



eLearnSecurity
Forging security professionals

NESSUS



PENETRATION TESTING | SECTION 3 MODULE 3 | LAB #9

LAB



1. DESCRIPTION

In this lab you will have to use and configure Nessus in order to perform a vulnerability scan against the target machine. However you are not told where the target machine is in the network. You only know it is in the same lab network you are connected to.

2. GOAL

The goal of this lab is to learn how to properly configure Nessus depending on the services running on the target machine.

3. TOOLS

The best tools for this lab are:

- *Nmap*
- *Nessus*
- *Metasploit*



4. STEPS

4.1. FIND A TARGET IN THE NETWORK

Since we do not have any information about our lab network and the hosts attached to it, the first step is to find our target!

4.2. IDENTIFY THE TARGET ROLE

Now that we know there is a host on the target network, let us scan the host and gather as much information as we can in order to properly configure the Nessus scan.

4.3. CONFIGURE NESSUS AND RUN THE SCAN

You should have identified few services running on the machine. Configure a new Nessus policy and scan depending on the scan results of the previous step.

4.4. ANALYZE AND EXPORT THE SCAN RESULTS

Once the scan completes, open the results and analyze them. You will find something very interesting! Moreover export the scan results, you may need them!

4.5. [OPTIONAL] EXPLOIT THE MACHINE

The target machine has few critical vulnerabilities. Once you finish studying the Metasploit module, start the lab over again and try to exploit the machine.



SOLUTIONS

Please go ahead **ONLY** if you have **COMPLETED** the lab or you are stuck! Checking the solutions before actually trying the concepts and techniques you studied in the course, will dramatically reduce the benefits of a hands-on lab!



[This page was intentionally left blank]



5. SOLUTIONS STEPS

5.1. FIND A TARGET IN THE NETWORK

We first need to verify which the remote network is. We can do it by running `ifconfig` and check the IP address of our `tap0` interface.

```
tap0    Link encap:Ethernet  HWaddr b6:3d:9d:26:73:b6
        inet addr:192.168.99.13  Bcast:192.168.99.255  Mask:255.255.255.0
        inet6 addr: fe80::b43d:9dff:fe26:73b6/64  Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:31 errors:0 dropped:0 overruns:0 frame:0
        TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:100
        RX bytes:3936 (3.8 KiB)  TX bytes:648 (648.0 B)
```

As we can see the target network is 192.168.99.0/24. Let's run `nmap -sn` in order to discover alive hosts on the network:

```
root@kali:~# nmap -sn 192.168.99.0/24

Starting Nmap 6.47 ( http://nmap.org ) at 2015-02-20 12:06 CET
Nmap scan report for 192.168.99.50
Host is up (0.19s latency).
MAC Address: 00:50:56:B1:D7:8B (VMware)
Nmap scan report for 192.168.99.13
Host is up.
Nmap done: 256 IP addresses (2 hosts up) scanned in 11.50 seconds
root@kali:~#
```

The previous screenshot shows that the only host alive in the network is 192.168.99.50 (besides our host: 192.168.99.13).



5.2. IDENTIFY THE TARGET ROLE

Let us run nmap in order to gather as much information as we can about our target. To do this we will run a -A scan as follows:

```
root@kali:~# nmap -A 192.168.99.50

Starting Nmap 6.47 ( http://nmap.org ) at 2015-02-20 12:08 CET
Nmap scan report for 192.168.99.50
Host is up (0.17s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE        VERSION
135/tcp    open  msrpc          Microsoft Windows RPC
139/tcp    open  netbios-ssn    Microsoft Windows XP microsoft-ds
445/tcp    open  microsoft-ds   Microsoft Windows XP microsoft-ds
MAC Address: 00:50:56:B1:D7:8B (VMware)
Device type: general purpose
Running: Microsoft Windows XP
OS CPE: cpe:/o:microsoft:windows_xp::sp3
OS details: Microsoft Windows XP SP3
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_ nbstat: NetBIOS name: ELS-WINXP, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:b1:d7:8b (VMware)
|_ smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   OS CPE: cpe:/o:microsoft:windows_xp::-
|   Computer name: els-winxp
|   NetBIOS computer name: ELS-WINXP
|   Workgroup: WORKGROUP
|_ System time: 2015-02-20T03:08:42-08:00
|_ smb-security-mode:
|   Account that was used for smb scripts: guest
|   User-level authentication
|   SMB Security: Challenge/response passwords supported
|_ Message signing disabled (dangerous, but default)
|_ smb2-enabled: Server doesn't support SMBv2 protocol

TRACEROUTE
HOP RTT      ADDRESS
1 174.71 ms 192.168.99.50

OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 27.05 seconds
root@kali:~#
```

As we can see in the previous output there are just few services enabled. Moreover, the machine is a Windows machine. Armed with this knowledge we can start configuring our new Nessus policy and scan.



