Vulnerability Scanning

Nicholas Valenti, Harika Vadapalli, and Ananth Jillepalli

July 1, 2017
Version 1.1

University of Idaho

CS 439/539: Applied Security Concepts

Executive Summary

Vulnerability scanning is often one of the first lines of defense when securing a system. Tools specific to identifying potential attack surfaces can reveal out of date software, services with loose permissions, or other areas of concern. Different tools have different objectives so it's important to be familiar with a variety of ways to analyze your own security capabilities.

Prerequisites

None.

Contents

1 Objectives >

- Understand the importance of vulnerability scanning in protecting a system;
- Know which tools can be used to perform vulnerability scans;
- Use vulnerability scans to identify mitigations to attacks.

2 Scanning and Legality <>

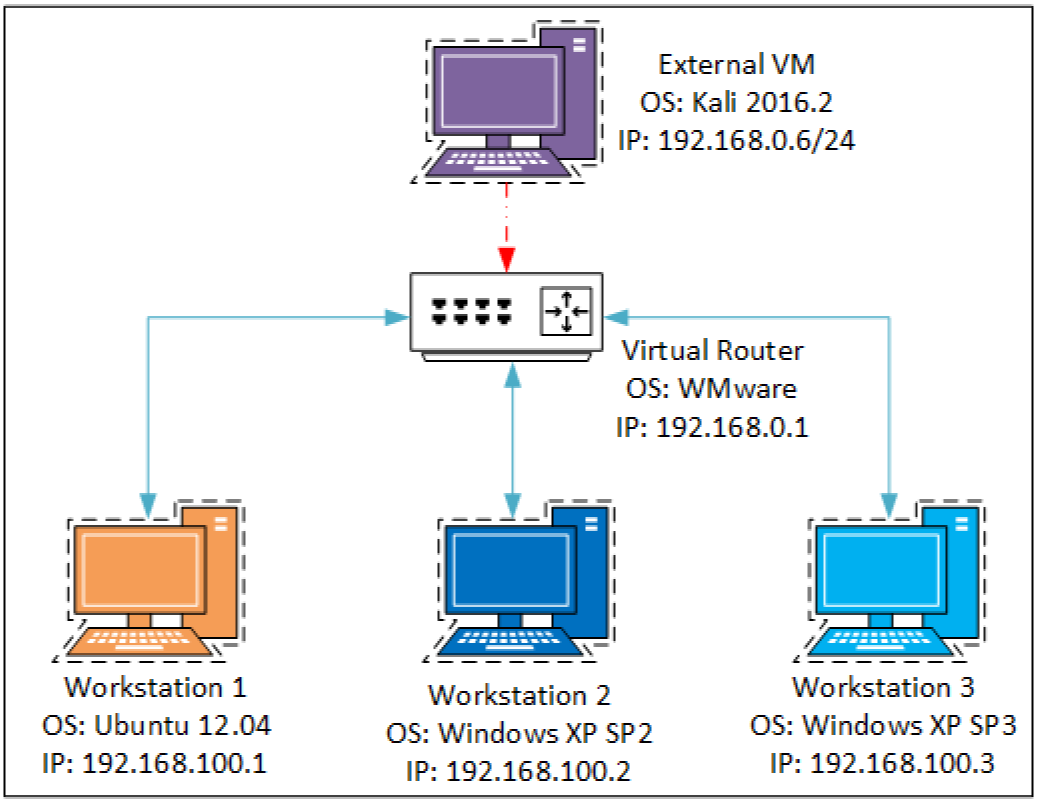
- Like with NMap, scanning a system or network is illegal without permission;
- Only perform scans on hardware and software that is isolated and you have written explicit permission from the system owner to scan;
- Some tools we will be using, such as metasploit, have even more severe legal implications if they are misused.

3 Hardware and Software Requirements <>

The tutorial was executed using the following environment:

1. A computer capable of hosting at least 4 virtual machines (VMs);
2. A virtualization software platform, e.g. VMWare or VirtualBox;
3. A) Kali VM, B) Ubuntu/Linux VM, C) Windows XP SP2 VM, and D) Windows XP SP3 VM.

Network Diagram:



4 OpenVAS

<>

- Open Vulnerability Assessment System;
- Free under GNU Public General Public License;
- OpenVAS is a framework that includes multiple services and tools to scan for vulnerabilities due to versioning, exploitable software, and more;
- Common Vulnerability Scoring System (CVSS).

1. OpenVAS split from Nessus, a comparable commercial service, in 2005 when it ceased to be open source.
2. Nessus still exists and has both a commercial and a limited free Home version.
3. OpenVAS maintains a free GNU GPL license and is free and was most recently updated with version 8.0 released in April 2015 [3].
4. Threats are ranked based on their potential to cause damage but this may differ from their actual impact. Because CVSS ranks threats based on the damage that can be caused if they are successfully exploited some threats may appear that may not pose an actual risk [1].

