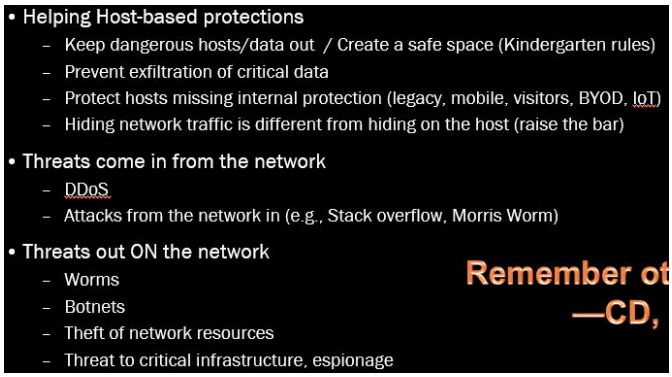
Writeup 6
CS 373
James Tyler Ball

Network Security Lesson 1 (Ram Venugopalan and Geoffrey Cooper):

The pre-reading seems to cover a lot of topics that were covered in the Networking course at OSU. I'll revisit this if I come across something I don't remember.

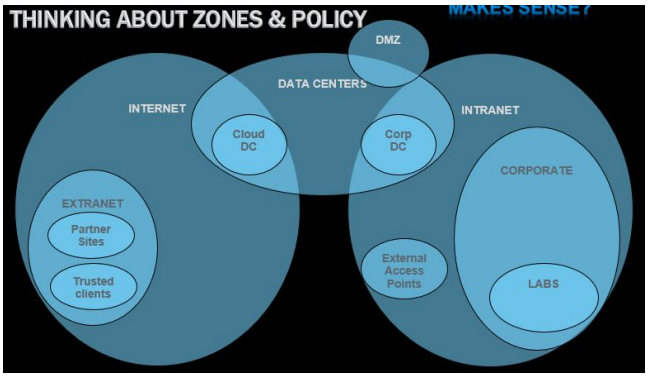
Why do we need network security?

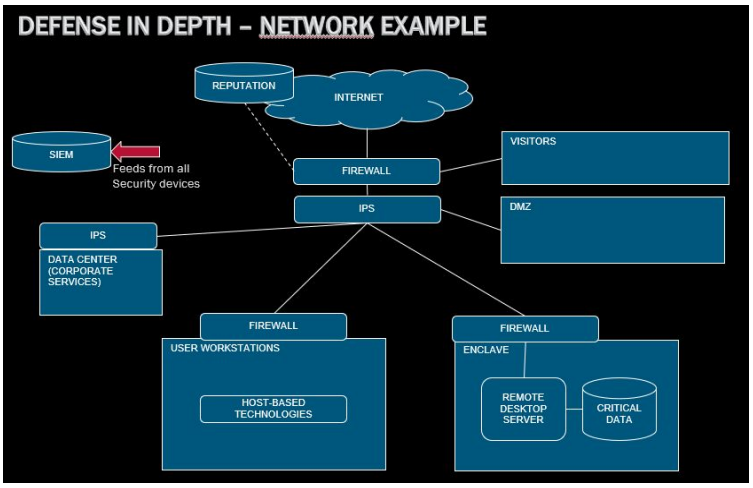
- Create a safe environment
- Keep critical data safe
- Avoid DDoS attacks
- 

In 1980, the Robustness Principle took form: "Be liberal in what you accept, and conservative in what you send." *The lecture has a blip during this section.* Venugopalan states that this principle helped from the standards of how the internet operates today.

My initial reaction on seeing this sentence is to disagree. One consistency across all lectures we have seen so far is that being too welcoming to incoming requests and software can easily lead to the host becoming the victim of attackers. Perhaps in 1980 this idea was safer, but after using script blockers and seeing how much data sites try to cram into my computer I am reluctant to accept any more than is needed to accomplish my goals.

