Bootcamp Intro PPT

Session 1.1 Security 101 I

Tuesday September 1, 2020 / 6:30-9:30 PM
Zoom Link: https://zoom.us/j/2246200754
Zoom Password: 508637

Introduction

- **Krishana Anderson**
    - **Office Hours:** 12-5 PM / **M-Th**
    - No more than **8 absences**.
    - No more than **2 missed or incomplete assignments**.
    - Hold at least a **70% average** on homeworks and pojects.
    - Participate in all projects.
    - Balance paid in full.
    - Academic Honesty.
    - **Drop Period** is the first week of class (including transferring section).
    - **Drop Deadline** is **Tuesday, September 8, 2020**.
    - Speak with Erin and Robert about any homework issues.
    - **CompTIA**: (Weeks 10-13)
        - Access to CompTIA CertMaster Practice Practice for Security+.
        - CompTIA Security+ Exam Voucher. (Good for 12 months.)
    - **Ways to get support**:
        - Speak up, reach out, and **attend office hours**.
        - There are 30 minutes of office hours after class.
        - Form study groups.
        - Use a **support ticket** in Bootcamp Spot to **request a tutor**. (1 hr/week)
    - Access to career services.
- **Erin, Robert, Siddartha, and Srividhyaa (Instructors)**
    - Assignments will be made available by the 2nd session of each weekly topic.
    - Assignments open until the end of the consecutive weekly topic.
    - Grade deductions for late homework.
    - Locked homework require tutoring fo submission.
    - Surprise Quiz Games, "Cold Calls".

    - Extra Credit Assignment.
    - Assignment exmpansion.
    - Hints. (Coughs when something is important.)
    - Ask good questions, take good notes.
    - Utilize resources.
    - Have a good attitude. (Be persistant.)
    - Teamwork. (Grades are shared - weakest link is the highest grade mark.)
    - Respect.
    - Class Goals
- **Why security and cyber-skills is important/relevant today.**
    - Explosive growth in dependence on IT
    - More user on conencted devices.
    - Better tools, bigger damage.
    - Significant investment by bad actors.
    - Dire shortage of skilled professionals.
- **Defining Cybersecurity**:
    - Assessment of threats and migitation of risks.
    - Example hack: Stuxnet, 2009. Malware worm distributed on USBs.
    - **Castle Model** vs **layers of security** (that assume a breach) to protect an **asset**, typically **data**.
- **Course Overview**:
    - **Goals**
        - Threat assesment.
        - Risk mitigation.
    - **Daily Routine**
        - Set objectives.
        - Brief background lecture.
        - Instructor demonstrations.
        - Thought exercises.
        - In-class skill builder.
        - Project work.
- **Tips**:
    - Curiosity.
    - Embrace being a beginner.
    - Find your community now.
    - Put in the hours.
- **Attacking the Wall Activity:**
    - Users and Admin **<-->** Web Login **<-->** Server **<-->** Data
- **Defining User Attack Strategies:**
    - Social engineering.
    - Phishing.

    - Credential reuse. (Check login events with time and amount. Policies.)
    - Malware.
    - Man-in-the-middle-attack.
    - Sniffing packets.
    - Stolen hardware.
- **Website Attacks:**
    - Brute force strategy.
    - Code-injection.
    - Faulty session management.
- **Server Attacks:**
    - Malicious software.
    - OS exploits.
- **Database Attacks:**
    - Unpatched database.
    - Lack of segregation.
    - Default credentials.

Bootcamp PPT#2

Session 1.2 Security 101 II

Thursday September 3, 2020 / 6:30-9:30 PM
Zoom Link: https://zoom.us/j/2246200754
Zoom Password: 508637

Securing Cyberspace

- Class Objectives
    - Definition of CIA triad and elements.
    - Contextualize technical terms in trends and reports.
- Phone
    - Wiped and re-sold.
    - Memory harvested.
    - Credentials for email.
    - Purchases made illegally.
    - Malware installed.
    - Contacts for social engineering.
- CIA Triad (Security Model)
    - **Availiability:** Ensure that the information expected is accessible to privileged users.
    - **Integrity:** Mainting **expected state of systems**. Honest, whole, and undivided.
    - **Confidentiality:** Keeping information secret. The state of being kept secret or private.
- Defending the Triad

