Arthur Liou
CS373

Week 6 Writeup

Prompt: Submitting a write-up of your thoughts, impressions, and any conclusions based on the material from the week. Each week will have its own assignment in the grades page.

For the first part of this week's writeup, I'm reflecting partially on the topic – Network Security, but then more important how the assignments and class were structure this week. As a student, I loved the depth and the breadth of the coverage of the topics we had. For what we covered and learned, see my lecture notes below.

I appreciated the opportunity to learn a lot In the past week. However, as a student, I did not appreciate that we had two assignments, in addition to this write up, due this week, especially as they took a LOT of time, did not have very clear and / or meaningful instructions, failing VM (for the lab). My whole weekend was dedicated to these two assignments, a separate classes's midterm, and this writeup. As an instructor, that might be nice to hear, but when a student spends a 3-day weekend to follow along and complete labs / assignments for a week, then you know there is something wrong with assignment management / due dates.

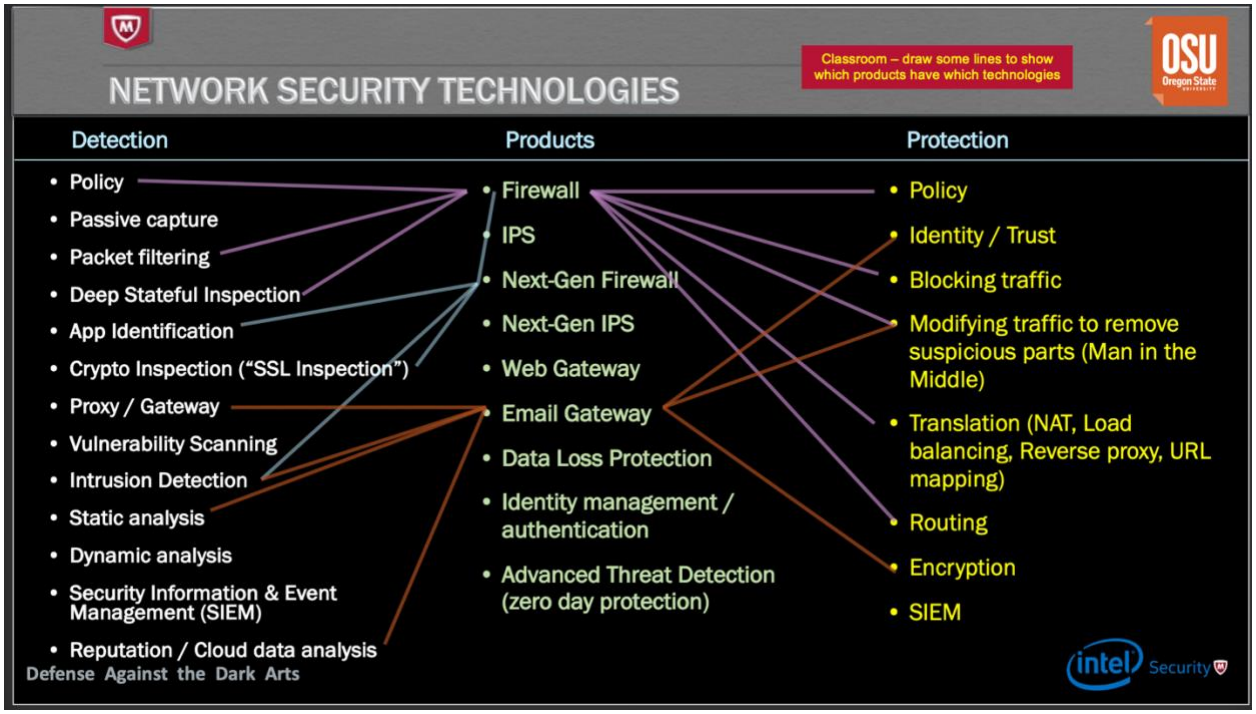
The content for this week was very heavy, and should have been split separately so that one assignment was due one week and one the next, similar to how Week6 Lab 2 is due this week with this week's writeup and next week we have Lab 2 and writeup 7. The HW5 program could have been due the previous week or even next week. As a student who works full-time, this was a very disappointing week, and I hope the staff takes this into account when setting this class up for next semester.