5 Task 1: OpenVAS [1] <>

1. Set an OpenVAS policy;
2. Run a scan on a Windows XP SP2 machine;
3. Research vulnerabilities using built in OpenVAS tools and Internet on BLUE side;
4. Have information on at least 3 vulnerabilities.

1. OpenVAS will require several pieces of information to create a scan policy including basic identification.
2. OpenVAS uses a suite of tools to probe a target for information. It is able to detect a number of potential issues and display the results of a scan in an easy to read format.
3. In order to gain additional information the internet may be used. There are a number of security related websites [1].
   - http://www.securityfocus.com/;
   - http://www.packetstormsecurity.org/;
   - http://www.exploit-db.org/;
   - http://www.cve.mitre.org/.
4. Task 1: 5-10 minutes.

6 NMap Scripting Engine (NSE) [2] <>

- NMap has expanded beyond its original scope of simple port scanning and now contains a scripting engine with several publicly available scripts;

- Scripts can also be written by users;

- Kali stores scripts in `/usr/share/nmap/scripts`;

- The **-sC** flag will tell NMap to run all scripts in the default category in addition to doing a port scan [1];
  Additional information can be found with the command `nmap -script-help <category>`.

Some NSE scripts can harm target systems. While we will not be using them there are entire sections dedicated to malware, DDOS, and other exploitation. It is important to use the help functions before running any NSE scripts in order to determine whether or not they're dangerous [2].

7 Challenge 1: NSE <>

1. Use the NMap Scripting Engine to run a script scan on all found machines;
2. Get information on the ftp-anon script from NMap's help function;
3. Use NSE to run only the ftp-anon script.

1. Vulnerable machines might be found on a different subnet.
2. We already know that the **-sC** flag will run all default scripts. How can we run scripts in other categories?
3. Try using the built in help in order to discover how NSE handles single script execution. What other scripts can you find that get you results? Research using the Internet if you get stuck.
4. Deliverable: What does this script look for and are there any machines that are susceptible.

8 Metasploit [4] <>

- The Metasploit Framework is a widely used penetration testing framework;
- Metasploit can be used to quickly assess the actual impact of a found vulnerability;
- Public exploits can be modified in order to work in your environment;
- Always be vigilant, not all public exploit code works as advertised.

1. There is both an open source version and a commercial version owned by Rapid7 [4].
2. Many of the same websites as listed in the NMap portion of this tutorial can be used to research exploits [1].

9 Task 2: Starting Metasploit [1]

The Metasploit console can be started using these commands:

```
root@kali:~# service postgresql start;
root@kali:~# service metasploit start;
root@kali:~# msfconsole.
```

1. PostgreSQL is used by Metasploit to keep track of your actions.
2. msfcli is a command line interface that can also be used to interact with metasploit without having to run the Metasploit console directly. We won't be using it in this tutorial.
3. In a GUI based system Metasploit will be listed under programs and can be launched this way as well, but will open the same console.