    - authorized personal, keycards, good policies, etc.
- Soft skills vs technical skills
- Security Domains

Bootcamp PPT#3

Session 1.3 Security 101 III

Tuesday September 8, 2020 / 6:30-9:30 PM
Zoom Link: https://zoom.us/j/2246200754
Zoom Password: 508637

Landscape of Certifications

- Security+ *(CompTIA Basic Certification)*
- Network+ *(CompTIA Network Certification)*
- Linux+ *(CompTIA Linux Certification)*
- Pentest+ *(CompTIA Pentest+)*
- CISSP *(ISC2 ISSAP Architecture)*
- CISSP *(ISC2 ISSEP Engineering)*
- CISSP *(ISC2 ISSMP Management)*
- GAWN *(GIAC Assessing Wireless Networks)*
- GREM *(GIAC Reverse Engineering Malware)*
- CCIE *(Cisco Certified Internetwork Expert)*
- KLCP *(Kali Linux Certified Professional)*
- CPEH *(Certified Professional Ethical Hacker)*

Bootcamp PPT#4

Session 2.1 Governance, Risk, and Compliance I

Thursday September 10, 2020 / 6:30-9:30 PM
Zoom Link: https://zoom.us/j/2246200754
Zoom Password: 508637

GRC: Security Within an Organization

- Identify 3 concrete benefits of a healthy security culture.
- Responsibitilty of C Suite Officers and CISO Roles.
- Security department roles responsibilities.
- Identify appropriate security controls for a given resource and situation.

Security Aligning within an Organization

- Tools for techincal roles.
- Soft Skills in demand.
- **Linux and Windows**
    - Managing users, permissions, scheduling tasks, manage installed software with **apt**.
- **Networking**
    - Configure firewalls, port scan remote hosts, analyze network traffic.
- **Web Vulnerabilities and Web Services**
    - Burp Suite
- **Offensive Security**
- **Defensive Security**
- Security Concerns VS Business Concerns
    - **Security Goal:** Protect data. (Improve **security posture**.)
        - **Passive** VS **Defensive**
    - **Business Goal:** Maximize profit and improve efficiency.
    - Balance of **adequate protection** for important **assets**.
- **GRC Framework**
    - **Governance:** Creating management **processes for implementing security practices**.
    - **Compliance:** Making sure the business follows **internal security policies**.
    - **Risk Management:** Identifying an organizations most important **assets** and determining how the might be **compromised**.

Security Culture and Framework

- Security Culture is the way members of an organization think about and approach security issues.
- How important or aware with regard to security are employees?
- **How to Motive Employees within a Culture Framework:**
    - Measure and Set Goals
        - Phishing email campaign with statistical expectations.
    - Involve the Right People
        - Inform Management
    - Create an Action Plan
        - Develop Training
    - Execute the Plan
        - Deploy training

    - Measure the Change
        - Phishing email campaign with statistical expectations.
- Encourage people, don't punish them.

Example Roles

- **CEO:** Chief Executive Officer
- **CFO:** Chief Financial Officer
- **COO:** Chief Operations Officer
- **CISO:** Chief Information Security Officer
- **CIO:** Chief Information Officer
- **CTO:** Chief Technology Officer

Reporting Structure

- **Network Engineer** reports to...
- **Performance Manager** reports to...
- **Director of IT** reports to...
- **VP of Networking**

Responsibilities

- Director of Networking
- IR or SOC Manager
- Security Architect

Security Controls

- Long term vs Short term
- **Security Control:** system processes or technology that protects CIA model.
    - **Preventative**
    - **Deterrent**
    - **Detective**
    - **Corrective**
    - **Compensating**
- **Access Points for Servers**
    - **VPN**
    - SSH protocol and **keys** and **passwords**.
    - Strong **updated passwords**.
- **Control Diversity**
    - Firewall VPN.
    - Authentication of keys and passwords.
    - Limited time of compromise.

