

IDS and Penetration Testing Lab

ISA656

(Defender)

Ethics Statement

Network Security Student Certification and Agreement

I, _____, hereby certify that I read the following:

University Policy Number 1301: Responsible Use of Computing

<http://www.gmu.edu/facstaff/policy/newpolicy/1301gen.html>

I understand that GMU takes its ethical obligations very seriously and violations will not be tolerated. I fully understand that GMU and its students must conduct the Program's activities in accordance with the highest possible ethical and legal standards. I know that I am responsible for ensuring that my personal conduct is above reproach. As a condition of studying in the ISA Program at GMU, I agree that violations of the standards described in the Code of Conduct shall be made known immediately to my appropriate faculty member(s) and that violations will result in dismissal from the Program and failure to receive the degree. I understand that this is a zero tolerance policy and that no second chances are given.

I agree to take all reasonable precautions to assure that sensitive University or faculty information, or information that has been entrusted to my fellow students or me by third parties (such as the students' employers), will not be disclosed to unauthorized persons. I understand that I am not authorized to use sensitive information for my own purposes, nor am I at liberty to provide this information to third parties without the express written consent of the faculty or the person who is the designated information owner or custodian.

I also understand specifically that GMU provides computer systems and networks for my use in academic studies and that I am not permitted to use those computer systems and networks for personal business or for any activities not related to my academic studies. I understand that GMU audits and monitors the use of those computer systems and networks and that I have no right to privacy or expectation of privacy when I use computer systems and networks provided to me by GMU.

Signature

Printed Name

Purpose:

This lab will expose you to various techniques and tools including protocol analyzers, network scanners, Intrusion Detection Systems, and Penetration tools. Attackers, whether hackers or penetration testers (or ethical hackers), follow certain techniques and steps when trying to hack into their target systems. We will explore these techniques and perform hands on exercises to illustrate these techniques and give you a better understanding of attacking as well as defending methodologies.

Techniques:

When trying to attack their target systems, attackers usually go through the first phase of reconnaissance. In this phase, attackers try to map out the network they are trying to attack and understand the architecture of the network. The next step usually involves scanning targets for vulnerabilities. These scans could be noisy and could trigger alerts on a target network especially when it has monitoring devices like an Intrusion Detection System. Another type of scanning is passive scanning, a silent scan based on traffic it detects and sees from the network, without having to send any packets to the target. Once some vulnerability is discovered, attackers usually use existing exploits or if more advanced, write exploit codes for certain vulnerabilities. The next step would be to launch an attack to exploit the vulnerability and try to gain access. Finally, attackers would do some cleaning of their traces and try to maintaining access to the system by installing root kits and backdoors.

Software Requirements:

1. VMware workstation.
2. Network Security Toolkit appliance (NST v.1.5.0). (Includes Snort IDS, Wireshark protocol analyzer, Nmap scanner, Nessus scanner, and other useful security tools)
3. Backtrack3 Beta, penetration testing appliance.

Lab Exercise:

1. Download the Network Security Toolkit (NST) appliance from the following link:

http://sourceforge.net/project/downloading.php?groupname=nst&filename=nst-vm-1.5.0.zip&use_mirror=internap

2. Locate your NST appliance. (nst-vm-windows-1.5.0.vmx file under "nst-vm-1.5.0" folder)
3. Before starting the virtual machine, verify that the network connection type for Ethernet devices is "bridged". Also you can increase the memory device to around 500 MB.
4. Start the image and login using:

Username: root

Password: nst2003

5. You can close the browser and Start a terminal. Identify the IP address of your guest machine (Right click on the desktop and under "desktop applications" choose "Aterm Terminal" to get a terminal).
6. Identify your host and guest IP addresses for you and get the same information for your partner. Fill out the following table:

IP information	host (windows)	guest (Linux)
You:		
Your partner:		

7. On your host machine, start up Wireshark. Before you start sniffing traffic, ask your partner to go ahead and launch attack1.
8. Once attack1 is performed, stop Wireshark sniffer and examine the packets. We need to perform some packet analysis. The goal is to identify what type of attack was launched. Remember IP headers have assigned protocol numbers: <http://www.iana.org/assignments/protocol-numbers>.

Also remember your TCP flags. Here is a refresher:

FIN = 1
SYN = 2
RST = 4
PSH = 8
ACK = 16
URG = 32
ECE = 64
CWR = 128

Here is an example to clarify. Let us say I want to write a filter to check if attack1 is a SYN/FIN scan. The way to identify such a pattern is by writing a filter on Wireshark that looks like this:

ip.proto == 6 and tcp.flags == 3.

We chose IP protocol 6 because it's TCP, and TCP flags is set to 3 because SYN and FIN flags are set on these packets.

Here is another example. A way for identifying a half open SYN scan is by comparing the number of SYN packets to the number of SYN/ACK packets.

Write the following 2 filters:

Filter for identifying SYN packets:

_____.

(answer) ip.proto == 6 and tcp.flags == 2.

Filter for identifying SYN/ACK packets:

_____.

(answer) ip.proto == 6 and tcp.flags == 18.

9. What type of attack do you think was performed? (You might need to test for more patterns including: SYN/FIN scan, FIN scan, NULL (no flags set) scan: _____.

(Answer) Null scan.

10. Now we need to use snort IDS. In order to start the snort daemon, we need to issue the following command in a terminal (guest OS).

```
/usr/local/snort/snort -c /etc/snort_eth0/snort.conf -D
```

-c is used to locate configuration files, and -D is to run snort in the background (i.e. daemon mode).

