**Cyber Security Notes**

Cyber Security = Preventative methods used to protect information from being stolen, compromised, or attacked.

Three points of attack: Data itself, network connection points, the people

**Types of Security**

* Network
* Application
* Information
* Disaster Recovery
* End-user education

**Topics**

* Network Structure
* Data Packets
* IP Addresses
* Uniform Resource Locators (URL)
* MAC Addresses
* Protocols\Ports

The Open Systems Interconnect (OSI) Model

**P**lease **D**o **N**ot **T**ell **S**ecret **P**asswords **A**nytime

Physical Data Link Network Transport Session Presentation Application

**Types of Attacks**

**Intrusion**

* Cracking
* Social Engineering
* War-Dialing
* War-Driving

**Blocking**

* Denial of Service
* Distributed Denial of Service

**Malware**

* Viruses
* Worms
* Trojan Horses
* Spyware
* Cookies
* Ley Loggers

**Hacking Terms**

White Hat Hackers

Grey Hat Hackers

Black Hat Hackers

Script Kiddy

Cracker

Ethical Hacker or Sneaker

Phreaking

**Security Terminology**

Firewall

Proxy Server

Intrusion-Detection System

Access Control

Non-repudiation

Auditing

UDP – User Datagram Protocol

* Connectionless
* Packets are sent in chucks
* Faster

TCP – Transmission Control Protocol

* Connected
* Bidirectional communication
* More reliable

**Denial of Service (DOS)** = Sending too much data to computer causing it to crash.

**Distributed Denial of Service (DDOS)** = A DOS attack launched from multiple clients (a botnet)

**Syn Flood** = Takes advantage of the TCP Handshake process

Protected by:

Micro blocks = Allocate little memory to process incoming SYN objects

Bandwidth Throttling = after detecting the source of the attack the firewall restricts the bandwidth

**Smurf Attack** = Uses ICMP packets to execute the attack

**Ping of Death (PoD)** = Attacks machines that cannot handle oversized packets. Most current OS’s drop oversized packets

**UDP Flood** = Sends packets to random ports, if enough data is sent the target computer shuts down. Variation to the PoD.

**ICMP** = Another name for a ping flood or Syn Flood

**HTTP Post DoS** = Hangs server with slowly delivered HTTP post messages

**Permanent DoS (PDoS) (a.k.a phlashing)** = Damages the system badly, often attacks firmware

**Distributed Reflection DoS (DRDOS) =** Uses routers to execute a DoS attack, fixed by configuring routers = to not forward broadcast packets

**DoS Tools**: Low Orbit Ion Cannon, High Orbit Ion Cannon, DoSHTTP, Kali Linux

**Buffer Overflow** = Designed to put more information in the buffer than it is meant to hold. Common in Java.

**IP Spoofing** = Source address of packet is changed.

**Session Hijacking (Man in the Middle):** Hacker takes over a TCP session. Can be done if the hacker gains access to the target machine.

**Virus** – Malware that replicates when executed

**Logic Bomb** – Set of instructions secretly incorporated into a program so that if a particular condition is satisfied they will be carried out.

**Backdoor** – Covert method of bypassing normal authentication or encryption

**My doom** – 2004 virus targeting Microsoft, sent via email attachment, opened a backdoor and sent to contacts in the targets email list.

Viruses require human interaction, Worms do not require human interaction.

**Trojan Horse** – Program that looks benign but has malicious intent.

**Gameover ZeuS** – Peer to peer botnet Trojan Horse, encrypted peer to peer communication, mainly used for bank theft, created by Evgeniy Mikhailovich Bogachev, $3 million reward.

**Chapter 3:** Firewalls

Firewall: Barrier in between the world and your network.

Firewalls provide: Packet filtering, Stateful packet filtering, User authentication, client application authentication

**Types of firewalls**

**Packet filtering firewall**

Very basic type of firewall

Also referred as screening firewalls

Works by examining packets

Does not compare packets

No authentication

Susceptible to SYN and ping floods

Does not track packets

Does not look at the data just the header

Not necessarily the most secure firewall

Rules: What types of protocol to allow, What source ports to allow, Destination Ports, and ip addresses

**Stateful Packet Inspection (SPI)**

Knows the context of packets = less susceptible to flood attacks

Knows if packets are part of a stream

Recognizes ip address in the firewall

Can look at contents of the packets

The recommended firewall

**Application gateway**

Known as a application proxy or application level proxy

Examines the connection between the client and the server applications

Enables admins to specify what applications are allowed

Allows user authentication

Requires more resources

Susceptible to flood attacks : due to time it takes to authenticate and once connected packets are not checked

**Circuit level gateway**

More secure than application gateways

Typically implemented on high end equipment

Authenticates users first

Virtual circuit is used to pass bytes between client and proxy server

External users only see the proxy ip address+

**Hybrid Firewalls**

Becoming more popular these configurations take multiple approaches to their firewall implementations

SPI and circuit level gateways might be used together0

**Network host-based**1

Software based solution runs on top of OS

Make sure all patches are updated, uninstall uneeded applications or utilities, close unused ports, turn off all unused services24