- **Redundancy** and Single Points of Failure
    - Multiple methods in case one fails

Bootcamp PPT#5

Session 2.2 Governance, Risk, and Compliance II

Sunday September 13, 2020 / 6:30-9:30 PM
Zoom Link: https://zoom.us/j/2246200754
Zoom Password: 508637

Class Objectives

- Identify threats, attacks, and vulnerabilities.
- Prioritize risks ased on likelihood.
- Choose and justify controls.

GRC: Risk Management and Threat Modeling

- Difference between **vulnerablity**, **threat**, and **risk**.
- **Vulnerability:** Lack of protection, asset that can be exploited.
- **Threats:** The actor or agent that will exploit a vulnerability.
- **Risks:** Outcomes and possibilites.

Risk Management

- Measured quantitatively.

Threat Modeling

- Results shared upwards, theoretical.
- **PASTA:** Process for Attack Simulation & Threat Analysis
- **STRIDE:** Spoofing tampering, repudiation, information disclosure, denial of service, elevation of privilege.
- **OWASP:** Open web application security project.
    - **Determine asset scope.** Developing inventory with priority.
    - **Identify threat agents.** Identifying ATP, Script Kiddies, Employees, and Incomptetence.
    - **Identify potential attacks.** Analyze each agent, identify **motivation**, **skill level**, and **funding**.
    - **Identify exploitable vulnerabilities.** Identify vulnerable points in the system or network.
    - **Prioritize identifies risks.**
    - **Mitigate risks.**

Risk Analysis

- **Qualitative:** identifying intuitive, unmeasurable factors.
- **Quantitative:** measuring expectation of risks with respect to data.
  - **Asset Value** *AV*
  - **Exposure** *EF*
  - **Annual Rate of Occurance** *ARO = AV x EF*
  - **Annual Lost Expectancy** *ALE = SLE x ARO*

Mitigating Risks

- **Control Types**
  - Physical, Administrative, Technical
- **Necessary Effectiveness**
- **Cost** / **Time** of Implementation

Practical Threat Modeling

- Answering the **4 Golden Questions**:
  - What are we working on?
  - What can do wrong?
  - What will we do about it?
  - Did we do a good job?
- Secure Coding Practices

Bootcamp PPT#6

Session 2.3 Governance, Risk, and Compliance III

Tuesday September 15, 2020 / 6:30-9:30 PM
Zoom Link: https://zoom.us/j/2246200754
Zoom Password: 508637

Class Objectives

- How to use policy procedures to formalize standards or right and wrong.
- Use governance frameworks to determine which policies an organization must develop.
- Explain how audits are used to ensure compliance.
- Develop business continuity and disaster recovery plans.

Governance and Compliance (BCP/DR)

- **Governance:** Codifying proper behavior.
- **Compliance:** Enforcing policies.

Codifying Rules and Policy Procedures

- **Policy:** rule that defines the right behavior.
    - Policies inform standards for behavior and operations.
- **Governance Framework:** defines the policies an organization must follow.
    - Federal or government standards.
- **GDPR:** General Data Protection Regulation
- Training plan, rules as examples of policies, and goal of defining and implementing new policy.
- **Internal/Volitional** vs **External/Imposed** goals.
    - Alphanumeric password policy.

Using Governance Frameworks to Guide Policy Desicions

- **External Objective** and **Policy**
    - Businesses often have to follow external rules in addition to those they set for themselves.
- **Governance Frameworks:** rules and policies that must be followed by an entire organization opr industry.
- **Securities and Exchange Commission** (SEC): regulators for security, policy enforcement, incident reporting enforcement, and auditing.
    - **GDPR:** General Data Protection Regulation
    - **HIPAA:** Health Insurance Portability and Accountability Act
    - **PCI-DSS:** Payment Card Industry Data Security Standard

Business Continuity and Disaster Recovery

- **Mild/moderate:** business has been impacted but can still handle day to day operations.
- **Serious/catastrophic breach:** impact so severe that operations are halted.
- Cyber attacks, human error, and enviromental disasters.
- **Business Continuity Plan** vs **Disaster Recovery**
    - Contingency planning:
        - Responsibility of emergency response.
        - Resource requirements.
        - Training requirements.
        - Scheduling maintenance.
    - Strategies for high-impact loss

