COSC362S2 (Data and Network Security) Assignment

DongSeong (Dan) Kim, Matthew Ruffell
Department of Computer Science and Software Engineering,
University of Canterbury
dongseong.kim@canterbury.ac.nz
msr50@uclive.ac.nz

10 August 2017

1 Introduction

1.1 Administration

This assignment is a part of the COSC 362 assessment process. It is worth 20% of the final marks. You will work in groups of two people, it is not an option to work alone or in larger groups, unless you have very convincing reasons and have obtained explicit approval from me (normally by e-mail or in person). Submissions by individuals or larger groups without such approval will not be marked. Please submit the after mentioned deliverables no later than **5pm, 11th October 2017**. Note that no late assignments will be accepted without prior approval.

1.2 Outline

This assignment is to give you a brief idea of how a penetration tester would go about their daily jobs, and to help you understand what kinds of attack vectors exist, and what an attacker can achieve once they are inside your system. In this assignment, you will be tasked with using two different vulnerability scanners, Nessus and OpenVAS, to scan for vulnerabilities in Metasploitable and Windows XP SP2 virtual machines. Afterwards, you will be using your discovered vulnerabilities to exploit those virtual machines with the help of publicly available exploits in Metasploit and Armitage. Finally, you will be tasked with using Snort to detect these attacks and making alerts when exploit payloads and port scanning activities are present on the network.

1.3 Help

This assignment can get confusing and frustrating at times when things don't work. Computer Security is a very fragile world and things go wrong all the time. If you are having problems, try not to help out your classmates, and instead ask for help from your tutor, Matthew. You can email him or ask him questions in labs. When the worst comes to worst, delete your virtual machines and start again. It is a good idea to write your report on the Lab machines or your own personal machines, as you may lose data on the virtual machines. Always save your report and backup data often onto a USB stick or similar to prevent data loss.

2 Setting Up The Environment

2.1 Getting the Virtual Machines

In this assignment, you will be using Kali Linux, Metasploitable and Windows XP SP2 as your primary virtual machines. To not use up too much space on your home network drives, we have installed the virtual machines for you on the network. This takes up less space, and you can then use them on any computer in the labs. You may also use your own personal computers, but you will need to create your own virtual machines. To get them in labs, run the following commands:

```
# Get Kali Linux
/netfs/share/bin/cosc362vm-kali
# Get Windows XP
/netfs/share/bin/cosc362vm-winxp-ie8
# Get Metasploitable 2
/netfs/share/bin/cosc362vm-metasploitable2
```

Kali Linux is a offensive security based Linux distribution, that is, it is designed to attack and break security, and is widely used by the security testing community. Kali is the successor to the excellent Backtrack Linux distribution, but is more easily updatable, more stable and has more hacking tools preinstalled.

Metasploitable is a intentionally vulnerable virtual machine designed by Rapid7, the company behind Metasploit. Metasploitable is built on an Ubuntu 8.04 base, and has been weakened and many old, vulnerable services have been installed in order to teach you how to hack. Metasploitable does not represent the security of Linux boxes, and is only used for educational purposes.

Windows XP is used because there are plenty of good, reliable exploits available publicly for beginners to be able to hack a real desktop operating system. At the time of writing, Windows 7 is just a little bit too difficult to hack for beginners, but this will change.

2.2 Configuring Networking

You need to set up some networking, to use a "host only" network. This allows you to launch attacks in a safe and controlled environment. If you launch attacks across the University network, there is a risk that the University network will detect and report your attacks, which might get you into some trouble. So please, configure your machines correctly.

2.2.1 Setup A Host Only Adapter

Set up a "host only" network adapter by opening Virtualbox, and going to File > Preferences > Network > Host only Networks. Press the + (Plus) button to create a new one. An adapter vboxnet0 will appear. Press Ok and exit.

2.2.2 Configure Host Only Networking

On each Kali virtual machines, right click them and select "Settings" and go to the network tab. In here, select Attached to: "Host only adapter" and make sure vboxnet0 is selected. In Promiscuous mode, select "Allow VMs" and make sure the cable is connected. Do the same for the Windows XP VM, but don't enable promiscuous mode.

2.2.3 Tips

You should turn off the firewall in Windows XP, as it will makeblock attacks. Go to Control Panel > Security Center > Firewall > Off.
Nessus will only work on Kali Linux if the MAC address of the adapter does not change. If you see a "feed error" try resetting your adapter to 080027A1B6E6 in Virtualbox network settings.

