Warning! Unexpected port scans are rude, and possibly even illegal! Port scans can set off intrusion detection systems and get us all into trouble. Don't scan other people's servers, just scan machines you have permission to scan. The only machines you should scan in this project are machines in S214, or on your own network at home.

What You Need for This Project

- Two computers running any version of Windows, with Internet access.
- You need administrator privileges on both computers.

Find a Partner

1. You will need two machines working together for this project: choose one to be the **Scanner** and the other to be the **Target**.

Use Windows 7 for Both Machines

2. Start both the **Scanner** and **Target** machines. Log in as **Student** with no password.

Installing the Nmap Security Scanner on the Scanner Machine

3. On the **Scanner Machine**, open Firefox. Go to **nmap.com**
4. In the upper center portion of the page, click **Download**.
5. Scroll down to the "Windows (NT/ME/2K/XP/Vista) binaries" section. Click the link labeled "**Latest stable release self-installer**". When I wrote these instructions, it was **nmap-4.76-setup.exe**.
6. Save the installer file on your desktop.
7. Minimize all windows. On your desktop, double-click the nmap installer file. Click through all the security warnings and install the software with the default options. It may also install a WinPCap program, that is normal.

Finding the IP Address of the Target Machine

8. On the **Target Machine**, click **Start**. In the **Search** box, enter **CMD** and press the Enter key.

Target IP: _____

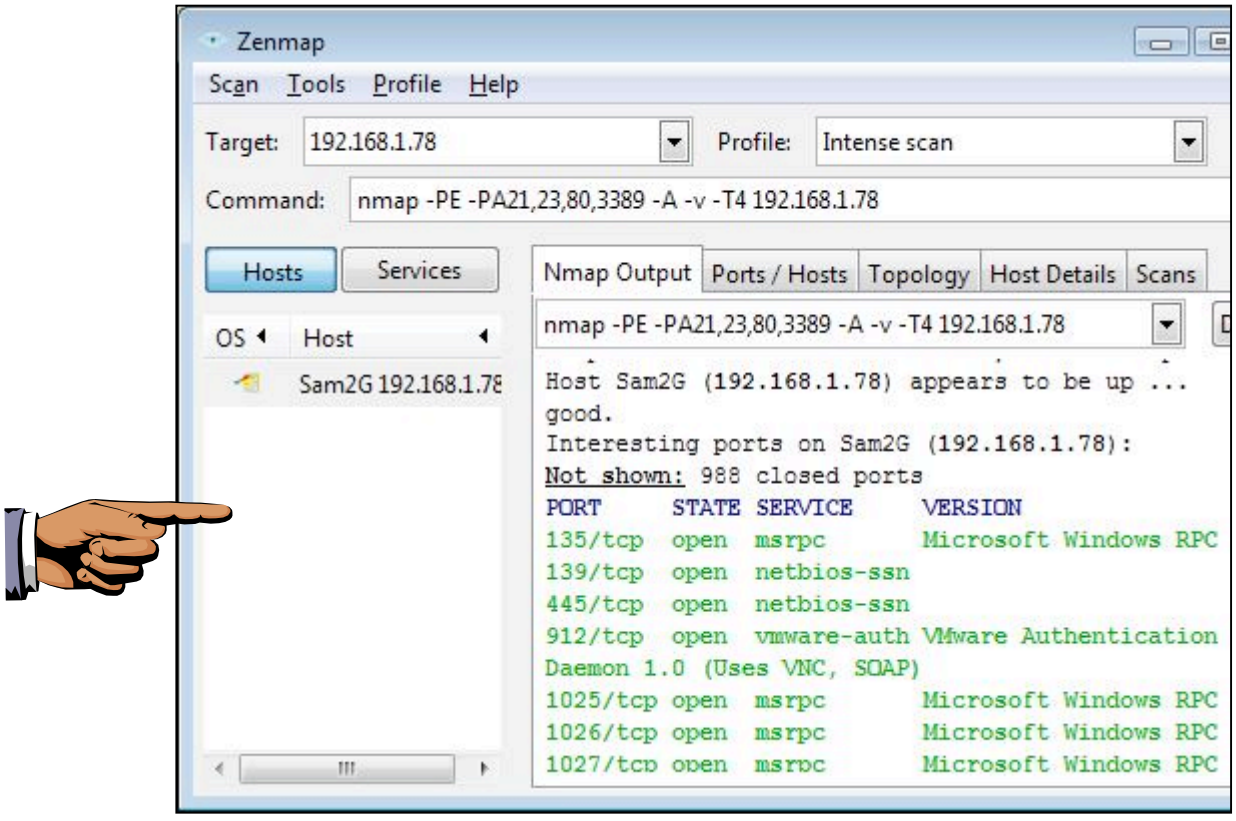
9. In the **Command Prompt** window, enter the **IPCONFIG** command and press the Enter key. Several IP addresses appear. Scroll back to see the first few addresses, and find the one that starts with **192.168.1**. That is the IP address of the network interface that connects to the room's LAN. Write that address in the box to the right on this page.

Turning the Target Machine's Firewall Off

10. On the **Target Machine**, press the Windows logo key on the lower left of the keyboard (⊞). Type **FIREWALL** into the search box.
11. "**Windows Firewall**" should appear in the Programs list. If it's not already highlighted, press the down-arrow as needed to highlight it. Then press the Enter key.
12. A "Control Panel ► System and Security ► Windows Firewall" box opens. On the left side, click "**Turn Windows Firewall on or off**". If a "User Account Control" box pops up, click **Continue**.
13. In the "System and Security ► Windows Firewall ► Customize Settings" box, click both of the "**Turn off Windows Firewall (not recommended)**" buttons. Click **OK**.

