Tutorial 1

Computer Security
School of Informatics
University of Edinburgh

In this first tutorial for the Computer Security course covering topics from the first two weeks of the class. The tutorial consists of the networking questions from the exam last year and from the re-sit exam.

The tutorial contains several topics you may not yet have seen in lecture. Questions involving these topics are marked with the name of the lecture where you will learn about the topic.

You are free to discuss these questions and their solutions with fellow students also taking the course, and also to discuss in the course forum. Bear in mind that if other people simply tell you the answers directly, you may not learn as much as you would by solving the problems for yourself; also, it may be harder for you assess your progress with the course material.

1 2015/16 Final Exam Question

An online marketing company ZoomMarket recently learned that an attacker named Eve hacked into their systems and stole their valuable customer data. ZoomMarket hired a security forensic analyst to determine how Eve accomplished the attack. ZoomMarket would like to implement some of the analyst's recommendations, but they are suspicious that the advice might not work for them. They have hired you to provide additional advice on how to prevent future attacks like Eve's.

Below are three attacks Eve used on ZoomMarket and the recommendations of the security analyst. Answer the questions for each attack. Marks will be awarded to succinct answers that address the points being asked, providing relevant specific details.

Attack: Eve sent phishing emails to ZoomMarket employees asking them to log into a fake website she controlled. One employee fell for the attack and logged into the fake site using his ZoomMarket username and password. ZoomMarket uses one-factor password authentication, so Eve was able to use the compromised credentials to log in as a legitimate employee.

Analyst Recommends: Use two-factor authentication for all logins.

1. Would two-factor authentication have protected ZoomMarket against the above attack? Why or why not? (Authentication Lecture)

2. Suggest a way two-factor authentication could be practically implemented on ZoomMarket's website without buying special equipment for each employee. Be specific, include the factors you would use. (Authentication Lecture)

3. Describe an alternative non-technical approach ZoomMarket could use to help their employees avoid falling for Phishing attacks. Give an example of how this approach might work.

4. ZoomMarket's board is concerned about spearphishing attacks containing malicious attachments. They want you to install a firewall that will protect employee email by removing all .zip and .doc attachments. Where would you recommend such a firewall be installed (router, email server, or the client computer), and why would you recommend that it be located there?

5. Would the firewall the CEO is asking for in (d) have prevented Eve's phishing attack? Why or why not?

Attack: Eve discovered that ZoomMarket had an internal website visible only to employees. She used the well known Shell Shock vulnerability to trick the web server into running shell commands using the authority of the web server user. Shell Shock is a well known vulnerability with patches avalible for the majority of software. She uses the attack to disable the database logging process.

Analyst Recommends: Update the server in accordance with Cyber Essentials requirements.

6. Would updating all the software on the server have protected ZoomMarket against the above attack? Why or why not?

7. The programmer who wrote the code on the web server no longer works for ZoomMarket and updating the server is impossible. Name two other requirements of Cyber Essentials and describe how you might use each to protect ZoomMarket's vulnerable web server.

8. There are five common security properties. What security property was violated by disabling logging? (Only answer in regards to the logging, not what might happen after.)

Attack: Eve uses a SYN flood attack sent from a single computer she controls to create a large amount of traffic that takes down ZoomMarket's main external web server.

Analyst Recommends: Install an Intrusion Detection System (IDS) and monitor it regularly for attacks.