11. Verify that snort process is running by issuing the following command:

```
ps -eaf | grep snort
```

12. Now you need to run mysql which will save generated alerts. To run mysql, use the following command:

```
/bin/sh /usr/bin/mysqld_safe --defaults-file=/etc/my.cnf --pid-file=/var/run/mysqld/mysqld.pid --log-error=/var/log/mysqld.log
```

13. Verify that mysql is running by issuing the following command (on a different terminal):

```
ps -eaf | grep mysql.
```

14. You should see something like the following Pids:

```
/bin/sh /usr/bin/mysqld_safe --defaults-file=/etc/my.cnf --pid-file=/var/run/mysqld/mysqld.pid --log-error=/var/log/mysqld.log  
  
/usr/libexec/mysqld --defaults-file=/etc/my.cnf --basedir=/usr --datadir=/var/nst/var/lib/mysql --user=mysql --pid-file=/var/run/mysqld/mysqld.pid --skip-external-locking --port=3306 --socket=/var/nst/var/lib/mysql/mysql.sock
```

15. To view alerts you can first check the number of alerts generated by issuing the following command:

```
/usr/bin/mysql -u snort -p${NSTCTSNORTPASSWD} snort
```

```
Password: ahjbiebiewo7n
```

16. You should be at a mysql> prompt. Now type the following Sql command to get the count from the database:

```
Select COUNT(sid) from event; -u snort
```

You should not see a 0 for your result. Otherwise this means that there were no alerts generated. Usually a real life network would generate some alerts that are a result of some false positives. At this point in time ask your partner to go ahead and launch attack2. After attack2 was performed, check for the number of alerts again. You should see more than 0. If not, verify that you have run snort and mysql correctly by checking previous steps.

17. Once you see alerts, we will now try to view these alerts. One way to do so is to use the Basic Analysis and Security Engine (BASE). BASE is basically a front end to snort that allows analysts to view alerts. It is already installed for you. If snort and mysql are running correctly, you should

be able to access the BASE interface by typing the following link in your Firefox browser:

http://127.0.0.1/base/base_main.php

(Note an underscore '_' between the words base and main (base_main.php))

18. Next to "today's alerts" click on listing. This should display some alerts with their snort signatures (which identifies the type of alerts), the timestamp, source IP, destination IP address, and other information. (You might see some SMB related alerts that are not part of the attack, this is an example of normal traffic that triggered some false positives).

19. Now we are ready for the second part of this lab. This time you will be an attacker. You will have the freedom of trying to attack your partner's host computer. Your partner will also be doing the same. If you truly manage to hack your partner's computer, you will get extra credit on this lab. After finishing this part, you will realize how harder it is to attack than it is to defend. The lab will provide you a famous penetration testing VMware appliance that already has many hacking tools. It's called Backtrack, and we will be using the latest beta version 3. Please go ahead and shutdown your current VMware machine. Follow the following steps to get your attacking system ready.
 - a. Download the Backtrack 3 ISO file, called "bt3b141207" to your Windows XP Host machine from the "IDS_LAB" folder.
 - b. In VMware click on the **File** menu and select **New Virtual Machine...**
 - c. Click the **Next** button
 - d. Select the **Custom** radio button, click the **Next** button
 - e. Select the **Linux** radio button, select **Other Linux** in the Version drop-down box, and click the **Next** button
 - f. Type **Backtrack** in the Virtual Machine textbox and click the **Next** button
 - g. Click the **Next** button again.
 - h. Accept the default for the Network Type and click the **Next** button.
 - i. Accept the default for the I/O adapter type and click the **Next** button.
 - j. Accept the default for the Disk and click the **Next** button.

- k. Accept the default for the Disk Type and click the **Next** button.
 - l. Accept the default for the Disk Capacity and click the **Next** button.
 - m. Type **Backtrack.vmdk** in the Disk File textbox and click the **Finish** button.
 - n. Edit the virtual machine settings for the Backtrack virtual machine.
 - o. Highlight the Hard Disk device and click the **Remove** button.
 - p. Highlight the CD-ROM device and select the **Use ISO image:** radio button.
 - q. Click on the browse button and point it to the "bt3b141207" file that you downloaded to your Windows XP Host machine.
 - r. Click on the **OK** button.
 - s. Click the **Start this virtual machine**. Your Backtrack should be up and running.
20. Now you are free to play around with this appliance and use the tools to attack your partner. Keep the following points in mind:
- a. Do NOT attempt to attack other than your partner's host computer.
 - b. Do not unplug your network cable to avoid attack from your partner!
 - c. Try to go to the start menu and under the Backtrack menu, you should see a list of tools categorized by the phases of attacks we talked about earlier.
 - d. As a hint, try to first scan your partner's computer and try to identify the type of ports that are open. Then try to find vulnerabilities associated to these open ports. For example if they have a web server with port 80 open, try to identify the version of that web server and look for vulnerabilities. The next step would be to try to launch attacks. Backtrack3 has an exploiting framework called Metasploit. It has a good list of exploits that could be used against your partner's computer. Try to learn how to launch them. The web interface is easier to use (try Framework3-Msfweb. After running that daemon, open up your browser and type:

<http://127.0.0.1:55555>

References :

1. <http://www.snort.org>
2. <http://base.secureideas.net/>
3. <http://www.nessus.org/plugins/index.php>
4. <http://www.vmware.com/appliances/directory/141>
5. <http://www.wireshark.org/>
6. Snort 2.1 Intrusion Detection by Baker, Beale, Caswell, and Poore.
7. <http://www.ethicalhacker.net/>
8. http://backtrack.offensive-security.com/index.php/Main_Page
9. www.remote-exploit.org/backtrack.html