Lecture Notes

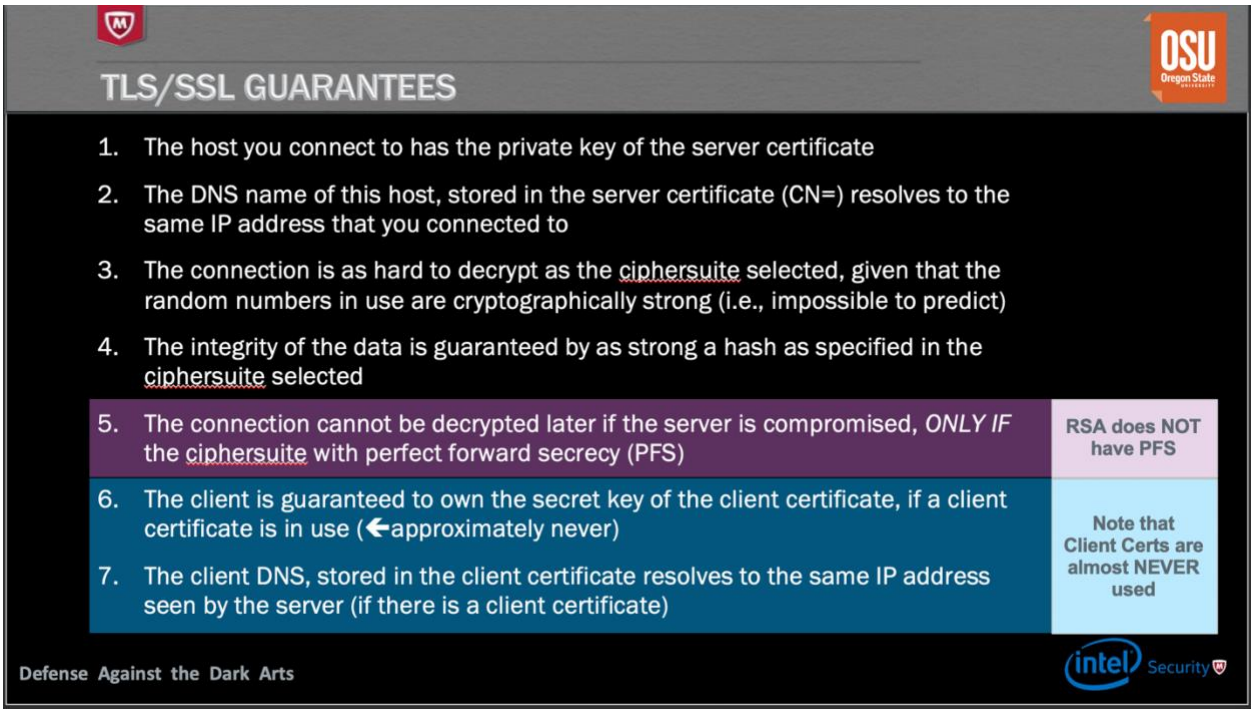
Lesson - Network Security

- Exercise – DADA Network Security
- Exercises – Zone Policy Diagram
- IP/UDP/TCP Wikipedia pages for Pre-readings
- Background info / light reading
- Overview of Network Security
- Why do we need this
    - Helping Host-based protections
        - Keep dangerous hosts/data out / Create a safe space (Kindergarten rules)
        - Prevent exfiltration of critical data
        - Protect hosts missing internal protection (legacy, mobile, visitors, BYOD, IoT)
        - Hiding network traffic is different from hiding on the host (raise the bar)
    - Threats come in from the network
        - DDoS