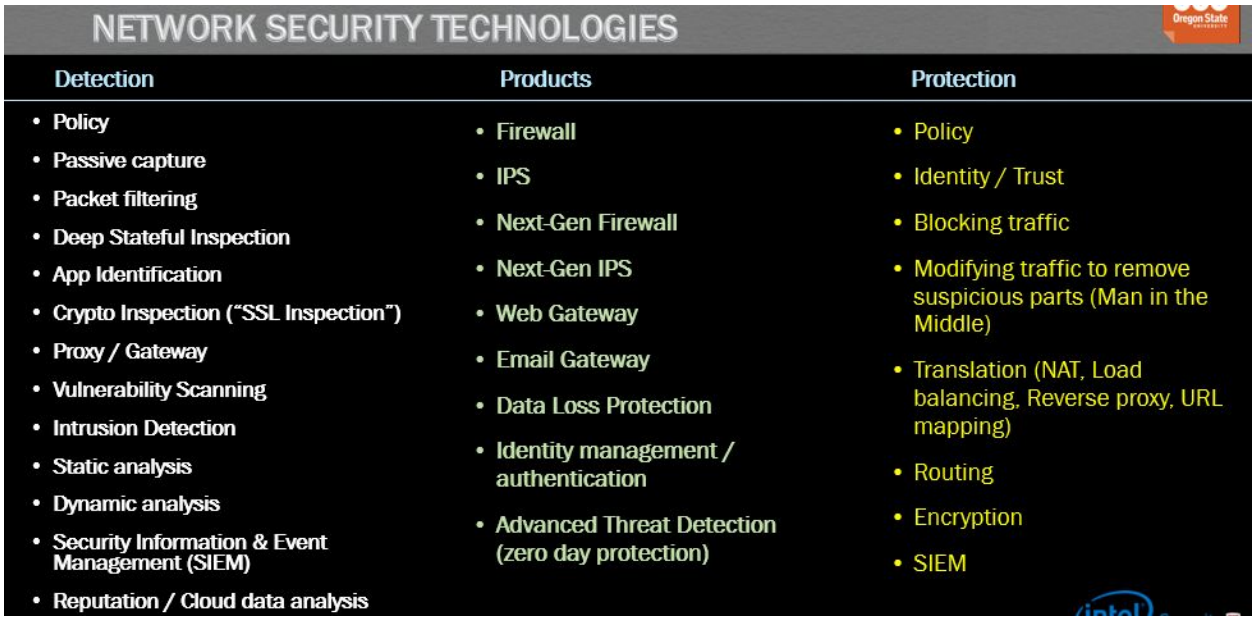
Protection strategies:

- Positive policy
    - white listing
    - only permit what you know is trustworthy
    - attackers have an innate advantage, so this approach allows you to set up your network to your unique layout that an attacker may not expect
    - make the attack surface smaller (fewer possible approaches for attackers)
    - threat management is looking for something that's not supposed to happen
- Firewalls and security zones
    - create zones, firewalls determine what interactions can take place between those zones
    - 

    - a proxy is a connection that splices two zones together
        - a firewall may block a whole webpage
        - web gateway analyzes data and might only block part of it
        - email gateway can filter and sort email
- Defense in Depth
    - This is a simple idea - layer your defenses
    - LOTR example, even if attackers break through one layer of defense, there are more protecting sensitive data
    - Compare this method to defending a medieval castle
    - 

- Intrusion Detection
    - An intrusion protection system will automatically block suspect sources
    - Zero day attacks (no tailored defenses or patches yet) are a weakness here
    - generally good at catching known attacks
- Honey nets
    - a honey pot is “bait” to see how attackers approach
    - the approach here is to create a fake network that looks worthwhile to an attacker
        - now the attacker is wasting their time and resources
    - this is difficult to set up, though
        - takes resources to build and maintain without interfering with your existing network
- Quarantine
    - hosts that are suspect are isolated from the network
        - hosts are either quarantined until processed or quarantined after suspect behavior
    - firewalls can do this to blacklist hosts
    - keep in mind that persistent users can quarantine multiple hosts with repeated attempts at the same process. Hard to account for human behavior
- Reputation
    - Many large companies subscribe to this idea
        - they are also willing to contribute their data to large collections
    - Big Data is where the magnitude of the data changes the value of the data
    - MAC addresses are supposed to be unique
        - mapping MAC addresses can be used to gather info on locations and user trends

Network Security Technologies



- Firewalls contain policies as well as packet filtering.
- DSI involves digging through a packet stream and performing the same operations on it that a host might to see through the protocol stack and analyze the stream
    - policy has to have the things policy defines (zones, data traffic)
- Next-Gen Firewall is still a firewall
    - firewalls are the largest financial segment of network security
    - add app-identification, user policy, crypto-identification
    - fancy and better
- Encryption also comes with rules
    - what if you send data between companies?