    - **NIST** Impact Levels: **Low**, **Moderate**, **High**
- **Business Impact Analysis and Risk Assesment**
    - **Identify** key processes.
    - **Establish** a detailed list of requirement.
    - **Determine** resource requirements.
    - **Evaluate impact** on daily operation.
    - **Develop priorities** and classifications of functions.
    - **Develop** recovery time requirements.
    - **Determine disruption** of financial operations and legal operations.
- **BIA Metrics**
    - **Recovery Point Objective:** amount of time that a business can afford to lose.
    - **Maximum Tolerable Downtime:** total amount of time a system can afford to be unavailable to users.
        - **RTO:** *Recovery Time Objective*
        - **WRT:** *Work Recovery Time*

Bootcamp PPT#7

Session 3.1 Intro to Terminal and Bash I

Thursday September 17, 2020 / 6:30-9:30 PM
Zoom Link: https://zoom.us/j/2246200754
Zoom Password: 508637

Notes

- File navigation and basic **bash** commands.
- Command line
- Virtual vs Physical Machines
    - **VM:** simulates computer architecture for a particular OS.
- **Basic Commands:**
    - `open` / `echo` / `cat`
    - `man` / `*` / `&&` / `tmux`
- **Directory Navigation:**
    - `pwd` / `ls` / `cd` / `which`
- **File/Directory Creation:**
    - `touch` / `mv` / `cp` / `mkdir`
- **File/Directory Removal:**
    - `rm` / `rmdir` / `clear`

- **File Viewing/Editing:**
    - `more` / `less`
    - `head` / `tail`
    - `vim` / `nano`
- **File/Data Search/Actions:**
    - `find` / `grep` / `file`
    - `curl` / `wget`
- **New Commands:**
    - `mkfifo` (open pipe)
    - **Absolute** path *vs* **Relative** path

Bootcamp PPT#8

Session 3.1 Intro to Terminal and Bash I

Saturday September 19, 2020 / 6:30-9:30 PM
Zoom Link: https://zoom.us/j/2246200754
Zoom Password: 508637

Introduction

- Today we willl be using `man` / `find` / `grep` and `wc` .

Notes

- Command Structure
    - `<command> <arguement>`
- Options
    - Set by *flags* `-`.
    - Options with arguements are *parameters*.
- **Man** Pages
    - Search document with `/`
- **Find**
    - Find files/directories by name.
- **Grep**
    - Find files by internal content.
- **Piping**

Bootcamp PPT#9

Session 3.1 Intro to Terminal and Bash I

Tuesday September 22, 2020 / 6:30-9:30 PM
Zoom Link: https://zoom.us/j/2246200754
Zoom Password: 508637

Introduction

- Benefits of CLI text processors.
- `sed` / `awk` / `and` / `nano`

Text Processing

- **sed**
  - stream editor
  - `sed 's/<oldValue>/<replacementValue>/g' fileName`
- **awk**
  - `awk -F<delim> '{print $NUM1,$NUM2,...}' fileName`
  - Delimeters can be `" "` or `,`
  - Note that the argument for the delimeter has not space after the delimeter flag, `-F`.

Bootcamp PPT#10

Session 4.1 - Linux Administration and Hardening I

Thursday September 24, 2020 / 6:30-9:30 PM
Zoom Link: https://zoom.us/j/2246200754
Zoom Password: 508637

Introduction

- **Linux**, Unix (FOSS or *Free Open Source Software*)
  - debian
  - ubuntu
  - kali
  - fedora
  - centos
- SELinux *(NSA Developed)*
- **LTS** *Long Term Support*
- **Operating System**
  - basic functions
  - scheduling

  - tasks
  - executing applications
  - controlling peripherals
- command line (headless)
- **linux desktop environments**
  - unity
  - gnome
  - mate
  - kde
  - xfce
  - lxde

Administration

- File Structure
  - Applications stored in `/usr/bin`
  - use Bash shell by default
- Important Locations
  - `/` root folder
  - `/home` personal files
  - `/etc` configuration files
  - `/bin` , `/sbin` program files
  - `/var` files that change over time
  - `/tmp` tempory files
  - `/media` , `mnt` media/mount locations
  - `/etc/shadow` passwords
  - `/etc/hosts` local dns
  - `/proc` , `/boot` processes and boot files
- boot process
  - *power on self test* **post**
  - *basic input output system* **bios** (Windows)
  - *unified extensible firmware interface* **UEFI** (Linux)
  - *grand unified bootloader* **grub** (Linux)
  - **boot order** (master boot record)
- *central processing unit* **CPU**
  - brain of the system

