**CS 425 - Group Proposal**

**Team 5:**

Austin Cari

Benjamin Eavenson

Tyler Higgins

Julian Keller

**Backdoor Man In the Middle Attack Proposal**

We are proposing a backdoor man in the middle attack. The basic idea is that we will intercept network traffic and then use it to set up a backdoor on the target machine. Initially we will use a linux virtual machine as our target. Intercepting traffic will be done by setting up a wifi access point on our machine. Once we have intercepted traffic we will redirect the user and trick them into downloading our backdoor code or enabling a backdoor with a command. Alternatively we will look into methods of injecting our code into the intercepted traffic without the target's knowledge. Finally we will explore various ways that we can protect ourselves from backdoor and networked man in the middle attacks.

**Links:**

* Intercepting Traffic
  + <https://hackernoon.com/a-hacker-intercepted-your-wifi-traffic-stole-your-contacts-passwords-financial-data-heres-how-4fc0df9ff152>
  + <https://null-byte.wonderhowto.com/how-to/hack-wi-fi-creating-evil-twin-wireless-access-point-eavesdrop-data-0147919/>
* Tricking Users
  + <https://www.thatsnonsense.com/how-websites-can-trick-you-into-downloading-malware/>
* Backdoors
  + <https://www.hackingtutorials.org/networking/hacking-netcat-part-2-bind-reverse-shells/>
  + <https://medium.com/@airman604/9-ways-to-backdoor-a-linux-box-f5f83bae5a3c>
  + <https://www.abusix.com/blog/how-hackers-access-networks-using-backdoors>
  + <https://dev.to/tman540/simple-remote-backdoor-with-python-33a0>
* Protecting Against Attacks
  + <https://www.malwarebytes.com/backdoor/#how-can-i-protect-against-backdoors>

**--------- Brainstorming ---------**

**Details/Brainstorming** (Probably to include in the paragraph)**:**

Phase 1 (Julian):

* write some code to create a backdoor on a remote machine
  + What machines can we exploit?
* insert the code into an image or pdf via steganography
* learn how to make the code execute when opened
* Links
  + <https://medium.com/@airman604/9-ways-to-backdoor-a-linux-box-f5f83bae5a3c>
  + <https://www.hackingtutorials.org/networking/hacking-netcat-part-2-bind-reverse-shells/>

Phase 2 (Ben):

* intercept victims network traffic
  + (true evil-twin where we trick the computer, or do we just set up our free public wifi and play off of the fact that people are idiots)
* figure out how to send the image with the malicious payload to the victim without their knowledge
  + Modern updated browsers won’t download files that aren’t confirmed by the user
  + Can we inject code into other kinds of files too?
* (or trick them into downloading it)

<https://hackernoon.com/a-hacker-intercepted-your-wifi-traffic-stole-your-contacts-passwords-financial-data-heres-how-4fc0df9ff152>

<https://www.thatsnonsense.com/how-websites-can-trick-you-into-downloading-malware/>

<https://null-byte.wonderhowto.com/how-to/hack-wi-fi-creating-evil-twin-wireless-access-point-eavesdrop-data-0147919/>

Phase 3 (Tyler):

* Remotely access the machine with the back door
* Figure out the method to remotely enter the machine through the back door.
  + Remote Access Tools(RAT’s)
  + Website/blog to decipher ip addresses
  + ‘Connect-Back’ backdoor (to bypass firewalls)
  + Connection Availability Abuse Technique: Using two malware programs - The first infiltrates the backdoor and evades detection while it downloads the second malware program within the target system (sort of what we are thinking about, except we’re using a downloadable image from what I understand).
* Using python to create a backdoor (see second link):

<https://www.abusix.com/blog/how-hackers-access-networks-using-backdoors>

<https://dev.to/tman540/simple-remote-backdoor-with-python-33a0>

Phase 4 (Austin):

* learn how to protect against this type of attack
  + VPN, Tor Browser, Proxy servers
* <https://www.malwarebytes.com/backdoor/#how-can-i-protect-against-backdoors>
* How DNS servers are attacked <https://www.esecurityplanet.com/network-security/how-to-prevent-dns-attacks.html>
* Create secure passwords
* From Wikipedia: Originally designed as a public, hierarchical, distributed and heavily cached database, DNS protocol has no confidentiality controls. User queries and nameserver responses are being sent unencrypted which enables network packet sniffing, DNS hijacking, DNS cache poisoning and man-in-the-middle attacks. This deficiency is commonly used by cybercriminals and network operators for marketing purposes, user authentication on captive portals and censorship.
  + Source: <http://ipj.dreamhosters.com/wp-content/uploads/2019/07/ipj222.pdf>
* The first step in spoofing is determining the IP address of a host the intended target trusts. After that, the attacker can change the headers of packets to make it seem like the transmissions are originating from the trusted machine.
  + Source: <https://www.csoonline.com/article/2115848/data-protection-ip-spoofing.html>