Tutorial 1: Solutions

Computer Security
School of Informatics
University of Edinburgh

December 10, 2016

1 2015/16 Final Exam

1. Yes - The user would have only lost one factor (the password) during the phishing attack. The second factor (such as an RSA key fob) would not have been compromised.
2. A cell phone could be used as the second factor by sending an SMS or having an app compute a number which changes.
3. User training, a game that teaches users how to read URLs. Or a fake phishing email that delivers training when a user clicks on it.
4. Email server. The client computer is too late, most personal firewalls can't parse email application data. The router needs to parse packets quickly, so it cannot afford to spend time parsing application content. The email server is already intercepting the packets for storage and has the capability to modify email.
5. No. Eve's attack involved a link to a website. A firewall that strips out attachments would not have helped.
6. Yes it would have. Shell shock is a well known vulnerability which has patches available.
7. Any two of the following:
   - Boundary Firewalls and internet gateways - Place a firewall in front of the server and scan for known incoming attacks
   - Secure configuration - Make sure there are no default open ports or default system passwords being used.
   - User access control - Make sure the web server user has minimal access rights on the system
   - Malware protection - Install an anti-malware product to detect dangerous programs Eve might run.
8. Accountability or Repudiation
9. No. An IDS typically does not prevent attacks, it just detects them. The attack on the external server is a DOS which IDS cannot prevent.
10. Denial of Service or DOS.
    Incorrect answer would be Distributed Denial of Service (DDOS). Because the attack came from a single server it is not Distributed.
11. SYN Flooding can be attributed to the source. Spoofing would fix the issue.

2 2015/16 Final Exam Resit

1. Any three of: 12-16 (best answer), or 2 or 3.

2. Best answer is "no" because of the mobile devices 2 and 3. One of them could become infected elsewhere and bring in the infection. Other optinos are the desktops 5 and 6 which could have an infected USB plugged into them.

3. Any one of the following:

   - Boundary firewalls and internet gateways - Firewalls could be used to segment the network, break it up similar to how nodes 9 and 10 are seperated from the rest of the network. Doing so limits the spread of the ransomeware.
   - Secure configuration - Malicious software commonly uses default passwords to get access to network resources, changing the passwords on these accounts would limit the spread of the ransomware.
   - User access control - Ransomware gets access to whatever the infected user has access to. By limiting access to what each person actually needs (principle of least privilege) you can limit the spread of the ransomware.
   - Patch management - Ransomware, like most malicious software, often uses unpatched vulnerabilities to spread. Patching removes those vulnerabilities and limits the ransomware's abilitiy to do things like get root access.

4. Best answer is C between the Wireless Access Point and the rest of the network. C is the best answer because mobile devices are moving in and out of the network possibly bringing with them infections. Putting a firewall on 4 protects the network from these threats.

5. If the new firewall is going to protect against ransomware then it needs to be able to compare traffic to known signatures, that means that it must reassemble the packets. That means that the firewall must opperate at a minimum of level 4 and more likely at level 6 or 7.

6. If anyone can connect to the wireless access point (4) then they could perform a denial of service on 4 by setting up a large number of connections.

7. To ensure Accountability we need to be able to link each connection to a particular employee. Any answer that strongly links the employee to the device would be acceptable. One option is that employees could be given an online portal where they can input the device's MAC address and be given a unique passcode which that device can use to log into the network. The passcode is necessary because the MAC can be spoofed by other devices. Passcodes also tend to work as nearly all internet connecting devices are already setup to work with them.

8. `iptables -A INPUT -j ACCEPT` is a very bad line to run on a boundary firewall. It tells the firewall to accept all connections by default. Because the lines above are all ACCEPT they are subsumed by this one line and the firewall will allow all connections through.