Cogoport-Security Documentation

1. Understanding Linux Security and applying its practices and protocols in Cogoport
2. Network Security to avoid misuse, exposure or modification of Cogoports Internal infrastructure.
3. Cyber Security
4. Firewalls and their working

Security requirements

Authorisation - Only allow those that need access to the data
Authenticity - Verifying they are who they say they are
Privacy / Confidentiality - Ensure personal information is not being compromised
Integrity - Ensuring that the data has not been tampered with
Non-repudiation - Confirmation that data is received. The ability to prove it in court
Availability - Ensure that the system can perform its required function

Linux Attack Detection

No matter how good our security gets, it can be compromised. That is why it is so important to have various forms of attack detection present, so that when an incident happens we are alerted to it as soon as possible (and not when we start getting complaints from other sites).
The netstat command, meaning network statistics, is a Command Prompt command used to display very detailed information about how your computer is communicating with other computers or network
Devices.
Command: **netstat** [**-a**] [**-b**] [**-e**] [**-f**] [**-n**] [**-o**] [**-p** *protocol*] [**-r**] [**-s**] [**-t**] [**-x**] [**-y**] [*time_interval*]

Specifically, the netstat command can show details about individual network connections, overall and protocol-specific networking statistics, and much more, all of which could help troubleshoot certain kinds of networking issues.Various tools exist to measure memory and disk usage: vmstat, free, df, du, all of which are covered by their respective man pages.

Intrusion Detection Tools

1.) **Linux Intrusion Detection System-** is a patch to the Linux kernel and associated administrative tools that enhances the kernel's security by implementing mandatory access control (MAC). When LIDS is in effect all system network administration operations, chosen file access, any capability use, raw device, memory, and I/O access can be made impossible, even for root. One can define which programs can

access specific files. It uses and extends the system capabilities bounding set to control the whole system and adds some network and file system security features to the kernel to enhance the security. One can finely tune the security protections online, hide sensitive processes, receive security alerts through the network, and more

2.) **Network Intrusion Detection Tools (NIDS) -** Network intrusion detection systems are placed at highly strategic points within the network to monitor inbound and outbound traffic from all devices in the network. But scanning all traffic could lead to the creation of bottlenecks, which impacts the overall speed of the network.

3.) **Host Intrusion Detection systems:** (HIDS)*:* Host intrusion detection systems run on separate machines or devices in the network, and provide safeguards to the overall network against threats coming from the outside world.

4.) **Signature based IDS**: Signature based IDS systems monitor all the packets in the network and compare them against the database of signatures, which are pre-configured and predetermined attack patterns. They work similar to antivirus software.

Note: *A system that monitors important operating system files is an example of an HIDS, while a system that analyzes incoming network traffic is an example of an NIDS. Intrusion Detection Systems (IDS) analyze network traffic for signatures that match known cyber attacks. Intrusion Prevention Systems (IPS) also analyzes packets, but can also stop the packet from being delivered based on what kind of attacks it detects — helping stop the attack.*

Difference between firewall and IDS:
Firewall is like a gatekeeper and IDS is like a bodyguard. A graphical representation of Firewall vs IPS vs IDS is shown on the next page.

Parameter	Firewall	IPS	IDS
Abbreviation for	–	Intrusion Prevention System	Intrusion Detection System
Philosophy	Firewall is a network security device that filters incoming and outgoing network traffic based on predetermined rules	IPS is a device that inspects traffic, detects it, classifies and then proactively stops malicious traffic from attack.	An intrusion detection system (IDS) is a device or software application that monitors a traffic for malicious activity or policy violations and sends alert on detection.
Principle of working	Filters traffic based on IP address and port numbers	inspects real time traffic and looks for traffic patterns or signatures of attack and then prevents the attacks on detection	Detects real time traffic and looks for traffic patterns or signatures of attack and them generates alerts
Configuration mode	Layer 3 mode or transparent mode	Inline mode , generally being in layer 2	Inline or as end host (via span) for monitoring and detection
Placement	Inline at the Perimeter of Network	Inline generally after Firewall	Non-Inline through port span (or via tap)
Traffic patterns	Not analyzed	Analyzed	Analyzed
Placement wrt each other	Should be 1st Line of defense	Should be placed after the Firewall device in network	Should be placed after firewall
Action on unauthorized traffic detection	Block the traffic	Preventing the traffic on Detection of anomaly	Alerts/alarms on detection of anomaly
Related terminologies	• Stateful packet filtering • permits and blocks traffic by port/protocol rules	• Anomaly based detection • Signature detection • Zero day attacks • Blocking the attack	• Anomaly based detection • Signature detection • Zero day attacks • Monitoring • Alarm

IDS TYPES

1) **Network Based:**
   - **Generally done at single point of entry.**
   - **Relatively Easy to deploy**
   - **Simple rules (signatures) for detection**
2) **Host Based:**
   - **Provides detection of Non-network based attacks.**
   - **Not affected when network traffic is encrypted.**
   - **Not affected when network traffic is switched**
   - **More labor intensive to deploy**
   - **To be deployed at every host that requires monitoring**

Open source tools for detecting Network Intrusion:

1) **SNORT (But don't snort in office)**

Snort is a free and open source network intrusion detection and prevention tool. The main advantage of using Snort is its capability to perform real-time traffic analysis and packet logging on networks. With the functionality of protocol analysis, content searching and various pre-processors, Snort is widely accepted as a tool for detecting varied worms, exploits, port scanning and other malicious threats.
Moreover, many large MNCs are currently using Snort based Intrusion Prevention systems(IPS) and Intrusion Detection Systems (IDS).
It can be configured in three main modes —
(i) Sniffer
(ii) Packet logger
(iii) Network intrusion detection.
In sniffer mode, the program will just read packets and display the information on the console. In packet logger mode, the packets will be logged on the disk. In intrusion detection mode, the program will monitor real-time traffic and compare it with the rules defined by the user.
Snort can detect varied attacks like a buffer overflow, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts, etc. It is supported on a number of hardware platforms and operating systems like Linux, OpenBSD, FreeBSD, Solaris, HP-UX, MacOS, Windows, etc.

A point worth mentioning for snort is that it has no GUI for rule manipulation.
Useful Links:

1) Using Snort for intrusion detection
2) Snort Documentation

   USAGE OF SNORT:

   Snort can detect varied attacks like a buffer overflow, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts, etc.

   1) Buffer Overflow: A buffer is a sequential section of memory allocated to contain anything from a character string to an array of integers. A buffer overflow, or buffer overrun, occurs when more data is put into a fixed-length buffer than the buffer can handle. The extra information, which has to go somewhere, can overflow into adjacent memory space, corrupting or overwriting the data held in that space. This overflow usually results in a system crash, but it also creates the opportunity for an attacker to run arbitrary code or manipulate the coding errors to prompt malicious actions.
   2) CGI Attacks - Implementing Malicious scripts in the Common Interface Gateway in order to either gain access to make DoS attack or to manipulate the database.

Components:

1) **Packet Decoder:**

    - Processes packets from different interfaces for processing
    - **SLIP, PPP, Ethernet etc**

2) Preprocessors:

- Modify packets before engine detection
- Typically because intruder has modified packet to evade detection

  Preprocessor Examples:
    - Rule to find: “scripts/iisadmin”
    - Packets Modified as such “scripts/./iisadmin”, “scripts/examples/../iisadmin” etc

3) Detection Engine:

- Used to detect intrusion activity in packets
- Applied pre-defined rules to different layers
- Applies pre defined rules to different layers

4) Alerting and Logging

- Alerts are logged
- May include Headers or packets

5) Output modules

- Control Format of logs - Text, Binary, conversion to XML, Sending windows messages via SMB, Log to a database.

Working with SNORT

Snort

Network Security Design

Network Security - focuses on protecting the underlying infrastructure. Concerned mainly with :

- **Unauthorized Access** : this measure ensures that only those with authorization gain access to the network. An example is the credentials you must enter when logging into your computer network.
- **Malicious Use** : this measure manifests itself in a number of ways. The most common is that high value network resources are locked away from public access. An example is your company's computer room.
- **Faults** : this measure is concerned with detecting and preventing potential issues when and before they occur. An example is the temperature sensors in the computers and devices that supply information on the operational state.
- **Tampering** : this measure monitors when devices are accessed, or when cases are opened to determine when something might have happened that shouldn't. An example is when credentials are used for access to the resource.

- **Destruction** : this measure is similar to malicious use, and works primarily in a preventative capacity. An example is the company's computer room, as mentioned above.
- **Disclosure** : this measure focuses on keeping the particulars of the network secret, so that exploits cannot be easily developed. An example is keeping the specifications under lock and key so that only those that need to know the particulars have access to them.

Network Protocols

Network Protocol is a set of rules that govern communications between devices connected on a network.

TCP/IP Protocol

IP corresponds to the Network layer (Layer 3) whereas TCP corresponds to the Transport layer (Layer 4) in OSI. TCP/IP applies to network communications where the TCP transport is used to deliver data across IP networks.TCP/IP protocols are commonly used with other protocols such as HTTP, FTP, SSH at application layer and Ethernet at the data link/physical layer.

OSI Model of Layer wise Distribution.

1) **Physical Layer-** responsible for the transmission and reception of unstructured raw data between a device and a physical transmission medium
2) **Data Layer -** The data link layer provides node-to-node data transfer—a link between two directly connected nodes. Further divided into MAC (Medium Access Control) and LLC (Logical Layer Control)
3) **Network Layer -** provides the functional and procedural means of transferring variable length data sequences (called packets) from one node to another connected in "different networks".
4) **Transport Layer -** The transport layer provides the functional and procedural means of transferring variable-length data sequences from a source to a destination host, while maintaining the quality of service functions.
5) **Session Layer -** The session layer controls the dialogues (connections) between computers. It establishes, manages and terminates the connections between the local and remote application. It provides for full-duplex, half-duplex, or simplex operation, and establishes procedures for checkpointing, suspending, restarting, and terminating a session
6) **Presentation Layer -** The presentation layer establishes context between application-layer entities, in which the application-layer entities may use different syntax and semantics if the presentation service provides a mapping between them. If a mapping is available, presentation protocol data units are encapsulated into session protocol data units and passed down the protocol stack
7) **Application Layer -** The application layer is the OSI layer closest to the end user, which means both the OSI application layer and the user interact directly with the software application. This layer interacts with software applications that implement a

communicating component. Such application programs fall outside the scope of the OSI model.