CIS 4163: Application Security Technologies

INSTRACTOR: John
MUNYAKAYANZA
DEPT. INFORMATION SYSTEMS
NYARUGENGE –CAMPUS
CST-UNIVESTIRY OF RWANDA

UNIVERSITY of RWANDA

Vulnerability scanning programs

Introduction

- Today, **data is the most active thing in organizations and the circular Internet**.
- The **attacker also travels across the Internet and is becoming more sophisticated bias**.
- Often administrators **can not identify the vulnerabilities of the system due to lack of means**.
- Mainly due to **the high cost of proprietary software solutions for vulnerability scanning** and **creating reports automatically**

Tools/programs: N**essus**

- is a **tool for vulnerability scanning**.
- it is **a fault verification program / security vulnerabilities** (ports, vulnerabilities, exploits).
- **It consists of a client and server**, and the **scan itself is done by the server (Nessus server).**
- Nessus **helps identify and resolve vulnerabilities some problems.**
- The **Server part executes the tests while the client part allows configuration and reporting**.
- Nessus is distributed under the terms of the **GNU General Public License**.

Skipfish

- This tool for **security test to fully automated sites and is very light and very fast** (can run 2,000 requests per second).

- As well as other security tools, **it has several types of safety tests, including Blind SQL Injection.**

- The program works on **Windows, Linux and Mac OS X.**

Wireshark:

- Formerly known as **Ethereal** **is a program that analyzes network traffic and organizes for protocols**.

- The features of **Wireshark are similar to tcpdump but with a GUI interface**, with **more information and the possibility of using filters.**

- It is then **possible to control the traffic of a network and know everything that goes in and out of the computer**, in different protocols, or network to which the computer is connected

For verification programs for security vulnerabilities visit:

- http://sectools.org/tag/sniffers/
- http://webresourcesdepot.com/10-free-web-application-security-testing-tools/
- http://insecure.org/tools/tools-pt.html

UNIVERSITY of RWANDA

Packet Sniffers

- A packet sniffer is **a wire-tap devices or software that plugs into computer networks and eavesdrops on the network traffic**.
- It basically **allows you to listen to other peoples conversations**.
- **This is done using a sniffing program**.
- The packet sniffer **can intercept and log traffic passing over a digital network or part of a network**.
- When **data streams moves with networks, the sniffer captures each packet and eventually decoded and analyzes it's content according with any specifications.**

How a packet sniffer works

- Ethernet was built around a principle known as **a shared principle where all machines on a local network share the same medium like same wire**.
- **This means that all machines can see and hear all the traffic that is transmitted over the same medium like same wire**.
- To avoid this issue, **the Ethernet hardware is built with a filter that ignores all traffic that does not belong to it.**
- This is **done by avoiding all frames whose MAC address doesn't match**.
- So in **order for a sniffer program to operate in these circumstances, it turns off this filter from the Ethernet hardware**.
- By turning the filter off, it puts the Ethernet hardware into a mode known as **promiscuous mode**.
- **This makes all the traffic visible from all machines that are sharing the same medium.**

The uses of a packet sniffer

- Packet Sniffer programs have been existing for such a long time and can be used in two forms:

➢ **Commercial packet sniffers**: These can be used to help maintain networks

➢ **Underground Packet sniffers**: These are used to break into computers

UNIVERSITY of RWANDA Cont'd

- This nature of packet sniffers means it can be used to do different things like:

- Analysing network problems
- Detecting network intrusion attempts
- Gaining information for effecting a network intrusion
- Gather and report network statistics
- Filter suspect content from network traffic
- Debug client/server communication

Components of a packet sniffer

- The components of a packet sniffer include:

- **The hardware:** Most **products work from the standard network hardware adapters, even though some require special hardware**. **The reason for special hardware is that they have the capability to analyze hardware faults like CRC errors, voltage problems, cable programs, jitter, etc**

- **Capture Driver**: This is the most important part. **It captures the network traffic from the medium like the wire, filters it for the particular traffic you want, then stores it in a buffer**

- **Buffer**: **Once the frames are captured from the network, they are stored in a buffer**

- **Decode**: This **displays the contents of the network traffic with descriptive text so that an analysis can figure out what is going on**.

- **Packet editing/transmission**: **Some products contain features that allow you to edit your own network packets and transmit them onto the network**

Vulnerability Scanners

- A vulnerability scanner is **software application that assesses security vulnerabilities in networks or host systems and produces a set of scan results.**

- However, because both administrators and attackers can use the same tool for fixing or exploiting a system, **administrators need to conduct a scan and fix problems before an attacker can do the same scan and exploit any vulnerabilities found.**

UNIVERSITY of RWANDA Cont'd

- A vulnerability **scanner can assess a variety of vulnerabilities across information systems (including computers, network systems, operating systems, and software applications)** that may have originated from a vendor, system administration activities, or general day to-day user activities:

- **Vendor-originated:** this includes **software bugs, missing operating system patches, vulnerable services, insecure default configurations**, and web application vulnerabilities.

- **System administration-originated:** this includes **incorrect or unauthorised system configuration changes, lack of password protection policies, and so on.**

- **User-originated:** this includes **sharing directories to unauthorised parties, failure to run virus scanning software**, and malicious activities, such as deliberately introducing system backdoors.

The Benefits of Vulnerability Scanners

- Firstly, **a vulnerability scanner allows early detection and handling of known security problems.** By employing ongoing security assessments using vulnerability scanners, it is easy to identify security vulnerabilities that may be present in the network, from both the internal and external perspective.