Most of the remainder of the lecture will focus on various network threats

Man in the Middle

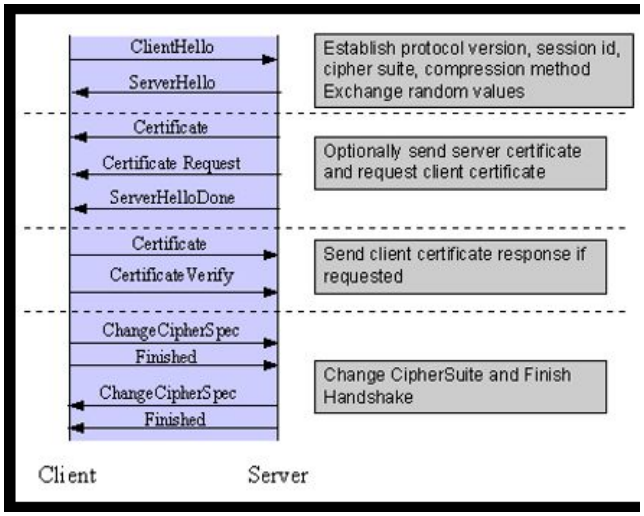
- Can be used for both offense and defense
- MitM is inspecting and potentially reading, changing, or blocking packets as they travel from their source to their target
    - obviously there is almost a limitless number of damages that can occur if the MitM is not detected
- ARP poisoning
    - an ARP associates an IP address with a MAC address
    - whoever responds to an ARP request first gets the traffic
    - network is unsecured at this layer

    - ARP packets are a huge proportion of flowing traffic
- TCP hijacking
    - because TCP is streamed, MitM can inject, read, delete, or change packet data
    - how would they get the packets?
        - wifi
        - ARP poisoning
- Can also be used for good
    - stop connections on one side
    - rewrite headers so attackers can't break firewalls
    - obfuscated URLs
    - stop exe files being sent over email
    - detect traffic flowing to the wrong places
- How is MitM detected?
    - cryptography
        - attach an HMAC to data. Now changing data involves cracking the encryption

```
Crypto Hash Example:
$ echo -n "3SECRET1052" | sha256sum
78e728e9cf18f13e7a6b71366a3143430d975ee180b7f4e79b41074262131399
```

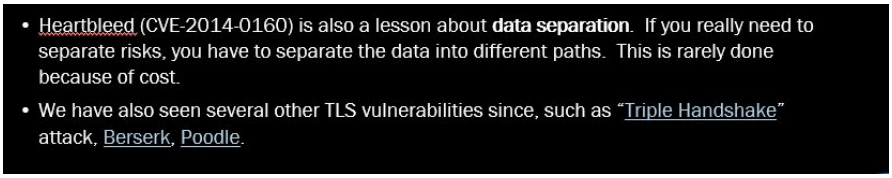
        - chain packets together to prevent to insure the stream's integrity
    - Note that we need keys (shared secrets) for encrypted communication
        - N^2 problem
        - Use Public Key Cryptography - one key locks, another key unlocks

So how do we secure communication?

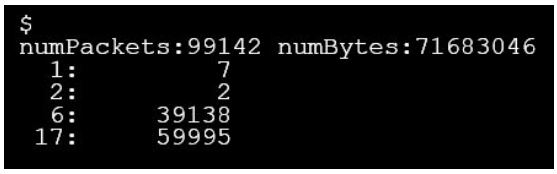


Transport Layer Security or Secure Socket Layer security - a secure connection. What does this mean?