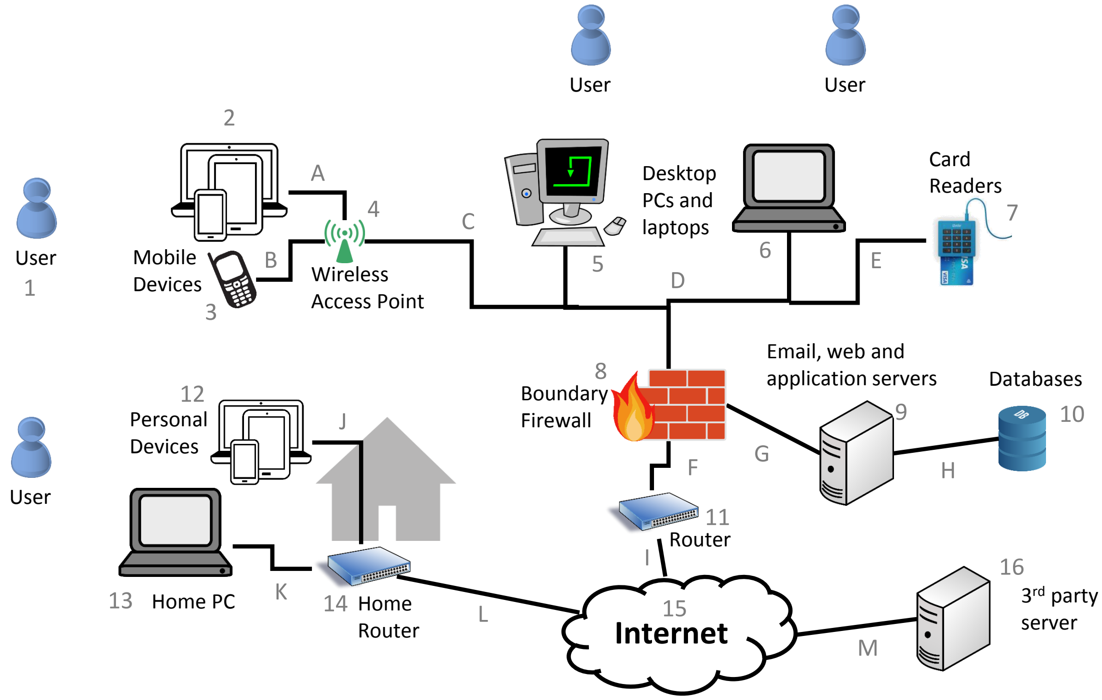
9. Would an Intrusion Detection System have prevented the above attack on ZoomMarket's external web server? Why or why not?

10. What is the general terminology for the type of attack Eve is using against the external website?

11. Describe one problem with SYN Flooding that makes it less than ideal for attackers and provide an alternative attack Eve could have used that would not have the problem.

2 2015/16 Final Exam Resit Question

The CEO of AcmeCo has been reading about how other companies have been compromised and is now nervous that his company may not be as secure as he would like. He has hired you as a security consultant to review AcmeCo's network setup. The following diagram shows the current network. Nodes have been labeled with numbers and edges on the graphic have been labeled with letters, please use these in your answers to refer to specific sections of the network.



1. List three nodes (numbers) on the network that are beyond the control of AcmeCo's network administrator.

2. The CEO is worried about ransomware causing damage to the network. Ransomware is a type of malicious software that infects computers typically through email attachments. It waits a bit and then encrypts all of the files that a computer account has access to, including network resources like databases. The malicious actors then ask for money to decrypt the files. If you installed a malware scanner on the boundary firewall (8) would it protect nodes 5-10 from ransomware? Explain. (You can assume that the malware scanner is 100% accurate.)

3. Cyber Essentials has 5 requirements. Name one requirement other than Malware Protection that if properly followed would limit the damage caused by ransomware. Give an example.

4. The CEO tells you that they have budget to add one more firewall to the network. On what edge (letter) would you add the firewall? Explain why you would place it there.

5. At what OSI network level should this new firewall operate? Explain.

6. When examining the network you find that the wireless access point (4) does not authenticate devices and you cannot tell what employee mobile devices 2 and 3 belong to. How might this impact the security property of Availability?

7. The CEO would like you to add authentication to the wireless access point (4) so that only employees can connect to the WIFI. When you look on the access point you see that it is currently being used by all types of devices including: mobile phones, laptops, printers, and a Smart TV. Describe an authentication system that would work for all these devices and ensure the property of Accountability on the network. (Authentication Lecture)

8. You inspect the boundary firewall and discover that the following commands were used to set it up:

```
iptables -A INPUT -p tcp --dport ssh -j ACCEPT
iptables -A INPUT -p tcp --dport 25 -j ACCEPT
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
iptables -A INPUT -j ACCEPT
```

   One of these commands is a very bad idea to run on a boundary firewall. Which line and why?

   Note: this question assumes that you have completed the VM coursework which involves IPtables. You may not be able to answer the question till you complete this coursework.