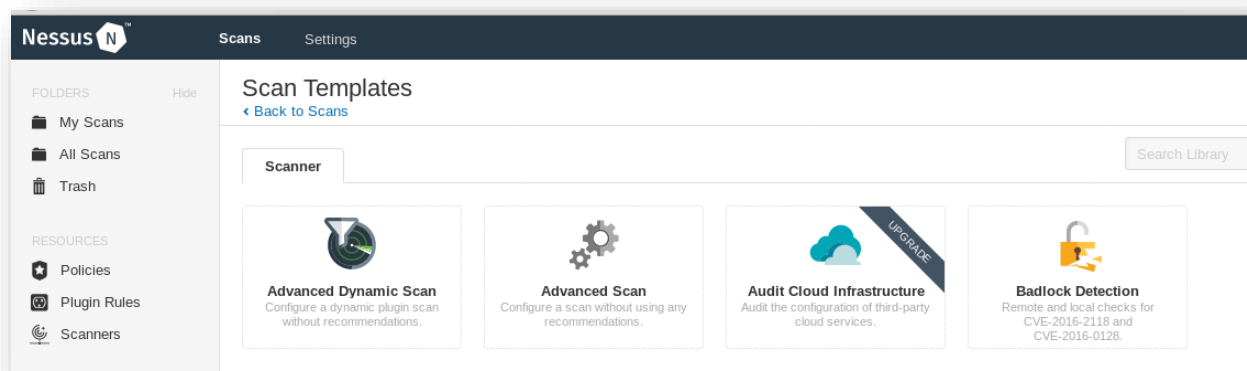
5.3. CONFIGURE NESSUS AND RUN THE SCAN

From the previous scans we can guess that the machine is a client (there are no services such as FTP, SSH, Apache or so). Moreover we know its OS is Windows XP, so we can create a new scan policy that will use only specific plugins such as Windows plugins.

In order to run the scan, we need to visit Nessus's web interface on <http://localhost:8834/> first.

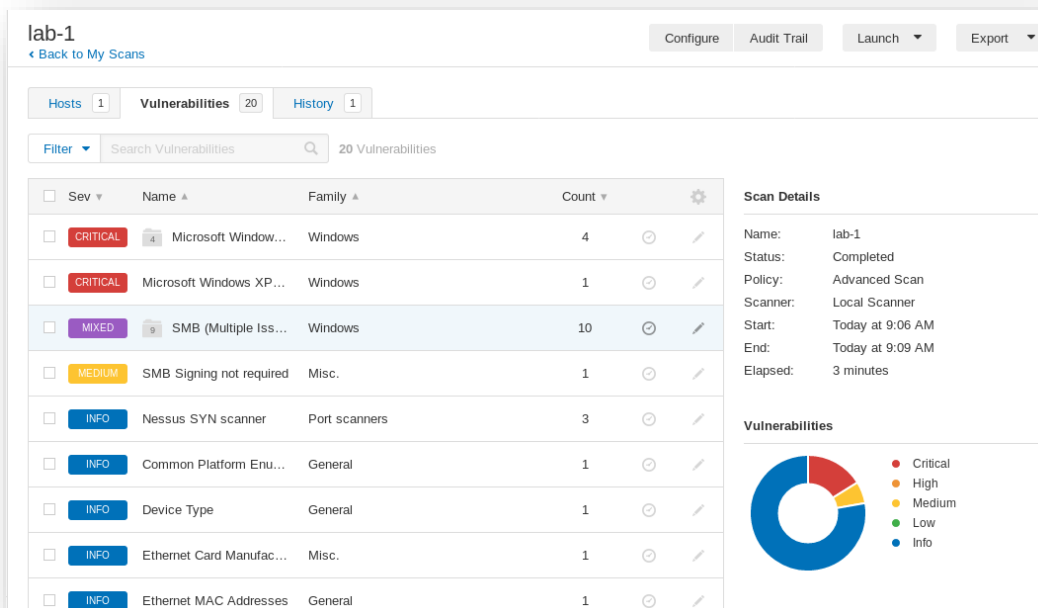
Then we should navigate to **Scans** and choose **New Scan -> Advanced scan**.

We only need to specify the target and the desired name of the scan. Now, we are ready to launch the scan.