- host connected to has private key of server cert
    - a different host may not
    - certificate changed? maybe the user becomes the host
- DNS name of host resolves to user IP address
    - Spoofing the DNS request by responding to a request or ARP Poisoning could compromise this
    - list of user's trusted sites could be compromised
- connection is encrypted
    - some encryptions are no longer considered secure.
    - When something is secured, it is important to specify how and what parts of a system are secured.
- TLS can also fail even if executed well
    - Heartbleed example
    - Cybersecurity is not passive, defenders must be vigilant



Lab 2 - Students are given high level data (addresses, ports, protocols) and will be asked to dig into it and see what kind of network this data belongs to. Starter scripts are in Python and Perl.



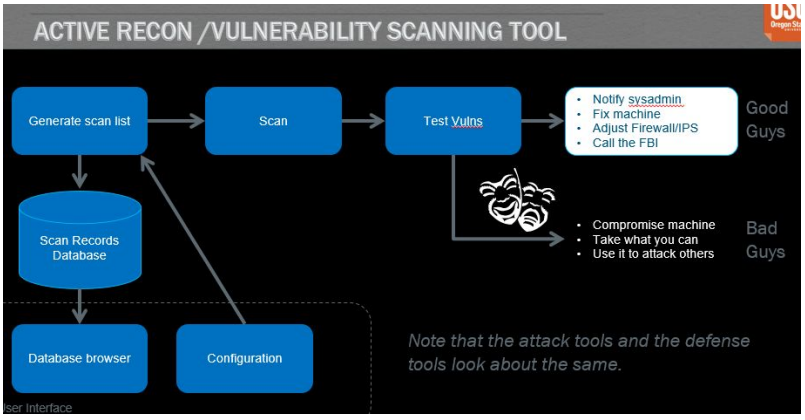
6 is TCP, 17 is UDP

"Perl is a better language than Python because there are less lines"

Network Security Lesson 1 (Ram Venugopalan and Geoffrey Cooper):

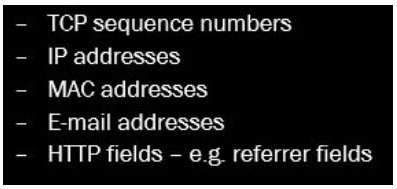
What is recon? How do you do recon? There is active and passive recon.

- Passive is about looking at data on networks, gathering information, looking at logs
    - use equipment like keyloggers
    - scan radio signals
    - watch for usernames and passwords
    - use wireshark to analyze and capture packets
        - connect packets to MAC addresses, IP addresses
        - 

- Active recon is about seeking out vulnerabilities
    - scanning to get ip addresses and ports
    - NMAP
    - hard for network admins to see this
        - look at different ports for surges of traffic
        - attackers can use slow scans
        - look for patterns in logs
    - 

- How to slow down and defend against recon?
    - Honey nets
    - layered defenses
    - firewalls
    - cryptography

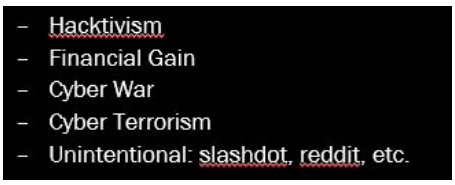
What is Spoofing? Why Spoof?

- Spoofing allows you to get data intended for another source (MitM)
- LAND attack was an early DoS attack - LAN DoS
- can bypass NATs
- Note TCP is random to prevent predictability
- what are the targets of spoofing?
    - 

How do you defend from spoofing?

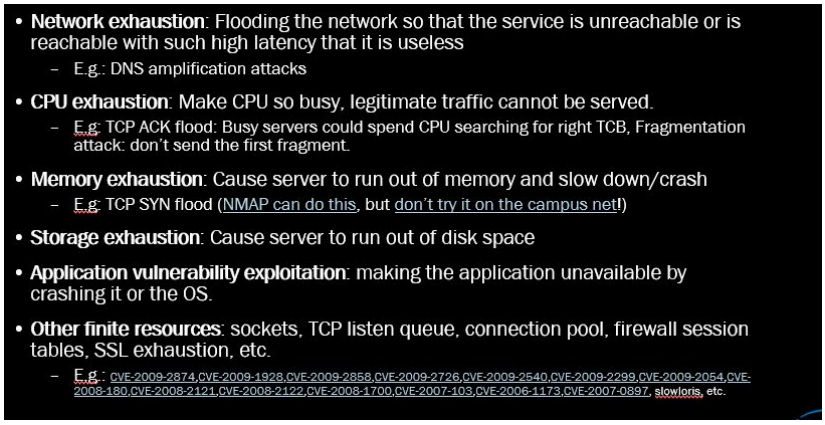
- check sources of data
    - MAC addresses
- egress filtering