Managing Processes

- **processes**
  - `top` , `ps` , `kill`
  - `pstree`, `pidof`
  - consuming resources
  - **CPU** and **RAM**
  - makes data active
  - **RAM** vs **Disk Space**

Packages

- Aptitude Package Manager

Bootcamp PPT#11

Session 4.3 - Linux Administration and Hardening III

Tuesday September 29, 2020 / 6:30-9:30 PM
Zoom Link: https://zoom.us/j/2246200754
Zoom Password: 508637

Managing Permissions and Services

- Access Controls and Managing Services
  - Inspect and set permissions.
  - Manage and monitor services.
  - Create and assign users for services.
- Access Controls

- Read (r), Write (w), and Execute

- Discretionary Access Control (DAC)

- Every file has a...
  - owner
  - group
  - other
- `chmod`
  - `u=` user
  - `g=` group
  - `o-` other
  - `+` add, `-` minus
- `chown`

    - example: `sudo chown root:root myFile`
- format
    - `-` = file , `d` = directory
    - `[f][uuu][ggg][ooo] N`
- `ln`
    - symbolic links
    - hard links
    - `-s <file1> <file2>`

Managing Services

- Servers
    - computers that offer services
- Services and Security
    - attackers can manipulate services
- `systemd` vs `systemcl`
- Important Commands
    - `systemd` vs `systemctl`
    - `systemctl -t service -all` list all services
    - `systemctl status <daemon>` list status
    - `systemctl stop <daemon>` stop daemon
    - `systemctl enable <daemon>` set autostart
    - `systemctl disable <daemon>` remove autostart

Bootcamp PPT#12

Session 5.1 Linux Archiving and Logging Data I

Thursday October 1, 2020 / 6:30-9:30 PM
Zoom Link: https://zoom.us/j/2246200754
Zoom Password: 508637

Backups & Restoring Data with tar

- Archiving Data
    - Ensuring data availability.
    - Overseeing backup and recovery.
    - Determining frequency of backups.
    - Determining data retention time.

- Scheduling Backups
    - Keeping things up to date and patched.
- Monitoring Log Files
- `gzip` and `gunzip` tar compression
- `tar` *(tape archive)*
    - **archive** vs **compression**
    - `tar cvf fileName.tar <location>`
    - `tar xvf fileName.tar -C <location> --wildcards "*filesToSave*"`
    - `cvf` is multi-option
    - `c` creating archive
    - `t` taking a peak
    - `x` unarchiving
    - `v` verbose prints progress status
    - `vv` very verbose
    - `f` title of archive
    - `-C <location>` move to location
    - `--wildcard`
- Backups
    - Saved by versions.
    - Hard drive VS every file.
    - Full backup (complete restoration)
    - Incremental backup (changes in data)
    - Differential backup(changes in data)
- Incremental Backup
    - `.snar`
    - `--listed-incremental=emerg_backup.snar`
    - `--level=0` incremental backup
    - `--incremental`
    - `D` directory
    - `Y` yes , `N` no

Bootcamp PPT#13

Session 5.2 Linux Archiving and Logging Data II

Saturday October 3, 2020 / 6:30-9:30 PM
Zoom Link: https://zoom.us/j/2246200754
Zoom Password: 508637