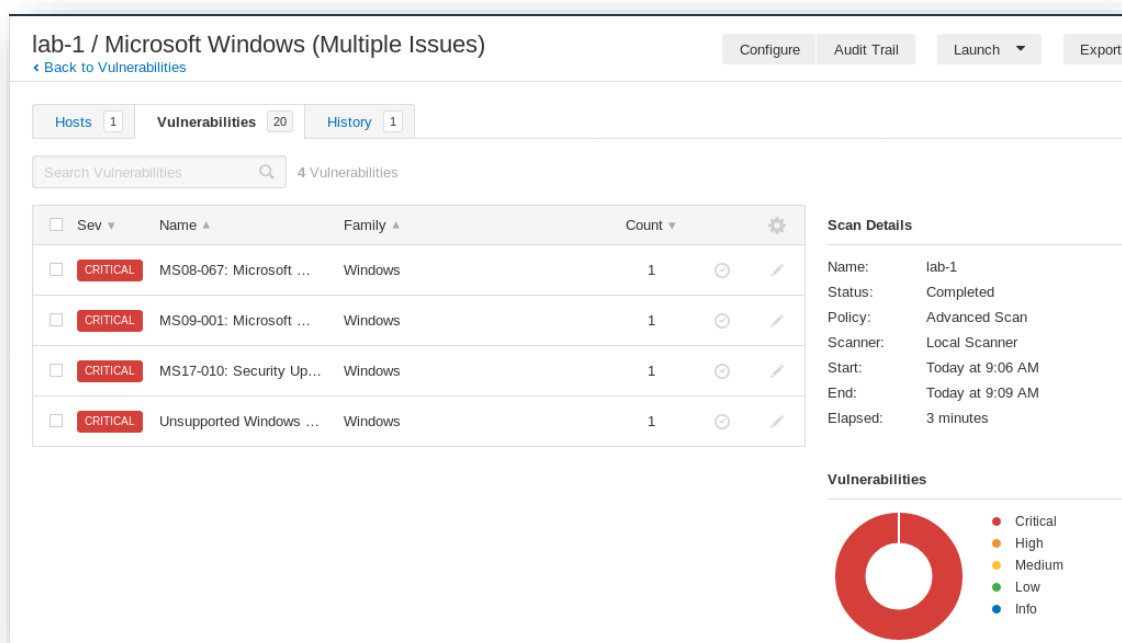


After the scan finishes, we can see the results:



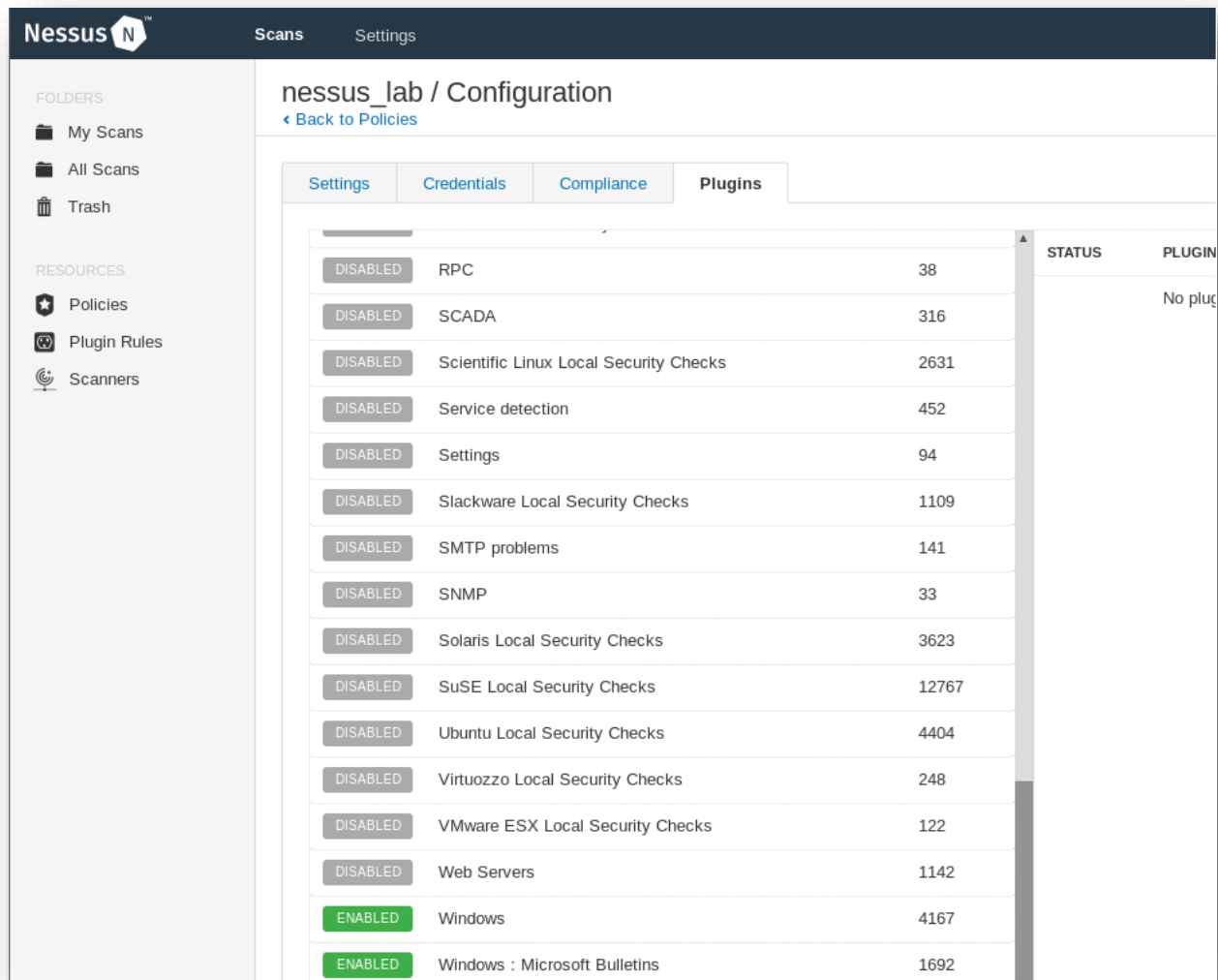


Clicking the first critical vulnerability provides us with a detailed list of the detected issues:



Note: If we wanted to use Windows plugins only so that a faster and a more specific scan is performed, this can be done as follows.

Policy -> New Policy -> Advanced Scan and configure the below.



STATUS	PLUGIN	COUNT
DISABLED	RPC	38
DISABLED	SCADA	316
DISABLED	Scientific Linux Local Security Checks	2631
DISABLED	Service detection	452
DISABLED	Settings	94
DISABLED	Slackware Local Security Checks	1109
DISABLED	SMTP problems	141
DISABLED	SNMP	33
DISABLED	Solaris Local Security Checks	3623
DISABLED	SuSE Local Security Checks	12767
DISABLED	Ubuntu Local Security Checks	4404
DISABLED	Virtuozzo Local Security Checks	248
DISABLED	VMware ESX Local Security Checks	122
DISABLED	Web Servers	1142
ENABLED	Windows	4167
ENABLED	Windows : Microsoft Bulletins	1692

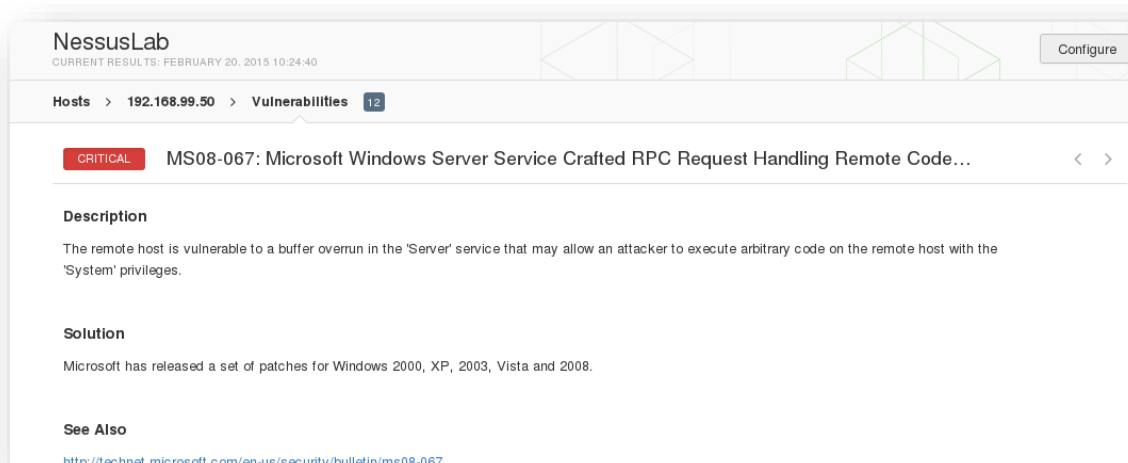
Then navigate to **My Scans -> New Scan -> User Defined** and launch the scan.



5.4. ANALYZE AND EXPORT THE SCAN RESULTS

From the scan results obtained in the previous step we can see that the machine has some critical vulnerabilities.

The most interesting one is the MS08-067:



This vulnerability allows attackers to execute code remotely! Keep it in mind if you want to exploit the machine!

5.5. [OPTIONAL] EXPLOIT THE MACHINE

In the previous step we found a very interesting vulnerability. Once you finish studying the Metasploit section of the course, come back in this lab and try to exploit it!