DoS (consume resources for an extended period of time) and DDoS (large number of computers performing resource exhaustion attacks, generally harder to defend against) - the idea is to bring down a network or put it temporarily out of service

- send an enormous amount of requests to the network
- generally easy to detect and easy to prevent
- Anonymous used slowloris recently
- Why do this?
    - 

    - hide real intent (another attack)

- different types



- any limited resource on a network can be exploited for a DoS
- TCP listen queue (inaudible definition, I looked at this page for an explanation: https://www.linuxjournal.com/files/linuxjournal.com/linuxjournal/articles/023/2333/2333s2.html)
- How to defend?
    - As a network device, create a session for everything that enters the network
        - look to see what the state is - if it stays in SYN sent mode without receiving, time it out sooner
        - watch for surges of high volume traffic, transfer operations when found (very expensive)

Bugs (unintentional) and Back doors (intentional) - both can be attacked

- default passwords on routers are especially vulnerable
- buffer overflow - one of the first methods

Packet filtering

- Stateful - inspecting packets, more intensive
- stateless - implement policy (UDP, multiclass)
- (*much of this was inaudible)*
- only allow whitelisted traffic

Deep inspection

- take an active approach with suspicious traffic
- MitM methodology sometimes

- Trace protocol headers
- Multiple protocols (modern firewalls recognize the protocols dynamically)
- Signature processing on content (IPS)
- Dictionary processing on content ("Data Loss Protection")

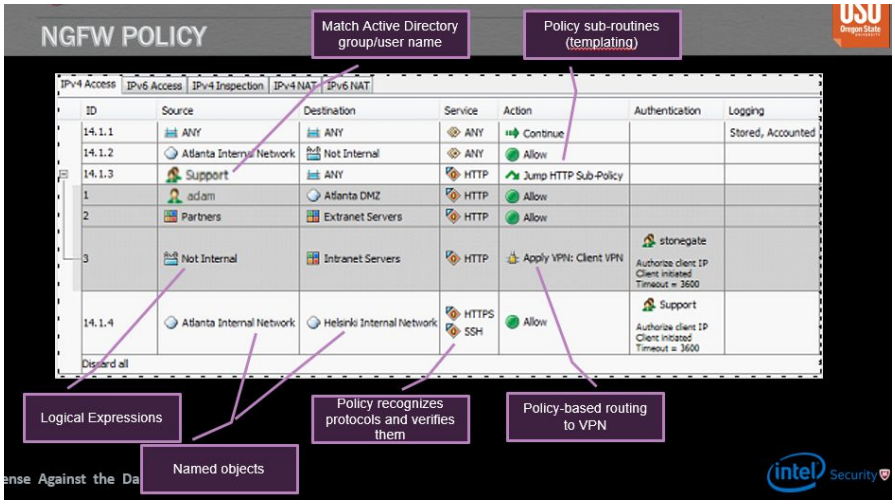
Proxy

- transparent - intercepts your traffic without you being aware of it
    - performance is lower than packet filtering, more work is being done
- H.323 and SIP are voice and video protocols, dynamic ports, proxies are required
- Note one port per active connection is required

NAT: Network Address Translation

- Is NAT a security feature or a networking feature? It can be both. Hides IP address
- STUN protocol can help to bypass NAT
    - connect directly to and endpoint behind NAT
- TURN
    - relay server communicates to parties behind NAT