Introduction

- Today we will be covering `cron` .
- Automation
  - Scripts are files that contain multiple commands.
  - Scheduled jobs run command or scripts at specific, designated times.
- `cron`
  - Script or command designed to run at predefined intervals.
  - Refers to a system daemon that keeps track of when to run scheduled tasks.
  - Tasks are stored and scheduled in a file called `crontab` .
  - Location: `/etc/crontab`
  - `<Minute> <Hour> <DayOfMonth> <DayOfWeek>`
  - Check status with: `systemctl status cron`
  - List cron jobs: `crontab -l`
  - Edit cron jobs: `crontab -e`
  - Step intervals with `/n`
- `cron` jobs run under the same permissions as the user who created them.
- Avoid using the **root** `crontab` .
- Excerise Paths:
  - `/tmp/crontab.Y6pyn4/crontab`
  - `/tmp/crontab.9du52u/crontab`
  - `/tmp/crontab.71qz3k/crontab`
  - `/var/spool/cron/crontabs/sysadmin`
- `crontabs`
  - **user-level** vs **system-level**
- `anachron`
  - Has no daemon, can only be used by root.
  - Periodic task execution program.
  - `ls /etc/cron.daily` , `ls /etc/cron.weekly`
- `lynis`
  - `sudo lynis show commands`
  - `sudo lynis update info`
  - `sudo lynis audit system -Q`
  - `sudo lynis show details <[KEY]>`
  - `sudo lynis audit system --pentest`

Bootcamp PPT#14

Session 5.3 Linux Archiving and Logging Data III

Tuesday October 6, 2020 / 6:30-9:30 PM
Zoom Link: https://zoom.us/j/2246200754
Zoom Password: 508637

Proper Log Management

- `journalctl` , `logrotate` , `audit` , `splunk`
- logs
    - management
    - pinpoint threats
    - application logs
    - event logs
    - service logs
    - `var/log/auth.log`
    - `var/log/cron.log`
- investigating
- size management
- auditing
- `systemctl`
- `journalctl`
    - `systemd` daemon used for logging system events
    - does not provide reader-friendly display
    - `journald` collects and store log information
    - `journalctl --list-boots`
    - `journalctl _UID=`
    - search with `/`
- `/etc/systemd`

Log Size Management

- log files can grow to be unmanageable
- **log rotation**: process of archiving a log
    - schedule creation of new logs files
    - compression of log files
    - executing command prior/after a log
    - `/etc/logrotate.conf`
    - `logrotate -vf <pathToConfFile>`
- `auditd`
    - kernel level tool
    - `ausearch` , `aureport`

Bootcamp PPT#15

Session 6.1 Bash Scripting & Programming I

Tuesday October 8, 2020 / 6:30-9:30 PM
Zoom Link: https://zoom.us/j/2246200754
Zoom Password: 508637

Introduction

- Compounds Commands
  - Convenience and automation.
  - Linked individual commands.
- Piping & Redirection
  - `>` overwrite
  - `>>` append
  - `|` pipe output
  - `;` end of *statement*
  - `&&` conditional sequence
- `file`
  - display filetype
- `chmod u+s <fileName>`
  - sticky bit
  - `g+s` group sticky bit
  - `u+s` user sticky bit

Bootcamp PPT#16

Session 6.2 Bash Scripting & Programming II

Saturday October 10, 2020 / 6:30-9:30 PM
Zoom Link: https://zoom.us/j/2246200754
Zoom Password: 508637

If and Lists

- Comments
  - `#`
- Conditional Statement
  - `if [ <condition> ] then`
  - `if [ <condition> ] else then`

    - `if [ <condition> ] && [ <condition> ] then`
    - `if [ <condition> ] elif [ <condition> ]`
- operands
    - `-gt` greater than
    - `-lt` less that
    - `&&` successive conditional
    - `||` or
- conditionals
    - `=`
    - `==`
    - `!=`
    - `-d` existence of directory
    - `-f` existence of file

Bootcamp PPT#17

Session 6.3 Bash Scripting & Programming III

Tuesday October 13, 2020 / 6:30-9:30 PM
Zoom Link: https://zoom.us/j/2246200754
Zoom Password: 508637

Introduction

- Capture the Flag
- Headless login activity

Bootcamp PPT#18

Session 7.1 Windows Admin & Hardening I

Thursday October 15, 2020 / 6:30-9:30 PM
Zoom Link: https://zoom.us/j/2246200754
Zoom Password: 508637

Introduction

- Windows Command Prompt
- **wmic** and **Task Manager**
- Manage password policies using **gpedit**
- Scheduling tasks using **Task Scheduler**

