Acceptance clause: by completing this project the student accepts that he/she is responsible for what he/she will do and that he/she will **not use** these tools outside the virtual one created for that purpose. The student also accepts the legal repercussions that some of these actions may be subject to if these actions are carried out on external sites.

Project 7: IDS (Intrusion detection System)

Level: 6

Difficulty: high

Environment: Linux Machines (VM)

Objective: Install and analyze the indicated tools to create a IDS (DO NOT USE outside the virtual network).

Task: The student will have to collect information about IDS tools, and configure Router to execute a IDS. After it, the user will use worker1 to attack router using nmap per example & detect this attack using IDS tools.

Necessary: Start with project 4-5-6.

An intrusion detection system (IDS; also intrusion prevention system or IPS) is a device or software application that monitors a network or systems for malicious activity or policy violations. Any intrusion activity or violation is typically reported either to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system combines outputs from multiple sources and uses alarm filtering techniques to distinguish malicious activity from false alarms.

IDS types range in scope from single computers to large networks. The most common classifications are network intrusion detection systems (NIDS) and host-based intrusion detection systems (HIDS). 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. It is also possible to classify IDS by detection approach. The most well-known variants are signature-based detection (recognizing bad patterns, such as malware) and anomaly-based detection (detecting deviations from a model of "good" traffic, which often relies on machine learning).

Another common variant is reputation-based detection (recognizing the potential threat according to the reputation scores). Some IDS products have the ability to respond to detected intrusions. Systems with response capabilities are typically referred to as an intrusion prevention system. Intrusion detection systems can also serve specific purposes by augmenting them with custom tools, such as using a honeypot to attract and

characterize malicious traffic. (Ref: https://en.wikipedia.org/wiki/Intrusion_detection_system)

Tools To Use:

Tripwire (also aide/samhain/fcheck): is a tool that aids system administrators and users in monitoring a designated set of files for any changes. Used with system files on a regular (e.g., daily) basis, Tripwire can notify system administrators of corrupted or tampered files, so damage control measures can be taken in a timely manner. https://github.com/Tripwire/tripwire-open-source

Snort: is a libpcap-based packet sniffer/logger which can be used as a lightweight network intrusion detection system. It features rules-based logging and can perform content searching/matching in addition to detecting a variety of other attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, and much more. Snort has a real-time alerting capability, with alerts being sent to syslog, a separate "alert" file, or even to a Windows computer via Samba. https://www.snort.org/

Suricata: is the net Generation Intrusion Detection and Prevention Tool. It is based on rules (and is fully compatible with snort rules) to detect a variety of attacks / probes by searching packet content. It can also be used as Intrusion Prevention System (IPS), and as higher layer firewall. This new Engine supports Multi-Threading, Automatic Protocol Detection (IP, TCP, UDP, ICMP, HTTP, TLS, FTP and SMB), Gzip Decompression, Fast IP Matching and coming soon hardware acceleration, https://suricata.readthedocs.io/en/latest/quickstart.html

Nikto: Open Source (GPL) web server scanner which performs comprehensive tests against web servers for multiple items, including over 6700 potentially dangerous files/programs, checks for outdated versions of over 1250 servers, and version specific problems on over 270 servers. It also checks for server configuration items such as the presence of multiple index files, HTTP server options, and will attempt to identify installed web servers and software. Scan items and plugins are frequently updated and can be automatically updated. Nikto is not designed as a stealthy tool. It will test a web server in the quickest time possible, and is obvious in log files or to an IPS/IDS. However, there is support for LibWhisker's anti-IDS methods in case you want to give it a try (or test your IDS system).

Not every check is a security problem, though most are. There are some items that are "info only" type checks that look for things that may not have a security flaw, but the webmaster or security engineer may not know are present on the server. These items are usually marked appropriately in the information printed. There are also some checks for unknown items which have been seen scanned for in log files. https://cirt.net/nikto2

tiger: security auditing and intrusion detection tools for Linux. 'tiger' scripts, is a set of tools (Bourne shell scripts and C programs) which are used to perform a security audit of different operating systems components. The tools can be both run all at once to generate an audit report of the system and to detect elements that could be fixed when hardening it. TIGER has one primary goal: report ways the system's security can be

compromised. Most of the tools are independent, but some of them rely on specialised external security tools such as John the Ripper, Chkroot and integrity check tools (like Tripwire, Integrit or Aide) to execute some tasks. The same checks are also configured by default to run periodically and detect deviations or unauthorised changes. This makes it possible to used them also as a host intrusion detection mechanism. This review mechanism relies on the use of the cron task scheduler and an email delivery system to report errors and deviations. http://savannah.nongnu.org/projects/tiger/