**DMZ (Demilitarized Zone)**

Two separate firewalls

One faces the outside

One faces inside

Web email and ftp servers are located in between the two firewalls

**Dual Homed-Hosts**

Expanded version of the network host

Runs on top of an existing OS

Relies on security of the OS

**Router Based Firewall**

Usually the first line of defense

Uses simple packet filtering

Ideal for novice admins

Can be preconfigured

Can be placed between segments of a network

**Screened Host**

Combination of firewalls

Bastion host and screening router

Similar in concept to a dual-homed host

**11/27/20**

**Ports**

80 – HTTP

443 -HTTPS

22-SSH

3389-Remote Desktop

20-21-FTP

IDS allows system admins to detect possible attacks to a network

Preemptive blocking aka banishment vigilance

Attempts to detect impending intrusions through foot printing

Susceptible to false positives = may block legitimate traffic

Anomaly detection

* Any activity that do not match normal use is save in a log

Threshold monitoring

* Defines acceptable behavior
* Presets acceptable behavior levels
* Monitors the exceeding of those levels
* Difficult to set times for monitoring behavior
* Susceptible to false positives and negatives

Resource profiling

* Measures system wide resource use to develop a historic usage profile
* Abnormal readings can indicate illicit activity

User\Group work profiling

* Each user\group typical activities are stored in its work profile
* Activities not typical of that user or group are suspect
* Changes in work patterns need to be updated in profile
* Dynamic users are hard to profile

Executable profiling

* Measures and monitors how programs use system resources
* Helpful in detecting many types of malware attacks
* System services cannot be traced to a particular user
* Profiles how system objects are normally used

IDS Components

* Activity
* Admittatur
* Sensor
* Analyzer
* Alert
* Manager
* Notification
* Operator
* Event
* Data source

IDS(Intruder detection System) IPS(Intruder prevention system)

Passive Active

Logs Activity Takes steps to prevent an attack to progress

Alerts an admin Problems of false positives

Snort

Most well know open source ids

Heuristic = Non-intrusive and doesn’t have a set procedure

Fiddler

Wireshark

Kali linux

Virtual system

1/29/20

Social Engineering = Social engineering is the psychological manipulation of people into performing actions or divulging confidential information

Attack techniques

Commitment = When the attacker tricks the victim in to making a promise which he or she will feel obligated to keep. Conformity is a special type where the commitment is a leveraged commitment made by society rather than an individual.

Authority = Process of an attacker assuming a role of authority which he does not possess. 3 types: Impersonation, Diffusion of responsibility, Reciprocation

Reciprocation = When the attacker gives the victim a gift and the victim feels a social pressure to return the favor

reverse engineering: Where the aggressor tricks the victim into asking him for assistance in solving a problem. 1) Sabotage, 2) Advertise, 3) Assist.

Likening = The process of an attacker behaving in a way to appear similar to a member of a trusted group

Scarcity = Occurs when the attacker is able to introduce the perception of scarcity of a high value item. Rushing involves putting severe time constraints on a decision.

Best defense is EDUCATION

Training

Reaction = raise alert state

Inoculation = attack resistance

Tailgating = Seeking entry to a restricted area secured by walking in after someone else has opened the door.

Shoulder Surfing = Looking over someone’s shoulder to see them type their password or to read a document

Leaving Computer Unlocked

PII (Personally Indefinable Information)

Full name

PIN = SSN , Drivers license, ect

Personal address

Personal phone and email

Personal characteristics

Biometric data

Financial data

Date of birth

Place you were born

Business phone email address

Race

Religion

Employment information

Medical info

Education info

Financial info

Phishing is the fraudulent attempt to obtain sensitive information

Spear phishing – directed at specific individuals

Whaling – Targets a specific individuals or companies

Vishing – voice call

Smishing – SMS\Text message

Facebook

HIPPA (Health Insurance Portability and Accountability Act) Act of 1996

Designed to protect the privacy and security of certain health insurance

2/3/20

Encryption

Scrambling information

Without it all firewalls IDS\IPS anti spyware antivirus and policies are inadequate

Cryptography = Art of deciphering codes

Encryption

* Algorithm scrambles plain text
* Sender and receiver agree on algorithm
* Message difficult to re-create without protocol

Decryption

* Reversal of the scrambling of text

Plain text > Key > cipher text > Key > plain text

Transposition rearranging each letter with a different letter

Substitution replaces each letter with a different letter

Atbash Cipher (Substitution) = Hebrew code that substitutes the first letter of the alphabet for the last letter ect.

Hello world becomes Svool Dliow

Rail Fence (Transposition) = Message is wrapped around a stick to be decoded

Ceaser Cipher = Shifts letters based on how big the key is

Hello World key of 2 = Jgnnq yqtnf

Vigenere Cipher = Grid like encryption

Charles Babbage broke Vigenere Cipher

Enigma = Arthur Scherbius invented in 1918

Turing = Created the colossus in 1940s, cracked the enigma code, developed the Turing test

Symmetric Encryption

Plain Text > Key > Cipher text > Key > Plain text

Bitwise substitution = If inputs match it prints 0 and if they don’t it prints 1

Data Encryption Standard created in 1977

Lucifer (Created by Horst Feistel in 1971) with 56 bit keys

Moore’s Law = Speeds of circuits double every two years due to the density of transistors

Triple DES = Encrypt the message 3 times

Diffie Hellman helped create asymmetric encryption

Asymmetric key

Plain text > Key 1 > Cipher Text > Key 2 > Plain text

**VPN**

PPTP (Point to point tunneling Protocol)

Pap = password authentication protocol, most basic authentication type; password and username is sent in clear text

SPAP = password and username is encrypted but susceptible to playback attack

Kerberos = password is never sent, server uses the stored hash

**OS** **Hardening**

Configure windows properly