Windows

- SOC Anylist
- System Administrator
- Penetration testing
- Endpoint forensics

Command Prompt

- `cd` or `chdir` change directories
- options with `/`
- `<PROGRAM> /?` , help for a program
- `dir` , similar to `ls`
- `>` and `|` are similar commands
- `find`
- `mkdir`
- `echo`
- `type nul` , similar to `touch`
- `call` editor
- `del` delete
- `type` is similar to `cat`
- `%<var>%` is for calling variables
- `doskey <alias>-<command>`
- `doskey /HISTORY` is similar to `history`
- `taskmgr` opens **Task Manager**
- `tasklist` , similar to `top`
- `taskkill /PID <PID>` kills processes
- `notepad` text editor
- `sc /<OPTION>` , service controller
    - `query`
    - `config`

Windows Management Intrumentation Command

- used for quick system queries and information
- `wmic /<GLOBAL SWITCHES> <ALIAS> <VERBS> /<PROPERTIES>`
- `/APPEND:` global switch example
- `wmic qfe list` searches for patches

Users and Password Policies

- `net`
  - `user`
  - `localgroup`
  - `accounts`

Bootcamp PPT#19

Session 7.2 Windows Admin & Hardening II

Saturday October 17, 2020 / 6:30-9:30 PM
Zoom Link: https://zoom.us/j/2246200754
Zoom Password: 606132

Introduction

- **Hardening** has 3 aspects.
  - **Network**
  - User
  - **Kernel**
- Powershell cmdlets.
- Piping and scripting.
- **Task Scheduler**.

Powershell

- Can manage and audit logs.
- Should be restricted to admins.
- Objects (anything PS can interact with)
- Commands
  - `Set-Location` - `cd`
  - `Get-ChildItem` - `ls` , `dir`

        - `gci -recurse -filter <thingToLookFor>`
    - `New-Item` - `mkdir` , `touch`
    - `Remove-Item` - `rm` , `rmdir`
    - `Get-Location` - `pwd`
    - `Get-Content` - `cat` , `type`
    - `Copy-Item` - `cp`
    - `Move-Item` - `mv`
    - `Write-Output` - `echo`
    - `Get-Alias` - `alias`
    - `Get-Help` - `man`
    - `Get-Process` - `ps`
    - `Stop-Process` - `kill`
    - `Get-Service` - `service --status-all`
    - `Get-WinEvent -ListLog`

Bootcamp PPT#20

Session 7.3 Windows Admin & Hardening III

Tuesday October 17, 2020 / 6:30-9:30 PM
Zoom Link: https://zoom.us/j/2246200754
Zoom Password: 606132

Introduction

- **Active Directory Domain Services**
    - Authentication
    - Authorization
    - Resources
    - Security Principles
- Central databasing and management system.
- Enterprise scale Windows environments.
- AD Architecture
    - Forest
    - Tree
    - Domain
    - OUs
    - Users

- AD Authentication Protocols
    - LDAP
    - Kerberos
    - NTLM (Outdated)
- Kerberos
    - Key Distribution Center (KDC)
    - Ticket Granting Ticket (TGT)
- Group Policy Objects (GPO)
    - Password requirements

Bootcamp PPT#21

Session 8.1 Networking Fundamentals I

Thursday October 22, 2020 / 6:30-9:30 PM
Zoom Link: https://zoom.us/j/2246200754
Zoom Password: 606132

Introduction

- Identify **clients**, **servers**, **requests**, and **responses**.
- Identify **topologies** and their advantages/disadvantages.
- Design a conceptual network.
- Convert **binary representations** into readable IP addresses.
- Modify DNS host files to redirect access of a website .

Networks

- Multiple devices connected together to share resources and services.
- **Services**, **Resources**, **Nodes**
- Security Operations Center (SOC)
- Network Security Engineers
- Penetration Testers
- **Client-Server** Model
    - **Client** = Platform
    - **Server** = Service Backend
    - Request and response method.
    - Client requests resource or service.
    - Server returns resource or executes the service.

Security

- Unauthorized access.
- Denial of Service (DOS) attacks.
- Eavesdropping.
- Data modification.

