NETWORK SECURITY ASSESMENT IN CRITICAL PRODUCTION SYSTEMS

Contents

Abstract

Evaluation of computing system security requires knowledge of the vulnerabilities present in the system and of potential attacks against the system. Vulnerabilities can be classified based on their location as application vulnerabilties, network vulnerabilities, or host vulnerabilities. This paper describes some tools which can collect vulnerabilities, a new software tool for checking host vulnerabilities. It helps system administrators by quickly finding vulnerabilities that are present on a host. It is designed and implemented in a way a different tool is used for each vulnerability checked,and each possible output format is specified by a tool. As a result vulnerabilities as they are discovered and generate pdf as report.

WIRELESS –ATTACKS

1. Aircrack-ng :-

Aircrack-ng is WEP and WPA-PSK keycracking program that can recover keys once enough data packets have been captured.

1.-a <amode> : force attack mode.
2. -e <essid>   : target selection: Network identifier.
3. -b <bssid> : target selection: accesspoint's MAC.
4. -q   : enable quiet mode (no status output).
5. -l <file>   : write key to file.

2. Aireplay-ng :-

It is a part of aircrack-ng package and is used to inject wireless frames the main role is to generate traffic for later use in aircrack-ng for cracking WEP and WPA-PSK keys. Main purpose is of deauthenticate wireless clients for the purpose of capturing WPA handshake data and fake authentications , ARP request injections etc.,

(A): Filter options:

1. -b bssid : MAC address,Acces point.
2. -d dmac   : MAC address destination.
3. -s smac   : MAC address, Source.

3. Airmon-ng :-

Airmon-ng is also included in the aircrack-ng package and is used to enable and disable monitor mode on wireless interfaces.

usage: airmon-ng <start|stop|check> <interface> [channel or frequency]

4.Airodump-ng :-

It is Ideal for collecting WEP Ivs for use with aircrack-ng and it is used for packet capturing of raw 802.11 frames.GPS receiver connected to the computer, airodump-ng can log the coordinates of the discovered access points.

Options:

1. --ivs : Save only captured IVs.
2. --gpsd : Use GPSd.
3. --write <prefix> : Dump file prefix.
4. -w : same as --write
5. --beacons : Record all beacons in dump file.

5.Wifite:-

This tool is used to attack multiple WEP,WAP and WPS encrypted networks randomly. It
automatically collects all the required methods to crack wifi

usage:- wifite

WEB APPLICATION

1.Sqlmap:-

Automates the process of detecting and exploiting SQL injection flaws and taking over of database servers.

Support to directly connect to the database without passing via a SQL injection, by providing DBMS credentials, IP address, port and database name.

Automatic recognition of password hash formats and support for cracking them using a dictionary-based attack.

OPTIONS:

1.-h, --help :Show basic help message and exit.
2.-hh :Show advanced help message and exit.
3.--version :Show program's version number and exit.
4. -v VERBOSE :Verbosity level: 0-6 (default 1).

2.WPScan:-

WPScan is a black box WordPress vulnerability scanner that can be used to scan remote WordPress installations to find security issues.

Usage:- wpscan <options> <url>

OPTIONS:

1.u : usernames from id 1 to 10.
2.u[10-20] : usernames from id 10 to 20 (you must write [] chars).
3. p :plugins.
4. vp :only vulnerable plugins.
5. ap :all plugins (can take al long time).

3.Vega:-

vega is a tool for testing platform to test security of web applications., and it can find the valid SQL Injection, Cross-Site Scripting (XSS) , This is a Scanner of quick tests and an intercepting proxy for tactical inspection

usage:-

```
root@kali:~# vega
```

4.BrupSuit:-

Brup suit is an security testing of web applications and it works with some tools at a time for entire testing process from initial mapping and analysis of an application’s surface through to find and exploiting security vulnerabilities.

Usage:-

```
root@kali:~# burpsuite
```

VULNERABILITY ANALYSIS

1. Lynis :

Lynis is an open auditing tool.It is used to evaluate the security defense of Linux and Unix-based systems.It runs on the host itself, so performs more extensive security scans than vulnerability scanners.

Scan options:

```
 --auditor "<name>"        : Auditor name
 --check-all (-c)          : Check system
 --no-log                  : Don't create a log file
 --profile <profile>       : Scan the system with the given profile file
 --quick (-Q)              : Quick mode, don't wait for user input
 --tests "<tests>"         : Run only tests defined by <tests>
 --tests-category "<category>" : Run only tests defined by <category>
```

3.Nikto

Nikto is a used to scan webserver assessment to find potential problems and vulnerabilities very quickly

```
root@kali:~# nikto -h www.targetwebpage.xyz
//here -h is used for scanning the site
```

4.DotDotpwn

It is used to discover traversal directory vulnerabilities in software such as HTTP/FTP/TFTP servers, Web platforms such as CMSs, ERPs, Blogs, etc.

