Finding Vulnerabilities

Contents

- Nessus
- Nmap scripting engine
- Metasploit
- Web application scanning
- Manual analysis

1. Nessus

Nessus

- Tenable Security's Nessus is one of the most widely used commercial vulnerability scanners, though many vendors provide comparable products
- Using TCP port 8834
- *root@kali:~# service nessusd start*

Nessus

Nessus

Scanner

Search Library

Advanced Scan
Configure a scan without using any recommendations.

UPGRADE
Audit Cloud Infrastructure
Audit the configuration of third-party cloud services.

Badlock Detection
Remote and local checks for CVE-2016-2118 and CVE-2016-0128.

Bash Shellshock Detection
Remote and local checks for CVE-2014-6271 and CVE-2014-7169.

Basic Network Scan
A full system scan suitable for any host.

Credentialed Patch Audit
Authenticate to hosts and enumerate missing updates.

DROWN Detection
Remote checks for CVE-2016-0800.

Host Discovery
A simple scan to discover live hosts and open ports.

Intel AMT Security Bypass
Remote and local checks for CVE-2017-5689.

UPGRADE
Internal PCI Network Scan
Perform an internal PCI DSS (11.2.1) vulnerability scan.

Malware Scan
Scan for malware on Windows and Unix systems.

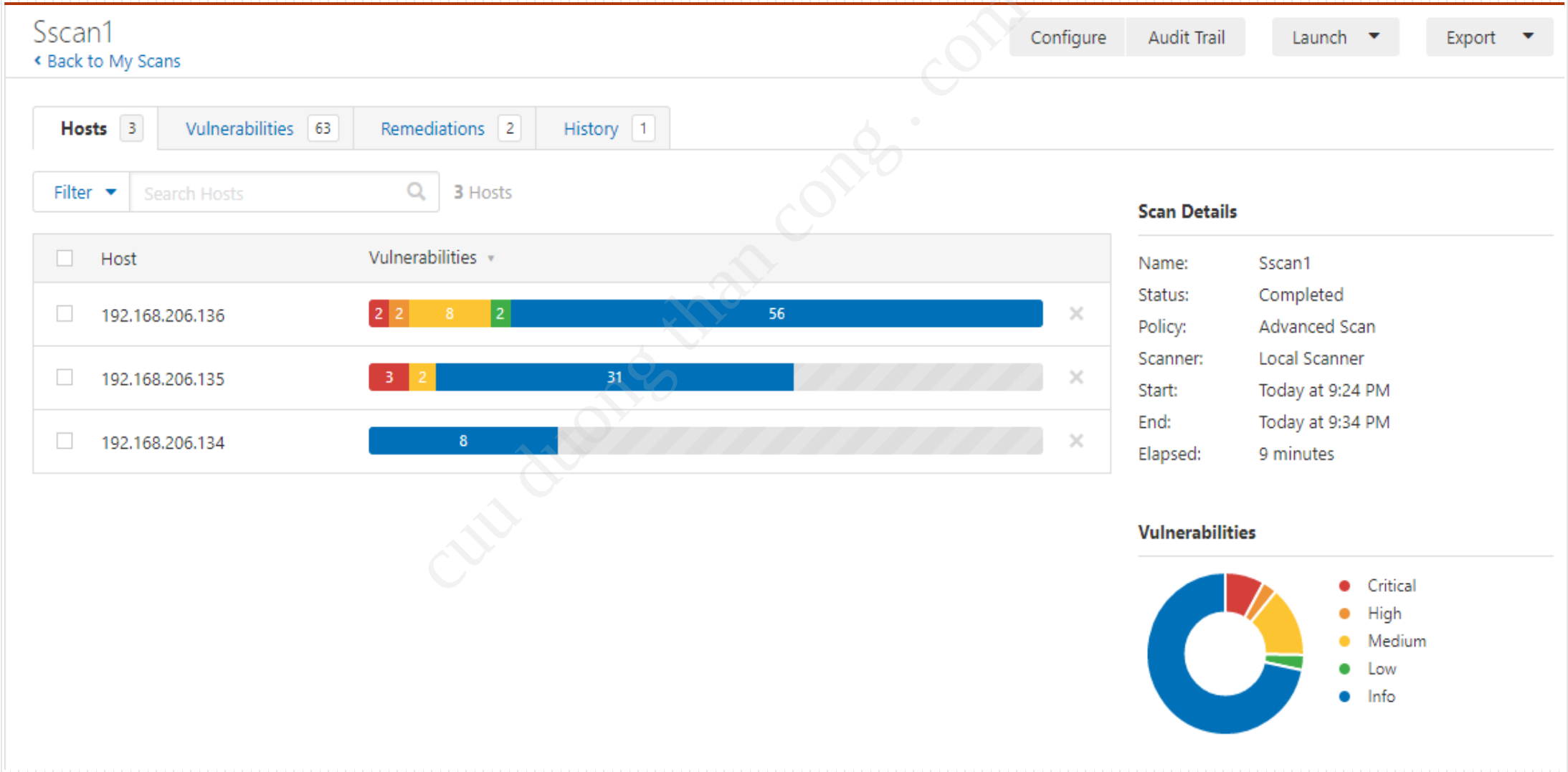
UPGRADE
MDM Config Audit
Audit the configuration of mobile device managers.