10 Challenge 2: Find information on the MS08-67 patch <>

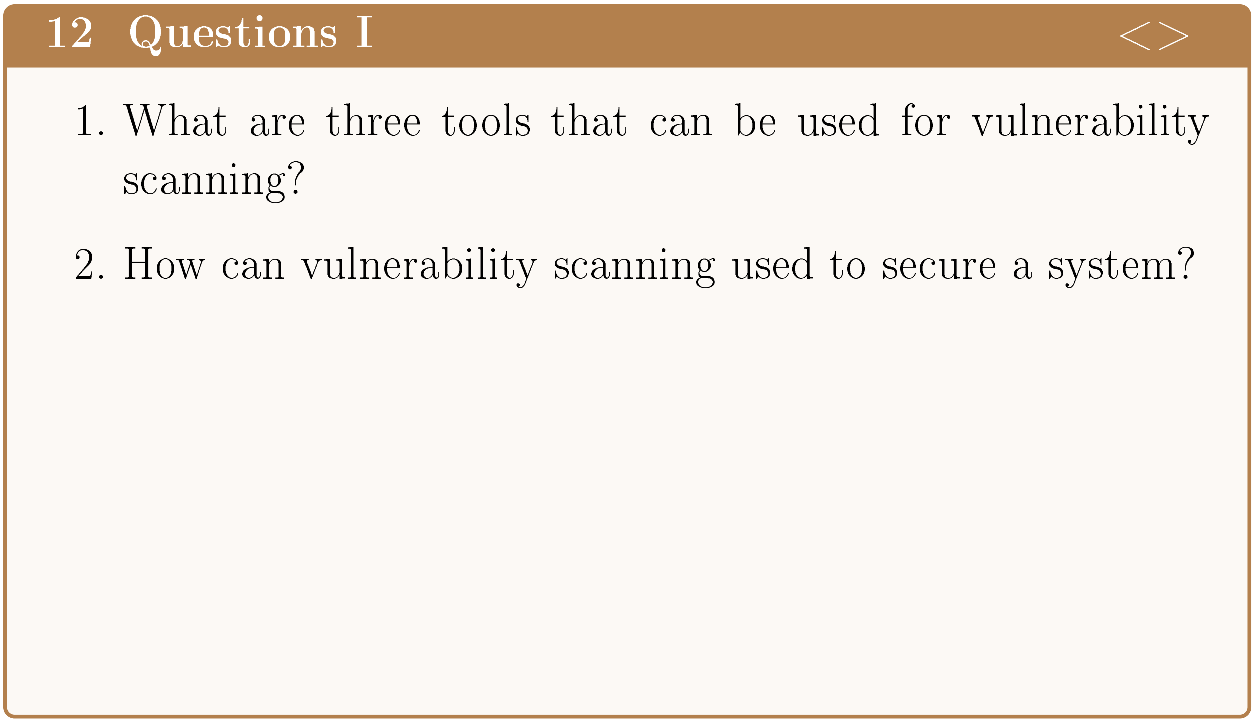
1. Use Metasploit's built in search function on RED;
2. Feel free to use the Internet on BLUE as well;
3. What is the issues that the MS08-67 patch resolved?
4. What platforms is it used on and how was it fixed?

1. MS08-067 was a patch that fixed the ms08_067_netapi vulnerability in 2008 (hence ms08) [6].
2. The vulnerability is commonly known and affects many Windows XP machines today, affecting a flaw in the NetAPI32.dll file.
3. We can scan for out of date patches or the signs of out of date services using OpenVAS, NMap, or even metasploit. Usually scanning is done when there is a suspected vulnerability and we can use our results to find out what is and isn't up to date. Remember the number one mitigation against known vulnerabilities such as the public Metasploit database is patching your software.
4. Deliverable: a report on the MS08-67 patch and the exploit it addressed, class discussion as information is discovered.
5. Time 5-10 minutes.

11 Metasploit Scanning [1] <>

1. Similarly to NMap, Metasploit has evolved beyond its original design and now incorporates vulnerability assessment;

2. Metasploit Scanner Modules allow us to identify vulnerabilities that might be exploited during an attack.



12 Questions I

1. What are three tools that can be used for vulnerability scanning?
2. How can vulnerability scanning used to secure a system?

- Many examples of tools are found throughout the tutorial.
- What is an attack surface? What resources do we have beyond the ones available in Kali?

1. OpenVAS/Nessus, NMap, Nikto, Metasploit, XAMPP, etc;
2. Identifying an attack surface, finding old versions of software, find neglected ports, etc.

13 Task 3: Metasploit Modules <>

1. Metasploit comes with many modules that can be used to do everything from scan to actual delivery of payloads;
2. We can use a scanner module to gain information about a target [4];

   msf > **use scanner/ftp/anonymous**;
3. Use **show options** to find more information about your current module;

- When loading a module (such as **scanner/ftp/anonymous**) the msf command line changes to reflect which module is currently in use [4];
- The **show options** command will show targets, ports, and more information that we will go over in more detail in the next slide.

14 Metasploit Modules [1]

Metasploit Options:

- RHOST;
- RPORT;
- SMBPIPE;
- Exploit Target.

- RHOST is the remote host Metasploit is targeting.
- RPORT is the port we are targeting and can be set manually. In our case if there is a default port that the currently loaded module uses it will be set automatically.
- SMBPIPE is out of the scope of this tutorial but is essentially the medium we are communicating across on the network.
- Exploit Target details the specific operating system and version we are targeting. By using the **show targets** command we can see what the possibly vulnerable targets for our current exploit can be. Automatic targeting will attempt to fingerprint the target and select an appropriate payload if it can.

15 Challenge 3: Metasploit Scanning <>

1. Use the **scanner/ftp/anonymous** module to scan machines on your local network;
2. How many systems can you find that allow anonymous FTP?
3. Use Internet on BLUE to find other scanning modules that could be used;
4. When you're satisfied change your module to the ms08_067_netapi exploit we researched earlier.

