Network Security – Practical 1 Feedback

Dr. Sandra Scott-Hayward

CSC3064 Week 4 – Practical 1 Feedback

School of Electronics, Electrical Engineering and Computer Science

CSC3064 – Practical 1 Review

Finding the IP address of a website and identifying route to the destination.

Lab1 Q1: Run the tracert command for IP address 8.8.8.8

From the results displayed, who owns this IP address and what service is predominantly hosted there?

A1: Google, DNS

Lab1 Q2: How does traceroute/tracert work?

A2: Trace Route works by setting the TTL for a packet to 1, sending it towards the requested destination host, and listening for the reply. When the initiating machine receives a "time exceeded" response, it examines the packet to determine where the packet came from - this identifies the machine one hop away. Then the tracing machine generates a new packet with TTL 2, and uses the response to determine the machine 2 hops away, and so on.

CSC3064 – Practical 1 Review

Exploring and auditing a network using nmap

Lab1 Q3: How many live hosts are detected when you run the Step 1 command?

nmap –sn –v 192.168.0.0/16

A3: 2

Lab1 Q4: How many addresses are scanned with the IP address range 192.168.32.0/24?

A4: 256

(Note: actually 254 possible hosts in this range; 0 is the network ID and 255 is the broadcast address)

CSC3064 – Practical 1 Review

Exploring and auditing a network using nmap

Lab1 Q5: What warning is displayed when you run the Step 2 command?

```
nmap –sn –v <VM2 ip address>
```

A5: mass_dns: warning: Unable to determine any DNS server. Reverse DNS is disabled.

Lab1 Q6: Why do you think the warning is displayed in the Step 2 command?

A6: No internet access, VM environment etc.

CSC3064 – Practical 1 Review

Packet crafting using HPING3 and observation using tcpdump

Lab1 Q7: What service/protocol was used in the Step 2 command?

```
sudo hping3 –A –c 5 <VM2 ip address> -p 80
```

A7: HTTP (TCP/IP)

Lab1 Q8: What service/protocol runs on port 53?

A8: DNS (UDP/TCP)

QUEEN'S UNIVERSITY BELFAST

CSC3064 – Practical 1 Review

Packet Analysis with Wireshark

Lab1 Q9: Which flags are set in a DNS standard query?

A9: recursion desired (distinction between standard query and response)

Lab1 Q10: What percentage of packets in Practical1.pcapng are between 40 and 79 bytes in length?

A10: 53.99/54

QUEEN'S UNIVERSITY BELFAST