Vulnerability

24 August 2018 14:16

We know how to gather information of target victim.

- [x] Open Ports
- [x] Service version
- [x] Servers
- [x] Operating System

Now we look potential vulnerabilities in order to get one step closer into compromising our target.
Nessus vulnerability scanner is one of the oldest and best vulnerability scanner.

Vulnerability Scanners and How Do They Work

Vulnerability scanners scan computer, networks, or application looking for weakness or vulnerability could be used by attacker to compromise the target.

Vulnerability scanners works: Sending specify data to the target host/network, based on it's analysis of the response, received from the target it can determine many things such as the following.

- [x] Open ports
- [x] Service
- [x] Operating system
- [x] Vulnerability

Pros and Cons of Vulnerability Scanner

1. Its task Is automation, it can automate many tasks such as reconnaissance, port scanning, service and version detection.
2. Main disadvantages is that vulnerability scanners very loud by nature and easily detected by since we are sending lots of traffic over the network. If you want to be anonymous during the pen-test, then this is not good way or choice.
3. False point is it can be produce lots of false positives, will report vulnerability in the target that may not exist in reality.

Vulnerability Assessment with NMAP

1. Most powerful scripting engine of NMAP, used for many automating tasks.
2. Scripting engine contains many scripts such as OS fingerprinting, DNS enumeration, and SNMP enumeration.
3. They used for vulnerability scanning purpose.
4. Script written in LUA language, Learning and write own scripting or modify existing ones.
5. Python is powerful and objected-oriented languages this is best for scripting.
6. NMAP script Location : /usr/local/share/nmap/scripts

Updating the Database

Good for practice to frequently update your NMAP scripting engine database.

```
$ $ namp -script-updatedb
```

Scanning MS08_067_netapi

- Most commonly found vulnerability (MS08_067_netapi) In windows XP
- NMPA script name is - "smb-check-vulns".
- This script automatic scan specify target against this vulnerability , report if this vulnerability find.

```
$ $ namp --script=smb-check-vulns <target ip>
```

We can use the --script=vuln to execute all the scripts that are related to vulnerability scanning and report them.

$ namp --script=vuln <target IP >

This type of scan could be loud and be easily detected.

Testing SCADA Environments with NMAP

SCADA = Supervisory Control and Data Acquisition;

1. SCADA is a Special devices used for monitoring industrial systems.
2. These system are very sensitive, they could to be handled with great care.
3. Using automated scanners such as Nessus, OpenVas, or Netexpose could be very dangerous.
4. Can be system crash with these tools.
5. With NMAP new script called vulnscan.nse.
   This script want to Two arguments to run :
   a. -sV (commonly used to perform service detection with nmap)
   b. -script=vulscan.nse (default syntax for using an nmap script)

Installation

A vulnscan.nse script is not installed in nmap , we need to download the script.

$ nmap -sV -script=vulscan.nse <target IP>

Nessus Scanner

Often By - Swiss army knife

1. Nmap gives you limited numbers of scripts it is only capable to only detecting few vulnerability
2. Most common used by Nessus to look is to at the banners/version headers.
3. Most of the time reveal interesting information about the target such as target version of service that running on currently target system.

Nessus comes in Two Used versions :
Home feed

(Personnel used it contains information about everything from a vulnerability scanning perspective.)

Profession feed :
Commercial usages mostly related to compliance checks and auditing purpose.
Not available for free.

Installing Nessus

- We need Nessus tool
- We need a Activation key (sign up on the site and the code will be send on email)
- Why need signup? First you need to code for your Nessus tool and code help you download latest-plugins for Nessus tool.

https://www.tenable.com/products/nessus/nessus-professional download link;

- Next Choose feed

Nessus Control Panel

Reports - Finding compiled in the form of a report
Mobile - Scanning mobile devices located on a network.
Scan - Most spend of our time after the polices. This enables the targets for vulnerabilities.
Polices - We define what type of scan we want to perform on the target, which plugin to use. What types of scan should be excluded, and so on.
Users- add or delete user's that can access the Nessus.

Configuration - allows to use a proxy and a bunch of other options for scanning.

Default Policies

1. Polices let us customize the type of scan and plug-ins we want to use to scan a target.
2. Nessus comes preloaded several default polices.
3. Each polices have different objective or types of pentests.

Default policies:

- External network scan
- Internet network scan
- Web app tests
- Prepare for PCI DSS audits

Nessus guidelines document available on the official website.