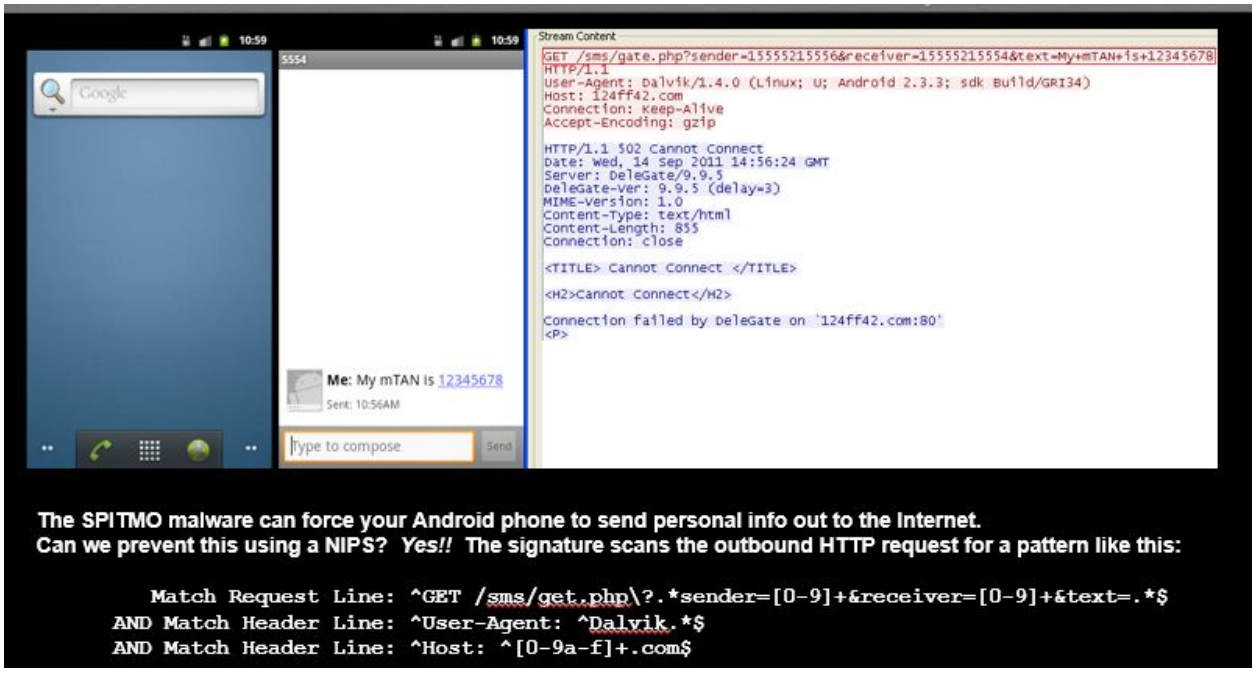
NEXT GEN FIREWALL



VPN/IPSEC

- if two people want to communicate privately, they need to establish a "shared secret"
    - next comes the IPv4 tunnel
- no dynamic ports, so NAT traversal mode is required to continue

Most Intrusion Prevention Systems are signature based IPSs, there are a lot of false anomalies - the bane of any security network administrator. The target breach is an example of “alert fatigue” - too many notifications can lead to security teams ignoring warning flags.



Actual attack on android

One big issue with looking at network traffic is that high volume makes it difficult to identify threats.

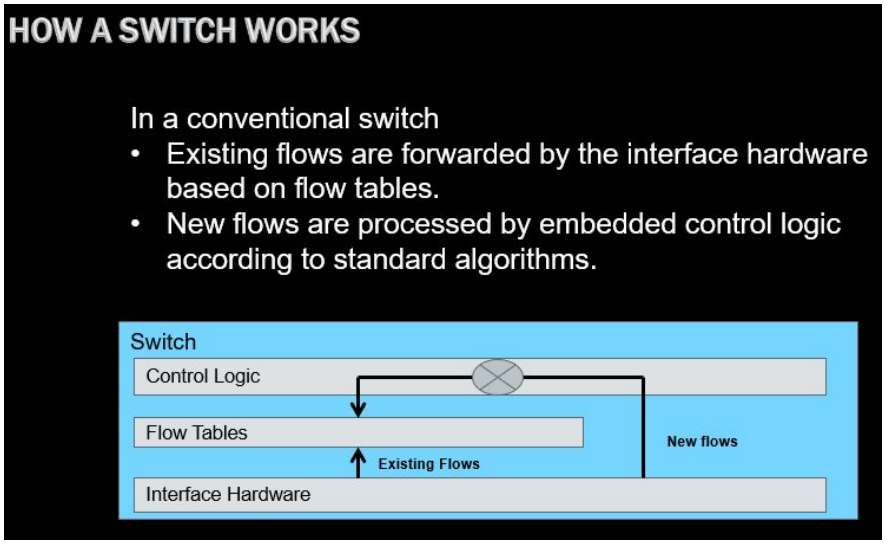
dynamic analysis - running a file in a VM to see what happens
How to do dynamic analysis? On IPS you take a file and look at the source. Check the reputation. Is it clean? If not…