2.2.4 How to Get Internet Access on Kali Linux

You might need internet access in Kali in this assignment. Make sure you internet enable your lab machine (search for Python Internet Enabler / pie) in Mint, and enable. Then in Virtualbox, go to VM > Settings > Network, and change "Host only" to "NAT". Make sure you put it back to "Host Only" when you are done, otherwise you will not be able to interact with the Windows XP and metasploitable virtual machines. Note you may need to use the "cable connected" option to make the change take effect. Also please do not connect Windows XP or Metasploitable to the internet, they are old and horrendously insecure operating systems. You WILL get owned if you connect them to the internet, and within ten minutes. You have been warned.

2.3 Starting Up and Checking Configuration

Start up your virtual machines. The username and password for Kali Linux is `root` and `toor`. Open Terminal and run `ifconfig`, noting down the IP addresses of the machine. Kali should be 192.168.56.101. Windows XP should automatically log in. Open `CMD` and run `ipconfig` and the IP address should be 192.168.56.102. Metaploitable logins are msfadmin and msfadmin. The IP address should be 129.168.56.103. Make sure you can `ping` each virtual machine, and if everything works, start the assignment.

Note the credentials for Kali Linux are `root:toor`

3 [100 Marks Total] Assignment Tasks

3.1 [20 Marks Total] Vulnerability Scanning

Vulnerability scanners attempt to find and report vulnerable services running on remote machines. They do this by enumerating services through intelligent port scanning, and comparing the version numbers of software to large databases that record what versions of software have known vulnerabilities. Reports are then generated to get a good idea of vulnerable hosts on the network.

3.1.1 [5 Marks] Use OpenVAS for Vulnerability Scanning

Start OpenVAS in Kali by first running the following commands to reset the scanner service: `openvas-stop`, `openvas-start` and `openvas-start` again. Then you can open Firefox and connect to the login page on `localhost:9392`, with username `admin` and password `362openvas`.

Now scan your Metasploitable and Windows XP virtual machines. How many vulnerabilities are found? What is the difference between "Full and Fast" and "Slow and Very Deep Ultimate"? Show some screenshots of how many vulnerabilities are found, and write a few sentences explaining what you see. What kinds of vulnerabilities are reported? How severe? Save your reports (as a PDF) and export your results.

3.1.2 [5 Marks] Use Nessus For Vulnerability Scanning

Start Nessus in Kali by opening Firefox and connecting to the login page on `localhost:8834` with username `admin` and password `362nessus`. Scan both your Metasploitable and Windows XP virtual machines. How many vulnerabilities are found? Show some screenshots of how many vulnerabilities are found, and write a few sentences explaining what you see. What kinds of vulnerabilities are reported? How severe? Save your reports (as a PDF) and export your results.

3.1.3 [10 Marks] Compare OpenVAS and Nessus

How does OpenVAS and Nessus compare? Please write a detailed comparison comparing: vulnerabilities found, how many overlapping vulnerabilities there were, what sort of detail or information each scanner outputs about vulnerabilities, time to complete scans, etc. Around one page is enough, and please use tables to compare features / vulnerabilities found.

3.2 [40 Marks Total] Exploitation and Exfiltration

3.2.1 Setting Up Metasploit and Armitage

You will be using the Metasploit Framework to do all the heavy lifting. You can find out more about Metasploit here: `https://www.metasploit.com/`. To make this easier to use, you will be using Armitage, a GUI designed for Metasploit. Launch Armitage in you Kali Attacker, and screenshot it running. You may need to enable the Metasploit background services first before Armitage will launch. You can do this by running the commands the Armitage error window tells you (in the Kali 2.x section), or by launching Metasploit first. This might help: `http://docs.kali.org/general-use/starting-metasploit-framework-in-kali`

3.2.2 Importing Scan Results into Metasploit Database

Import the reports generated by either Nessus or OpenVAS and show the hosts appear in Armitage's window. Or you can scan for vulnerabilities directly from Armitage by launching a Nmap Scan. You can do this from Hosts > Nmap scan > Intense Scan (whatever variation you want). Once you have either imported or completed scans, click a host and select Attacks > Find Attacks. Take a screenshot of your efforts. The `hosts` and `vulns` commands supplied by Metasploit may be useful.

3.2.3 [10 Marks] Exploiting Metasploitable

You now need to leverage some exploits to gain root access to the Metasploitable VM. Right click the Metasploitable Machine in Armitage and select the Attacks menu. From there, try and find an exploit that triggers a vulnerability. You will know you have succeeded when you see red bolts of lightning take over the machine. For more attacks, look in the "exploit" folder in the side bar, and look for Linux specific exploits. Hint: Exploits may work more reliably if you tick the "Use a reverse connection" box. When an attack succeeds, there will be a new Meterpreter right click menu option, which lets you open shells on the Machine as root. Find multiple ways to get inside the Metasploitable VM (at the bare bare minimum 2, I am expecting 4+ from everyone. Matthew knows at least 8 different ways off the top of his head).