UPGRADE
Mobile Device Scan
Assess mobile devices via Microsoft Exchange or an MDM.

UPGRADE
Offline Config Audit
Audit the configuration of network devices.

UPGRADE
PCI Quarterly External Scan
Approved for quarterly external scanning as required by PCI.

Nessus



Nessus

- Nessus ranks vulnerabilities based on the Common Vulnerability Scoring System (CVSS), version 2, from the National Institute of Standards and Technology (NIST). Ranking is calculated based on the impact to the system if the issue is exploited

2. Nmap scripting engine

Nmap scripting engine

- The available scripts fall into several categories, including information gathering, active vulnerability assessment, searches for signs of previous compromises

```
root@kali:~# cd /usr/share/nmap/scripts
root@kali:/usr/local/share/nmap/scripts# ls
acarsd-info.nse                          ip-geolocation-geobytes.nse
```

Categories

auth
broadcast
brute
default
discovery
dos
exploit
external
fuzzer
intrusive
malware
safe
version
vuln

Nmap scripting engine

- #nmap --script-help <ten_catelogy>

```
root@kali:~# nmap --script-help default

Starting Nmap 6.40 ( http://nmap.org ) at 2015-07-16 14:43 EDT
--snip--
ftp-anon
Categories: default auth safe
http://nmap.org/nsedoc/scripts/ftp-anon.html
  Checks if an FTP server allows anonymous logins.

  If anonymous is allowed, gets a directory listing of the root directory and
highlights writeable files.
  snip
```

Nmap scripting engine

```
root@kali:/# nmap --script=nfs-ls 192.168.20.11

Starting Nmap 6.40 ( http://nmap.org ) at 2015-12-28 22:02 EST
Nmap scan report for 192.168.20.11
Host is up (0.00040s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 5.1p1 Debian 3ubuntu1 (Ubuntu Linux; protocol 2.0)
80/tcp   open  http        Apache httpd 2.2.9 ((Ubuntu) PHP/5.2.6-2ubuntu4.6 with Suhosin-Patch)
111/tcp  open  rpcbind     2 (RPC #100000)
```

3. Metasploit

Metasploit scanner modules

- Metasploit can conduct vulnerability scanning via numerous auxiliary modules. These modules will not give us control of the target machine, but they will help us identify vulnerabilities for later exploitation

```
msf > use scanner/ftp/anonymous

msf  auxiliary(anonymous) > set RHOSTS 192.168.20.10-11
RHOSTS => 192.168.20.10-11
msf  auxiliary(anonymous) > exploit

[*] 192.168.20.10:21 Anonymous READ (220-FileZilla Server version 0.9.32 beta
220-written by Tim Kosse (Tim.Kosse@gmx.de) ❶
220 Please visit http://sourceforge.net/projects/filezilla/)
```

Metasploit exploit Check Functions

- Some Metasploit exploits include a check function that connects to a target to see if it is vulnerable, rather than attempting to exploit a vulnerability

```
msf > use windows/smb/ms08_067_netapi

msf  exploit(ms08_067_netapi) > set RHOST 192.168.20.10
RHOST => 192.168.20.10
msf  exploit(ms08_067_netapi) > check❶

[*] Verifying vulnerable status... (path: 0x0000005a)
[+] The target is vulnerable.❷
msf  exploit(ms08_067_netapi) >
```

4. Web application scanning

Web application scanning

- Nikto

```
root@kali:/# nikto -h 192.168.20.11
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          192.168.20.11
+ Target Hostname:    192.168.20.11
+ Target Port:        80
+ Start Time:         2015-12-28 21:31:38 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.2.9 (Ubuntu) PHP/5.2.6-2ubuntu4.6 with Suhosin-Patch
--snip--
+ OSVDB-40478: /tikiwiki/tiki-graph_formula.php?w=1&h=1&s=1&min=1&max=2&f[]=x.
tan.phpinfo()&t=png&title=http://cirt.net/rfiinc.txt?: TikiWiki contains a
vulnerability which allows remote attackers to execute arbitrary PHP code. ❶
+ 6474 items checked: 2 error(s) and 7 item(s) reported on remote host
+ End Time:           2015-12-28 21:32:41 (GMT-5) (63 seconds)
```

Web application scanning

- Acunetix Web Vulnerability Scanner

5. Manual analysis

Manual analysis

- Exploring a Strange Port

```
root@kali:~# nc 192.168.20.10 3232
GET / HTTP/1.1
HTTP/1.1 200 OK
Server: Zervit 0.4 ❶
X-Powered-By: Carbono
Connection: close
Accept-Ranges: bytes
Content-Type: text/html
Content-Length: 36

<html>
<body>
hi
</body>
</html>root@bt:~#
```

Manual analysis

- Finding Valid Usernames

```
root@kali:~# nc 192.168.20.10 25
220 georgia.com SMTP Server SLmail 5.5.0.4433 Ready ESMTP spoken here
VRFY georgia
250 Georgia<georgia@>
VRFY john
551 User not local
```