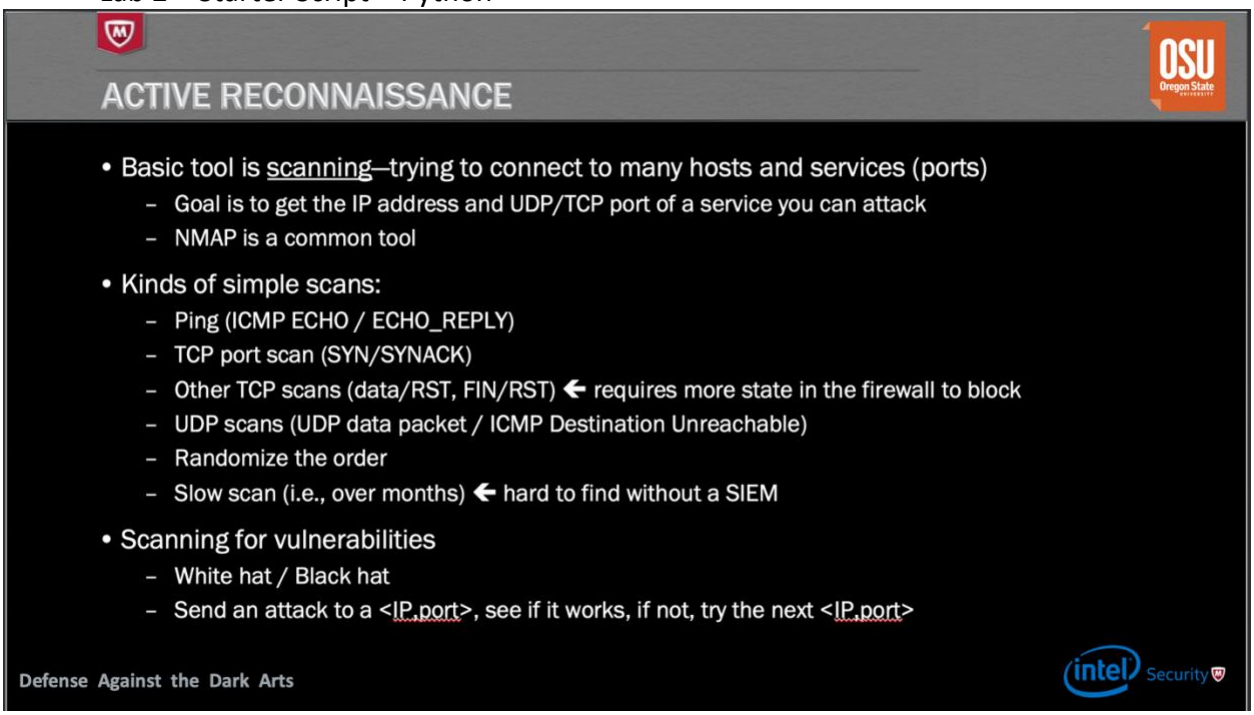
        - Attacks from the network in (e.g., Stack overflow, Morris Worm)
    - Threats out ON the network
        - Worms
        - Botnets
        - Theft of network resources
        - Threat to critical infrastructure, espionage
- Robustness Principle: 1980-1989
- "Be liberal in what you accept, and conservative in what you send.
- Network-based protection strategies: Positive policy, Firewalls / Security Zones, Defense in Depth, Intrusion Detection, Honeynets / Intrusion Deception, Quarantine, Reputation (also host-based)
- Positive Policy ("Whitelisting" in the host). Definitino of what you expect / allow to happen. This is a fundamental concept because: Defender advantage, allows use of internal conventions and choices, attacker has to guess (e.g., which addresses are valid, where are the servers, critical data?), Limits the attack surface (makes other kinds of protection more effective), Provides a hook for other trust mechanisms: identity, trust chaining, Policy domain versus threat domain (finite vs. infinite enumeration), However, Policy may *detect* a threat, but it doesn't *name* the threat!
- Firewalls and Security Zones: Most common implementation of policy is to define zones in the network with policy between zones.
- Firewalls are devices that sit between the zones and filter traffic for policy.
- Firewalls are best at describing policy from IP⇔IP address. More advanced concepts:
    - Application + IP to IP (GMAIL from User Stations to Internet)
    - User + IP to IP (Finance Worker from User Stations to Financial Data Center)
- Other firewall-like devices – web gateway, email gateway
- Intrusion Detection (IDS/IPS) – use signatures/anomaly detection to detect attacks.
- Advantages
    - Catch known attacks quickly and efficiently
    - Good information on attacks
    - Virtual patching
- Disadvantages:
    - Zero day attacks (arms race phenomenon)
    - False positives
- Honeynets – attackers don't know the structure of the network under attack, so use a phony network, unassigned internal addresses, use sucker algos,
- Network Security Technologies