Scanning the Target Machine

14. On the **Scanner Machine**'s desktop, double-click "**Nmap – Zenmap GUI**".
15. In the **Zenmap** window, in the **Target:** box, type the "**Target IP**" you wrote in the box on the previous page. Click the **Scan** button.
16. Nmap results appear in the lower pane. Scroll down to the main chart showing "**PORT STATE SERVICE VERSION**" in blue letters with green results under it, as shown below on this page.



17. The purpose of this scan is to determine what ports are open, so you can determine how secure a device is, and whether a firewall is working properly. Nmap should find at least one port open on the machine—almost all Windows machines have ports 135, 139, and 445 open. There may be other ports open as well. Those ports are potential vulnerabilities an attacker could use to enter your computer.

Saving a Screen Image

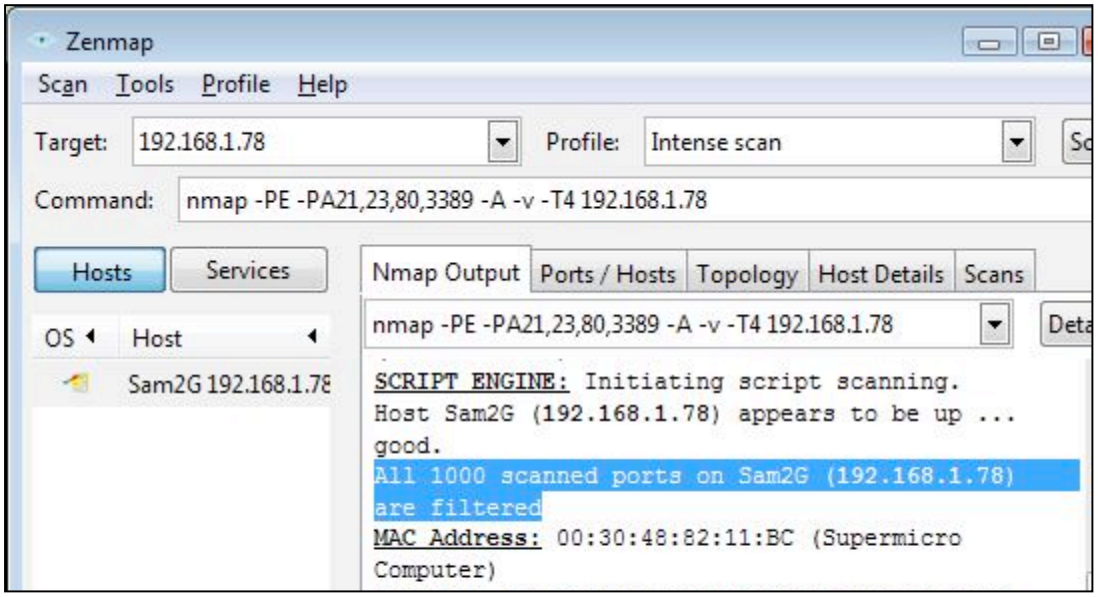
18. On the **Scanner Machine**, make sure the Zenmap window is visible, showing at least one open port.
19. Press the **PrintScrn** key to copy the whole desktop to the clipboard.
20. Click **Start**. Type **PAINT**. Click **Paint**. Click in the Paint window and press **Ctrl+V**.
21. Save the image with the filename **Your Name Proj 4a**. Select a **Save as type** of **JPEG**.

Turning the Target Machine's Firewall On with No Exceptions

22. On the **Target Machine**, press the Windows logo key on the lower left of the keyboard (⊞). Type **FIREWALL** into the search box.
23. "**Windows Firewall**" should appear in the Programs list. If it's not already highlighted, press the down-arrow as needed to highlight it. Then press the Enter key.
24. A "Control Panel ► System and Security ► Windows Firewall" box opens. On the left side, click "**Turn Windows Firewall on or off**". If a "User Account Control" box pops up, click **Continue**.
25. In the "System and Security ► Windows Firewall ► Customize Settings" box, click both of the "**Turn on Windows Firewall**" buttons. Also check both of the "**Block all incoming connections, including those in the list of allowed programs**" boxes. Click **OK**.

\Scanning the Target Machine

26. On the **Scanner Machine**'s desktop, double-click "**Nmap – Zenmap GUI**".
27. In the **Zenmap** window, in the **Target:** box, verify that the "**Target IP**" is entered correctly. Click the **Scan** button.
28. Nmap results appear in the lower pane. Scroll down and find this message "**All 1000 scanned ports … are filtered**", as shown below.



29. Now all ports are closed. This is a safer setting for the firewall, but it will prevent the machine from sharing files or printers.

Saving a Screen Image

30. On the **Scanner Machine**, make sure the Zenmap window is visible, showing the message "**All 1000 scanned ports … are filtered**".
31. Press the **PrintScrn** key to copy the whole desktop to the clipboard.
32. Click **Start**. Type **PAINT**. Click **Paint**. Click in the Paint window and press **Ctrl+V**.
33. Save the image with the filename **Your Name Proj 4b**. Select a **Save as type** of **JPEG**.

Turning in Your Project

34. Email the JPEG images to me as attachments to a single email message. Send it to: **cnit.120@gmail.com** with a subject line of **Proj 4 From** *Your Names*, replacing *Your Names* with the complete names of both partners. Send a Cc to yourself.

Last Modified: 8-21-12