1. Use NMap to find potential targets on your network.
2. How much additional information can you find about these systems in an unobtrusive way?
3. The module we used earlier is pathed at **windows/smb/ms08_067_netapi**. How do you change your active Metasploit module?
4. Deliverable: a brief report with any found systems that have open FTP (we found this earlier using NSE so this challenge should be brief), class discussion about other scanning modules.
5. Time: 5-10 minutes.

16 More Metasploit Scanning [1]

<>

- Metasploit can be used to connect to a target to see if it's vulnerable without actually delivering a payload;
- Set RHOST to the IP address of the Windows XP SP2 machine and make sure the proper module is set;
- Use the **check** command to probe the specified target;
- Check only works on some supported modules.

17 Task 5: Metaspoit Payload Delivery <>

- Post-scanning of our Windows XP SP2 target, lets take a moment to see just how vulnerable an unpatched system is;
- Make sure RHOST is set correctly and the proper module is loaded into Metasploit;
- A list of compatible payloads can be found by using the **show payloads** command.

18 Task 5 (Cont): Metasploit Payload Delivery <>

- Use the **exploit** command to launch the payload once you're happy with the settings;
- Observe and make a note of subsequent happenings.

1. Gaining root access or setting up reverse shells is usually a somewhat labor intensive process;
2. This is not even the easiest way to exploit a vulnerable system.

19 Challenge 4: Windows XP SP3

<>

1. One of the biggest tools in our defensive arsenal is patching;
2. Find the Windows XP SP3 machine on your network and scan it using all the tools you have so far;
3. How many vulnerability differences can you find between the two? (Note that they are both largely unpatched);
4. BE CAREFUL not to push a payload on this machine, it can cause damage and will probably be noticed. Remember you want to defend your network, not destroy it!

- Time: up to 15-20 minutes as available;
- There are a lot of vulnerabilities on both machines, it might take time to find differences;
- Deliverables: a list of any found vulnerabilities.

20 Nikto [7] <>

1. Nikto is like OpenVAS for network services;
2. Checks for dangerous files, outdated versions of services, server options, etc.;
3. In order to run a scan use **nikto -h <IP Address>**;
4. Full feature list can be found at http://cirt.net/Nikto2.

21 Challenge 5: Nikto

<>

1. There is a metasploitable Ubuntu machine located on your local RED network;
2. If you haven't already found it do so now and run a Nikto scan on it (RED side);
3. Research some of the potential issues Nikto discovered:
    - Research can be done on the Internet.

- Time: 5-10 minutes.

22 Challenge 6: Mitigations [1]

<>

1. There is a metasploitable linux machine located on your local network;
2. Use everything you've learned to identify and close as many attack surfaces as you can;
3. Assume the owner of the metasploitable machine wants to keep FTP, HTTPS, and IRC open.

- What services are required? How do you handle services that might be vulnerable but are required for business or personal purposes?
- Feel free to use material from previous tutorials such as firewalls to assist you in your efforts.
- Time: 30+ minutes.

23 Bonus Slide: Armitage [5]

- Armitage is a utility suite built around NMap, Metasploit, and other tools to provide easy access to the functions of all programs under its umbrella.
- It is capable of sharing logs and information between team members as well as making exploit suggestions, and remembers details about systems found from any platform.
- Check out http://www.fastandeasyhacking.com/manual, for more information on Red Team Operations.

24 Conclusion <

- Vulnerability scanning is an important tool in any security professional arsenal;
- Keeping your tools and services up to date and understanding what is going on with your network and ports.

A significant source for this tutorial is: [1]

Changelog:

Vulnerability Scanning			
Ver.	Date	Authors	Changes
v1	Feb 13th 2017	Nicholas Valenti and Harika Vadapalli	Initial Tutorial.
v1.1	July 1st 2017	Ananth Jillepalli	Standardization (network layout diagram, edits, consistency, TeX markup cleaning, and more).

References

[1] Weidman, Georgia, "Penetration Testing: A Hands-On Introduction to Hacking", No Starch Press. San Francisco, CA, 2014.

[2] Gordon Lyon, Charles McFarland, "NMap Scripting Engine (NSE)", Insecure.org. https://nmap.org/book/man-nse.html

[3] N.A., "About OpenVAS Software", Systems Characteristics Producer http://www.openvas.org/software.html

[4] ckirsch, "What is Penetration Testing", Rapid7, https://community.rapid7.com/docs/DOC-2248

[5] N.A., "Fast and Easy Hacking", Strategic Cyber LLC. http://www.fastandeasyhacking.com/manual

[6] N.A., "Microsoft Security Bulletin MS08-067 - Critical", Microsoft. https://technet.microsoft.com/en-us/library/security/ms08-067.aspx

[7] Chris Sullo and David Lodge, "Nikto2", CIRT.net. https://cirt.net/Nikto2