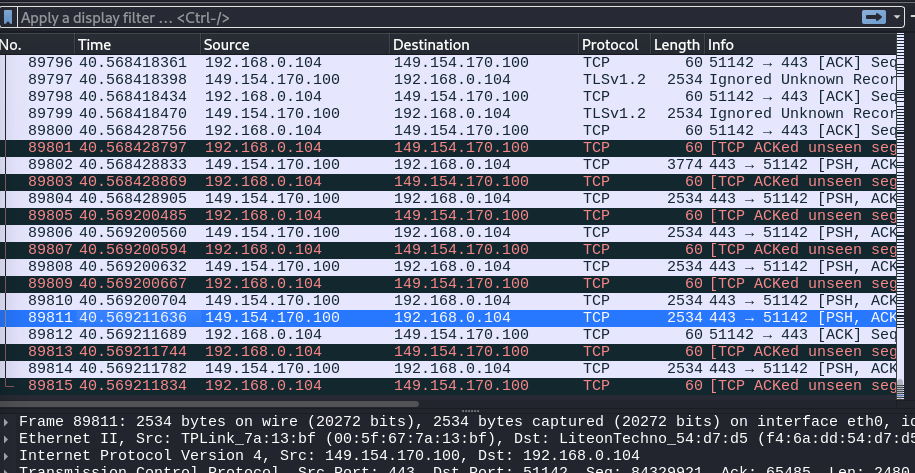
****

****

****

****

****

****

**Bypass Antivirus using Metasploit Templates:**

