

# HOMWORK 5 KEY

## ENTS 689i Network Immunity Fall 2008

**QUESTION 1: (20 pts) Use the data found in the three sections of the Wireshark window to answer the following questions.**

- 1. What is the date and time of when the first packet was collected?**

Arrival Time: Nov 21, 2008 11:31:27.398458000

- 2. What is the IP address of the host that initiated the connection (client)?**

192.168.1.102

- 3. What is the IP address of the server?**

64.233.169.103

- 4. Are any of the packets fragmented? If so, give the packet numbers (1<sup>st</sup> column of traffic summary section)?**

No

- 5. What layer-4 (assuming OSI layers) protocol is being used to send the data?**

TCP

- 6. The client is attempting to access a service on what port?**

80

- 7. What is the packet number of the final ACK packet in the three-way-handshake?**

3

- 8. What are the sequence and acknowledgement numbers associated with packet #7?**

Sequence number: 1431

Acknowledgement number: 505

- 9. What application layer protocol can be found in the trace?**

HTTP

- 10. Which IP address terminates the connection?**

192.168.1.102

**QUESTION 2: (10 pts) Based on the packet capture what is the user (client) attempting to accomplish and from the generated traffic what can you discern about the client (ie application, OS, etc )?**

The user is attempting to connect to the main page (domain root index file) at [www.google.com](http://www.google.com). Assuming the information in the User-Agent request-header field can be trusted and has not been spoofed, it would suggest that the client is using Microsoft Internet Explorer 6 with enhanced security features. It can also be determined that the client operating system is Windows XP SP2 (Windows NT 5.1).

**QUESTION 3: (5 pts) By looking at the output that is returned, what ports are currently open on your virtual machine?**

```
22/tcp open  ssh
25/tcp open  smtp
111/tcp open rpcbnd
631/tcp open  ipp
```

**QUESTION 4: (5 pts) By looking at the output, what new port has been opened by the lab\_server program and what service does nmap claim is listening on that port?**

```
4321/tcp open rwhois
```

**QUESTION 5: (5 pts) If you run the same scan again while including the OS fingerprinting command line option, what operating system does nmap identify as running on your virtual machine?**

```
Running: Linux 2.6.X
OS details: Linux 2.6.15 – 2.6.25
```

**QUESTION 6: (15 pts) What IP addresses within the honeyd network are currently being used? What ports are open on each honeypot?**

```
IP address: 10.0.0.25
```

```
Ports:
```

```
23/tcp open  telnet
```

```
IP address: 10.0.0.144
```

```
Ports:
```

```
23/tcp open  telnet
```

```
80/tcp open  http
```

```
IP address: 10.0.0.234
```

Ports:

23/tcp open telnet

80/tcp open http

**QUESTION 7: (5 pts) What is the alert message found in the alert file?**

```
[**] [1:1:0] magritte08 Detected [**]
```

**QUESTION 8: (10 pts) What modifications would need to be made to the rule in snortlabbroke.conf in order for it to only generate an alert on the fourth packet in the file?**

```
alert tcp any any -> 64.233.169.103 80 (content:"GET / HTTP/1.1"; msg:"Packet 4 detected"; sid:1;)
```

**QUESTION 9: (25 pts) What rule did you generate to detect the exploit? What is the packet number, within the trace, that your rule is attempting to detect? What is the significance of the packet content that your rule is looking for? Why is that a good indicator for this particular exploit?**

```
alert tcp any any -> 172.16.3.128 445 (msg:"Detect Canonicalization Vulnerability "; content:"\00 2E 00 2E 00 5C 00 2E 00 2E 00 5C"; sid:1;)
```

The Snort rule is designed to detect the exploit attempt in packet number 25. This rule is looking for packets with payload content “.\\.\\”. The vulnerability being exploited is a stack-based buffer overflow in the path canonicalization of certain RPC requests that contain dot-dot-slash path names. By having the rule detect characteristics of the path content, detection is not limited to a particular operating system version or exploit implementation. On the other hand, rules based on the return address or the DisableDep address, which were given as hints, are only effective at detecting the specific Metasploit attack that targets vulnerable systems running Windows XP SP3.