- Secondly, **a new device or even a new system may be connected to the network without authorisation. A vulnerability scanner can help identify rogue machines, which might endanger overall system and network security.**

- Thirdly, **a vulnerability scanner helps to verify the inventory of all devices on the network.** The inventory includes the device type, operating system version and patch level, hardware configurations and other relevant system information. This information is useful in security management and tracking.

UNIVERSITY of RWANDA

The Limitations of Vulnerability Scanners

- The drawbacks of vulnerability scanners are:

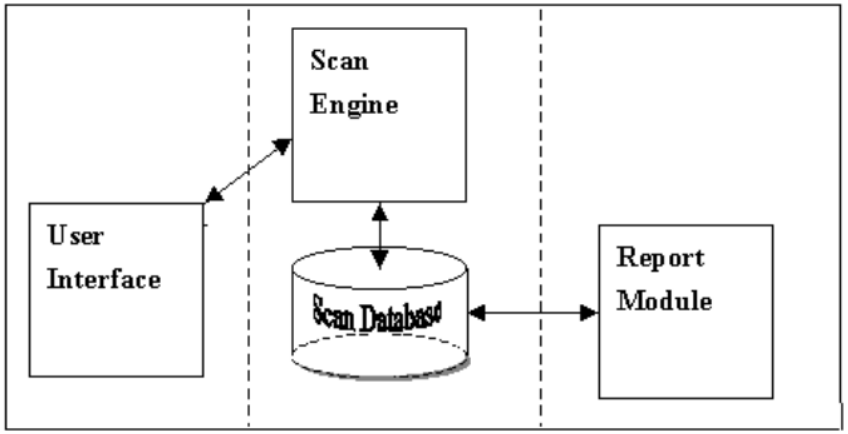
➢ **Snapshot only**: a **vulnerability scanner can only assess a "snapshot of time" in terms of a system or network's security status**. Therefore, scanning needs to be conducted regularly, as new vulnerabilities can emerge, or system configuration changes can introduce new security holes.

➢ **Human judgement is needed**: **Vulnerability scanners can only report vulnerabilities according to the plug-ins installed in the scan database**. They cannot determine whether the response is a false negative or a false positive. Human judgement is always needed in analysing the data after the scanning process.

➢ **Others: a vulnerability scanner is designed to discover known vulnerabilities only. It cannot identify other security threats**, such as those related to physical, operational or procedural issues.

Architecture of Vulnerability Scanners

- In general, a vulnerability scanner is made up of four main modules, namely, **a Scan Engine, a Scan Database, a Report Module and a User Interface**



Components of Scanner

UNIVERSITY of RWANDA Cont'd

- The **Scan Engine** **executes security checks according to its installed plug-ins, identifying system information and vulnerabilities**. It can scan more than one host at a time and compares the results against known vulnerabilities.

- The **Scan Database** **stores vulnerability information, scan results, and other data used by scanner**. The number of available plug-ins, and the updating frequency of plug-ins will vary depending on the corresponding vendor. Each plug-in might contain not only the test case itself, but also a vulnerability description, a Common Vulnerabilities and Exposures (CVE) identifier; and even fixing instructions for a detected vulnerability. Scanners with an "auto-update" feature can download and install the latest set of plug-ins to the database automatically.

UNIVERSITY of RWANDA Cont'd

- The **Report Module** **provides different levels of reports on the scan results, such as detailed technical reports with suggested remedies for system administrators**, summary reports for security managers, and high-level graph and trend reports for executives.
-
- The **User Interface** **allows the administrator to operate the scanner.** It may be either a Graphical User Interface (GUI), or just a command line interface.

Types of Vulnerability Scanners

- Vulnerability scanners can be divided broadly into two groups:

➢ **Network-based scanners that run over the network**

➢ **Host-based scanners that run on the target host itself**.

Network-Based Scanners

- A network-based scanner is **usually installed on a single machine that scans a number of other hosts on the network.**

- It helps **detect critical vulnerabilities such as mis-configured firewalls, vulnerable web servers,** risks associated with vendor-supplied software, and risks associated with network and systems administration.

Different types of network-based scanners include:

- **Port Scanners** that **determine the list of open network ports in remote systems**
- **Web Server Scanners** that **assess the possible vulnerabilities (e.g. potentially dangerous files) in remote web servers**
- **Web Application Scanners** that **assess the security aspects of web applications (such as cross site scripting and SQL injection) running on web servers**. It should be noted that web application scanners cannot provide comprehensive security checks on every aspect of a target web application. Additional manual checking (such as whether a login account is locked after a number of invalid login attempts) might be needed in order to supplement the testing of web applications.

Host-Based Scanners

- A host-based scanner **is installed in the host to be scanned, and has direct access to low level data, such as specific services and configuration details of the host's operating system**.
- **It can therefore provide insight into risky user activities** such as using **easily guessed passwords or even no password**.
- **It can also detect signs that an attacker has already compromised a system**, including looking for suspicious file names, unexpected new system files or device files, and unexpected privileged programs.
- Host-based scanners **can also perform baseline (or file system) checks**. Network-based scanners cannot perform this level of security check because they do not have direct access to the file system on the target host.

Type of Host-based scanner

- **A database scanner** is an example of a host-based vulnerability scanner.

- **It performs detailed security analysis of the authorisation, authentication, and integrity of database systems**, and can identify any potential security exposures in database systems, ranging from weak passwords and security mis-configurations to Trojan horses.

Thank You

……..Murakoze…….!