- prevalence - how often has this file been seen in the world and where?
- age - when was this file first seen?
- This is part of why sharing intelligence between endpoints is critical when defending against malware

Evasion

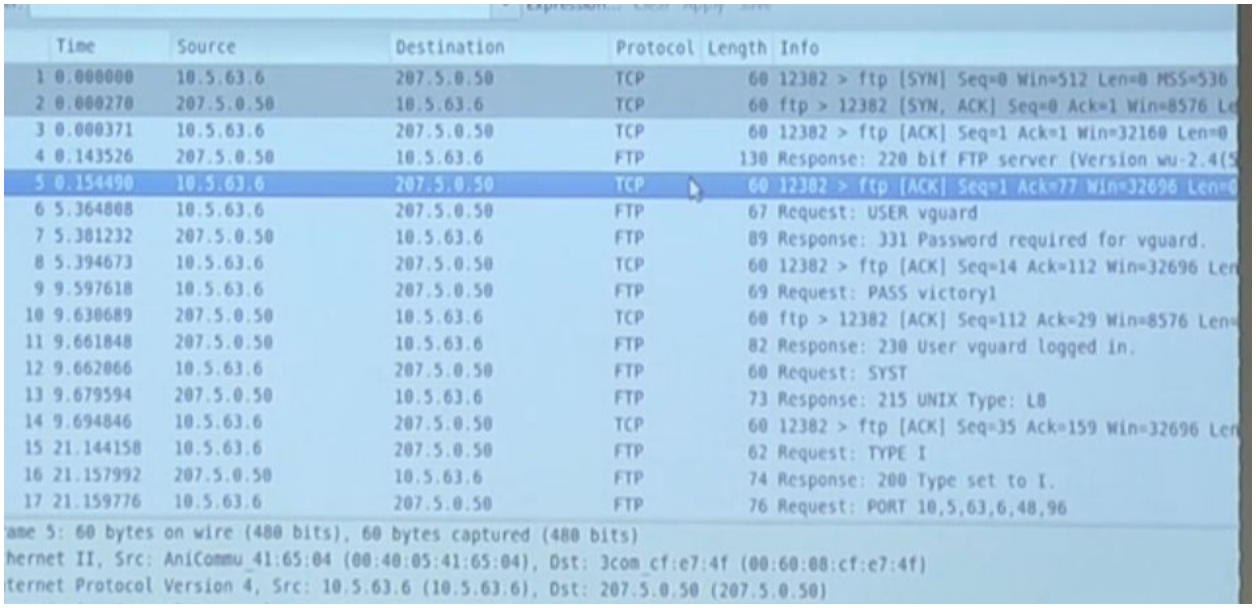
- IPS can fooled via fragmenting packets
    - use TCP segments
- even well known and old evasion techniques can still be effective
- Look up the “Evader” tool (Stonesoft)

Having many virtual machines is cheaper to maintain. This leads to a virtual network which has big advantages. However, in a software defined network, the control logic is separated from data flow.



switch directs data, can make quarantine relatively easy

LAB



TCP conversation

From the above page, we can right-click and follow the events.

Statistics > Conversations - can tell you what conversations occurred, what protocols were used, how many bytes were sent, when the start time was and how long it lasted.

Wireshark can also see file details of files sent over HTTP.

Find Packet operation can be used to search for a string.

The rest of the lecture covers the Lab details, which I will cover in Homework 3