Policy name	Description
External network scan	This policy is tuned to scan externally facing hosts, which typically present fewer service to the network. Web application vulnerabilities are enabled in this policy.
Internal network scan	Used for better performance, scan large internal networks with many hosts, several exposed service, and embedded systems such as printers.
Web app tests	Scan your systems and have Nessus detect both known and unknown vulnerabilities in your web application, this is for you. Include scan : XSS, SQL, command injection and several more.
Prepare for PCI DSS audits	This policy enables built-in PCI DSS compliance check that compare scan result with the PCI standards and produces a report on your on your compliance posture. It is very important to note that a successful compliance scan does not guarantee compliance or a secure infrastructure.

Creating New Policy

Here video

SAFE CHECKS

1. Always enable "**Safe Check**"
2. Only run the low-risk checks so availability of the target system is not compromised.
3. Do not enable it mostly to crash older system and hence causing denial of service.

Silent Dependencies

1. Not include dependent checks in your report, which will make your report much more effective without the list of dependencies.

Avoid Sequential Scans

1. When it enabled Nessus will scan given IP addresses in a random order and not in the default sequential order.
2. Advantage of this is pass some that block the "consecutive port" traffic.
3. Example : Nessus will scan for port 21 and then it will jump over to 53 and then jump to another port.

Port Range

1. By default scan ports: 1 - 1024 this is not fix because some administrative consoles and web service run on ports higher than 1024.
2. Check for all ports changing the "default" keyword to "all".
3. More time for process all ports but help to find more or additional vulnerabilities.

Credentials

1. "Credentials" allow to specify OS IDs, SMB, FTP, HTTP and other credentials.
2. Help to scan in depth analysis with Nessus.

Plug-Ins

1. "Plug-Ins" which will you tell you what type of vulnerabilities it shall look for.
2. Coded in "Nessus Attack Scripting Language"
3. Learning it make your own plug-ins or modify existing once.

Preferences

1. Nessus that you can customize to handle different types of contents.

Scanning the Target

1. We need to specify the targets to scan.
2. All you need to do is to inside the scan options and specify the target and the policy that we created in the last step.

Nessus Integration with Metasploit

1. Nessus can be integrated into Metasploit for performing a far more effective penetration test.
2. We can easily perform vulnerability scanning from within the Metasploit console.
3. These result outputted to the Metasploit console itself.
4. We have both vulnerability assessment and exploitation within a single tool.

Importing Nessus to Metasploit

1. Load Metasploit "msfconsole"
2. Enter the "load nessus" command, automatically load nessus
3. Nessus_help command contains a list of all the options that can be used within Metasploit from nessus.
4. "nessus_connect" command to the nessus server
5. $ msf > nessus_connect username:passowrdhere@127.0.0.1:8834
6. Localhost > 127.0.0.1 and port is 8834 default port for nessus.

Scanning the Target

1. You are now connected to the server.
2. Check the available policies.
3. You check available policies by running the "nessus_policy_list" command.
4. Try running a scan against target system.
5. $ nessus_scan_new - 3 mypentest <target IP>
   a. -3 > name of the scan that is "mypentest" the target IP
   b. Start a scan in the background.
   c. Check progress of the scan by simply typing the
   d. $ msf > nessus_scan_status
   e. This will display the information about your current scan such as scan id status, current hosts And start time. If don not see status that mean your scan complete.

Reporting

1. If we verified our scan has been finished. We can check for the list of current reports in our database
2. $ msf > nessus_report_list
3. We will import our scan information;
4. $ msf > nessus_report_get <id>
5. We have import information we will type "access the scan results" hosts
6. "" command to list all the hosts that were scanned.
7. Use the "vulns" command from the Metasploit console to list down all the possible vulnerabilities

OpenVAS

1. Open-source network vulnerability scanner;
2. Unlike Nessus it's free;

Vulnerability Data Resources

1. Nessus, OpenVAS don't show a vulnerability it doesn't necessarily mean that the target is not vulnerable.
2. Every day, there is another zero day (a type of exploit that not discovered before) released, and Nessus and other scanners just don't update, keep a track of all the information that is out there.
3. There are huge numbers of databases that keep track of all the recently released exploits.
4. The databases contains everything needed to exploit a vulnerability. So Update your database up-to-date;
5. Vulnerability database gives you information about different types of vulnerabilities where an exploit would give you information on how to exploit those of vulnerabilities;
6. My recommendation is that you review both database simultaneously.

List of databases:

a. **Seclist.org (subscription highly recommended)**
b. **Exploit DB (exploit-db.com)**
c. **Nist (nvd.nist.gov)**
d. **Security focus (securityfocus.com)**
e. **CVE- Common vulnerability and exposure (cve.mitre.org)**
f. **1337day.com**
g. **Open-sourced vulnerability database (osvdb.org)**

h. **Exploitsearch.com**
i. **Exploitsearch.net (collecting information from various exploit database)**
j. **Packetstormsecurity.com (highly recommended)**