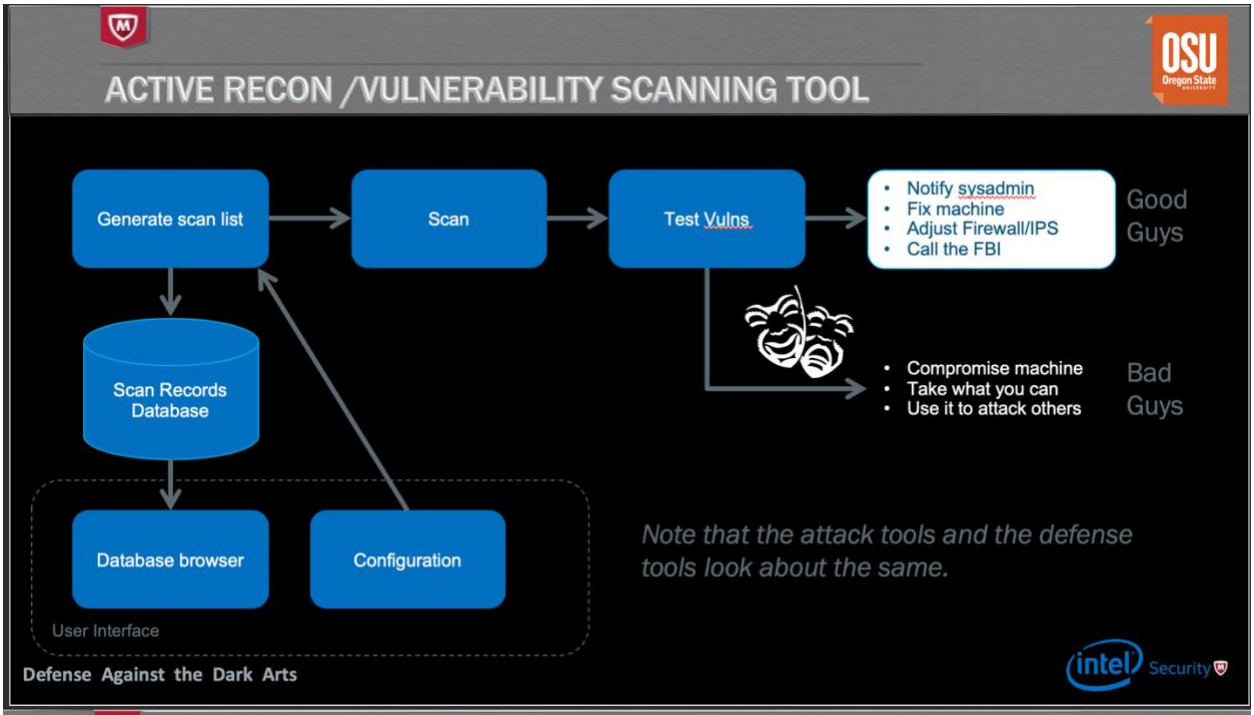


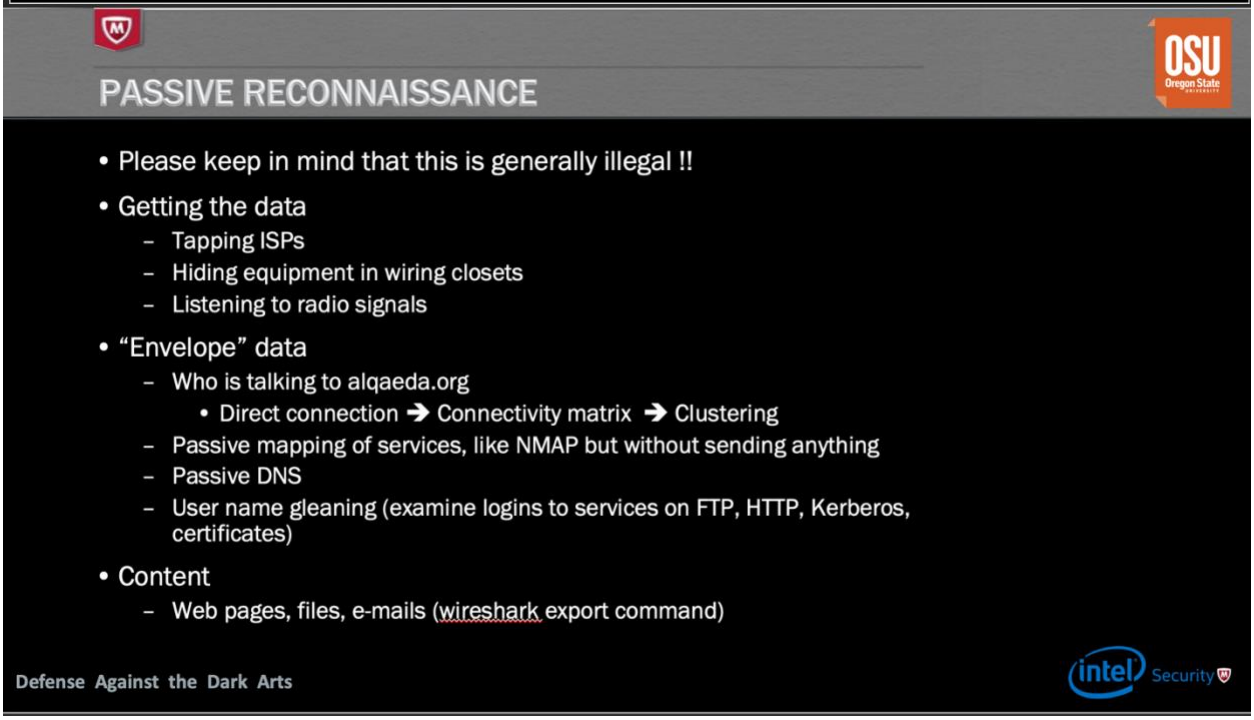
- Network Security Products
- IDS ➔ Passive Capture + Deep Stateful Inspection + Intrusion Detection
- IPS ➔ IDS + Blocking traffic
- NGIPS ➔ IPS + Packet Filtering + Crypto Inspection + Static Analysis
- Firewall ➔ Packet Filtering + Deep St. Inspection + Policy
- NGFW ➔ Firewall + IPS + Crypto Inspection + App ID
- Web Gateway ➔
- Proxy + Intrusion Detection + Static Analysis + Crypto Inspection + Policy
- Email Gateway ➔ Proxy + Intrusion Detection
- Data Loss Prevention (Data at Rest) ➔
- Vulnerability Scanning + Intrusion Detection + Dictionary Lookups
- MITM – Man in the Middle
- Detection of MITM
- Putting it Together: SSL/TLS. Guarantees and Vulnerabilities



- Covert Channels: Hidden from traditional network control devices, Leverages channels to transmit information that weren't intended to do so, Usually very low bandwidth
- Policy Hold and Limitations
- Lab 2 – Starter Script – Python







- RECON – Defenses
- Policy and Deep Inspection helps. Honeynets can slow down recon. Usually detected during log-correlation – SIEM, IPS, Firewall. Hard to defend against passive recon
- Spoofing Threat: Attacker masquerades as another network entity in order to gain some advantage over the network defenses of the target.
- LAND Attack: A DoS attack that relied on spoofing
- IP and ARP spoofing to perform MITM attacks
- Used to poison ARP DBs to perform MITM