Usage:-

```
./dotdotpwn.pl -m http -h 192.168.1.1 -x 8080 -f /etc/hosts -k "localhost" -d 8 -t
200 -s
```

(-t) against the Web server
(-m) listening on port 8080
(-x) and installed in 192.168.1.1
(-h). Additionally, this will try to retrieve the /etc/hosts file
(-f) and to avoid false positives

4.Doona

Doona is a fork of the Bruteforce Exploit Detector Tool (BED). BED is a program which is designed to check daemons for potential buffer overflows, format string bugs etc.

Usage:-

```
root@kali:~# doona -m HTTP -t 192.168.1.15 -M 5
```

//Use the HTTP plugin ***(-m HTTP)*** to fuzz the target ***(-t 192.168.1.15)***, stopping after 5 cases ***(-M 5)***:

5.OsScanner:-

Oscanner is an Oracle assessment framework used to scan server side vulnerabilities like server list , portno, be verbose....,

Usage:-

```
root@kali:~# oscanner -s 192.168.1.S15 -P 1040
```

//Scan the target server *(-s 192.168.1.15)* on port 1040 *(-P 1040)*

```
OracleScanner -s <ip> -r <repfile> [options]
 -s <servername>
 -f <serverlist>
 -P <portnr>
 -v  be verbose
```

EXPLOITATION-TOOLS

1.Armitage:-

Armitage is a tool for Metasploit that visualizes targets, recommends exploits, and exposes the advanced postexploitation features in the framework. Use the same sessions Share hosts, captured data, and downloaded files Communicate through a shared event log. Run bots to automate red team tasks.

2.BeEF:-

BeEF is for The Browser Exploitation Framework. It is penetration testing tool that focuses on the web browser. BeEF looks past the hardened network perimeter and client system, and examines exploitability within the context of the one open door: the web browser.

3.Metasploit Framework:-

Metasploit can be used to test the vulnerability of target systems either to protect them or to break into them. And it can gain access for some unothorirised

4.Exploitdb:-

This tool is used to search exploit database searchsploit – Utility to search the Exploit Database archive.

5.SET(Social-Engineer Toolkit):-

The Social-Engineer Toolkit is an open-source penetration testing framework designed for SocialEngineering. SET has a number of custom attack vectors tha allow you to make a believable attack in a fraction of the time.

INFORMATION GATHERING :-

1.Dmitry:-

Dmitry (deepmagic information Gathering tool) is a UNIX/GNU Linux commad Line Application codded In C. It has the ability to gather all info about the Host. Base Functionality is able to gather possible personal sub domains emails, tcp port scan

Usage:- dmitry <option> <url>

-w   -who is look up

2.Netdiscover

It is used for Active or Passive scanning of wireless networks without the DHCP server. The tool help in the quick discovery of the IP address on a given network.

Usage:- netdiscover -r 192.168.1.0/24

-r gives the range of ip and mac address

3.ARP Scan Tool

This tool uses ARP packet will discover all active device In a IPV4 range even if protected by firewall designed to hide the presence of the device whether you are using wifi or Ethernet

Usage:- root@kali:~# arp-scan --interface=eth0 --localnet

`--interface=eth0` represents the interface to use for scanning,

`--localnet` makes `arp-scan` scan all possible IP addresses on the network connected to this interface,

4.Nmap

Nmap (Network Mapper) is a security scanner used to discover hosts and services on a computer network, thus creating a "map" of the network. To accomplish its goal, Nmap sends specially crafted packets to the target host and then analyzes the responses.

Usage:- nmap <option> <ipaddress>

<options>   -O means os detection

TARGET SPECIFICATION:

Can pass hostnames, IP addresses, networks, etc.

Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254

-iL <inputfilename>: Input from list of hosts/networks

-iR <num hosts>: Choose random targets

--exclude <host1[,host2][,host3],...>: Exclude hosts/networks

--excludefile <exclude_file>: Exclude list from file

5.Zenmap:-

Zenmap is the official Nmap Security Scanner GUI.It provides advanced features of Nmap and scans can be saved as profiles to make them easy to run repeatedly. Scan results can be saved and viewed later. Saved scan results can be compared with one another to see how they differ. The results of scans are stored in a searchable database.

Usage: root@kali:~# zenmap