3.2.4 [10 Marks] Harvesting Credentials from Metasploitable

Metasploitable is running numerous services, as you can see from Nmap scans and your vulnerability reports. But what are the credentials to these services? Find, harvest and explore the Metasploitable VM and try to figure out the user names and passwords to as many services as possible. When you find some, try logging into them from Kali terminal, or inside Armitage, and see what havoc you can muster.

3.2.5 [10 Marks] Exploiting Vulnerabilities In Windows XP

Time to leverage some exploits in the Windows XP VM. Right click the Windows Machine in Armitage and select the Attacks menu. From there, try and find an exploit that triggers a vulnerability. You will know you have succeeded when you see red bolts of lightning take over the machine. For more attacks, look in the "exploit" folder in the side bar, and look for Windows specific exploits. Screenshot how you launched attacks, what options you used and what the results are. When the attack succeeds, there will be a Meterpreter menu, and you can explore post exploit operations. Find multiple ways to get inside / crash the Windows XP VM (at the bare minimum 2 ways, I am expecting 3-4, Matthew knows about 6 different ways off the top of his head).

3.2.6 [10 Marks] Exploring Post Exploitation Capabilities in Windows XP

Windows XP has a graphical user interface, compared to the headless Metasploitable VM which just presents a console prompt. Because of this, you can do a lot more post exploitation wise. On your successful exploits, there will be a Meterpreter menu. Try out multiple post exploitation activities, such as opening shells, taking screenshots, uploading / downloading files, viewing / killing processes, remote control over VNC, installing keyloggers etc. Document them. How much can you do? How can you gain persistence?

3.3 [40 Marks Total] Detection and Prevention

3.3.1 Perform a Port Scan With Nmap

Run Nmap from the Kali Attacker and scan the Metasploitable and Windows XP machines. Try and use at least four different Nmap flags, and document what they do. Show screenshots of the output of Nmap. Note, run Nmap from Terminal, not Armitage.

3.3.2 [10 Marks] Mitigate Port Scanning With Snort

Modify the snort configuration file on the Kali Victim to detect the two port scans performed in the previous section (3.3.2). You will need to add or modify rules and preprocessor settings to achieve this. Document what changes you made, and show the rules working by performing a scan and taking a screenshot of the alerts generated. You can configure snort properly by modifying the snort configuration file `/etc/snort/snort.conf` and write down what settings you changed. You can then run snort with these custom settings with the command `snort -c /etc/snort/snort.conf -l /var/log/snort`

3.3.3 [5 Marks] Mitigate Exploitation With Snort

Modify the snort configuration file on the Kali Victim to detect the attacks carried out on the Windows XP virtual machine from section 3.2.5. You may need to use wireshark to work out what the packet contents are. Document what changes you made, and show the rules working by performing a scan and taking a screenshot of the alerts generated. Note that snort rules are overly complex, and I fully expect you to Google for rules that match the exploits you use. Please don't spend too much time looking for rules that work, as there are MANY variants of particular exploit payloads, and frustratingly, there aren't many snort rules that match payloads sent by Metasploit. If you get stuck, ask Matthew.

3.3.4 [10 Marks] Installing Host Based Protections

Snort is a network IDS, but protections can be enabled on the hosts too. Enable the firewall on Windows XP. Do your exploits still work? Why do they work / not work? Download and install a free or trial of antivirus (Download on Linux Mint and move to Windows XP through a USB stick, NEVER connect the Windows XP VM to the internet). Whatever one you trust, it doesn't matter. Does the antivirus prevent your exploits? What messages do you receive when an exploit is launched?

3.3.5 [10 Marks] Discuss the Pros and Cons of Snort

Discuss the pros and cons, strengths and weaknesses of snort, and what attacks it can detect. Can it prevent / stop attacks in progress? Are rules the best way to define content to remove? How easy is configuration? How easy is it to write rules for complicated attacks like the exploits from section 3.2.5? Etc.

3.3.6 [5 Marks] Discuss Other Countermeasures and Mitigations

What other mitigations can be applied to the Windows XP VM to enhance their security? Talk about things like firewalls, updates, additional software, etc.

4 Deliverables

Each group has to submit a **single PDF** (a PDF file with all fonts embedded, other formats will not be accepted) which includes the following items:

- The names and student-ID's of both group members. If you have received approval to work individually, then please state this and also give the date on which you have received this approval.
- You need to give an agreed-upon percentage of contribution from each partner, reflecting how much work each partner has spent on the assignment. The relative weights will influence the marking.
- Detailed responses to the above tasks. You should use screenshots to show how you achieved what as asked of you. One line responses will not be accepted. Please describe what you did, what you saw and how the action is happening.

The PDF file has to be submitted to the assignment dropbox on learn. You have to submit your report no later than **5pm, 11th October 2017**. Note that no late assignments will be accepted without prior approval.