- Most network security solutions perform some basic checks to detect and defend against spoofing
- Threats – Resource Consumption Attacks
- DoS = Denial of Service
    - About consuming resources for an extended period of time such that the targeted service is degraded, some times to a point where it is unusable
- DDoS = Distributed DoS
    - Asymmetrical resource utilization (attackers needs to spend fewer resources than the subject of attack) is the key to the success of most DoS attacks
    - DDoS leverages large numbers of computers to perform one or more resource exhaustion attacks against a target such that it is overwhelmed and unable to perform its function.
    - Harder to defend against
- Motivation for a DoS attack:
    - Hacktivism
    - Financial Gain
    - Cyber War
    - Cyber Terrorism
    - Unintentional: slashdot, reddit, etc.
- Types of DOS
- **Network exhaustion**: Flooding the network so that the service is unreachable or is reachable with such high latency that it is useless
- E.g.: DNS amplification attacks
- **CPU exhaustion**: Make CPU so busy, legitimate traffic cannot be served.
- E.g: TCP ACK flood: Busy servers could spend CPU searching for right TCB, Fragmentation attack: don't send the first fragment.
- **Memory exhaustion**: Cause server to run out of memory and slow down/crash
- E.g: TCP SYN flood (NMAP can do this, but don't try it on the campus net!)
- **Storage exhaustion**: Cause server to run out of disk space
- **Application vulnerability exploitation**: making the application unavailable by crashing it or the OS.
- **Other finite resources**: sockets, TCP listen queue, connection pool, firewall session tables, SSL exhaustion, etc.
- DOS Defenses – Network traffic validation and cleansing by network products, traffic scrubbing centers
- Threats – Bugs and Back Doors
    - Backdoors are intentional, bugs are unintentional, the threat of compromise is the same
- Defense Basics – Packet Filtering, NAT, and Proxying
- Packet Filtering: Basic first step toward protecting your network. Clear network boundaries and segmentation is key
- Basic packet validation including defense against segmentation, fragmentation attacks, malformed packets and streams is implicit

- Deep Inspection - Adds inspection of the data portion of the packet in addition to the network headers: Trace protocol headers, Multiple protocols (modern firewalls recognize the protocols dynamically), Signature processing on content (IPS), Dictionary processing on content ("Data Loss Protection")
- Proxying: Basic limitation of basic packet filtering: Cannot understand higher level applications and protocols and hence cannot easily shield internal endpoints from application level attacks
- Proxies:
    - MITM: Terminate TCP connections and establish new ones
    - Inspects and sometimes modifies application data to prevent attacks
    - Provides nuanced and granular access control based on application specific information.
    - Transparent vs. non-transparent proxy.
    - Cons: lower performance compared to basic packet filtering (why?)
- NAT: Network Address Translation: Initially proposed to allow multiple endpoints to share the same IP address. Makes it harder for attacker to learn the network architecture by hiding local IP addresses
- How it works: Temporarily maps a connection from a local private IP and port to a public IP address and port to be used on the public side of that communication.
- NAT prevents you from connecting directly to a specific endpoint behind a NAT device
- STUN: Simple Traversal of UDP through NAT
- TURN: Traversal Using Relay NAT
- VPN / IPSec - IPSec is most commonly deployed in tunnel mode, where complete IP packets are encapsulated inside the AH. This "IP-in-IPSec" tunnel allows a connection between a machine and a network (or two networks) over the Internet.
- Defense – NIPS
- NIPS: Network Intrusion Prevention System
- IPS detection strategies – signature-based (looks for patterns presumed to be malicious) and anomaly-based (network behavior analysis)
- IPS Today AKA NGIPS
- Intelligence and Connected Security – network devices & IoT
- AET – Advanced Evasion Techniques
- Software Defined Networks (SDN) - This turned into Software Defined Networking. In 10 years, this may be renamed "network switching."
- Switch Working – Openflow SDn
- Overflow sections
- Predictive Attacks - In a predictive attack, the attacker predicts the behavior of the target, causing the target to help play a part in the attack.
- TCP Reconnaissance through firewall—FIN scan
- Database Poisoning, also ARP poisoning (MITM), DNS poisoning
- DNS queries work from the root servers down. www.unixwiz.net - Each query either gives the answer or tells you where to ask next, so eventually you get the answer
- Kaminsky DNS Poisoning
- New Stuff: Attack on OSPF Routing (RFC 2328)