Structure

- Nodes / Endpoints
- Local Area Network (LAN)
    - Speed / Performance
    - Security
    - Versatility
- Wide Area Networks (WAN)
- Network Topologies
    - Named for geometric shape and design
    - Ring Network
        - Unidirectional
        - Bidirectional
    - Linear Topology
    - Star Topology
    - Bus Topology
        - Central Link
    - Tree Topology
    - Fully Connected
    - Mesh Topology
    - Hybrid Networks

Devices

- Router
- Switch
- Hub
- Bridge
- Modem
    - Modulater / Demodulator
    - Digital (Devices) / Analog (ISP)

- Wireless Acces Point (WAP)
- Firewall
    - Protects traffic.
- Load Balancer
    - Offsets processing loads.
    - better spread over assets.
    - Reduces Points of Failure.
- Demilitarized Zone (DMZ)
    - Subnetwork within a LAN
- CIDR-IP
- MAC Address
    - Media Access Control Address

Bootcamp PPT#22

Session 8.2 Networking Fundamentals II

Saturday October 24, 2020 / 6:30-9:30 PM
Zoom Link: https://zoom.us/j/2246200754
Zoom Password: 606132

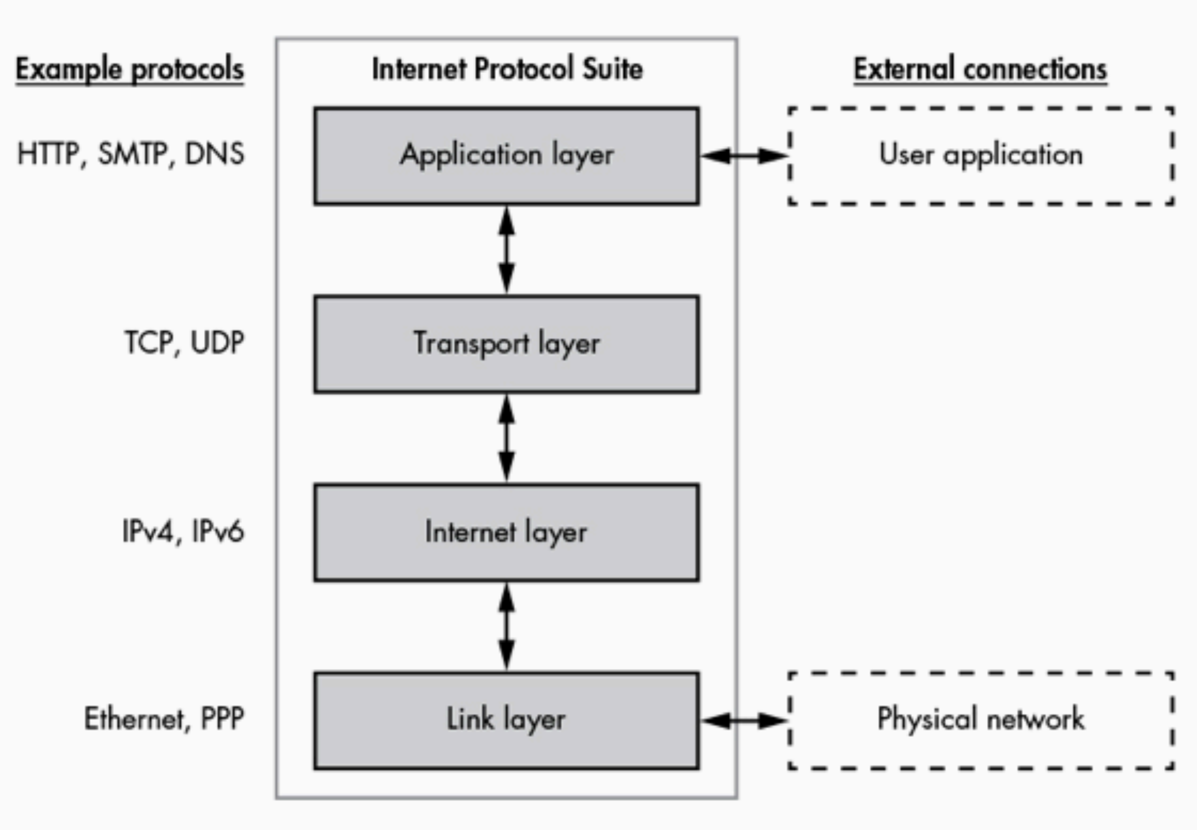
Expectations

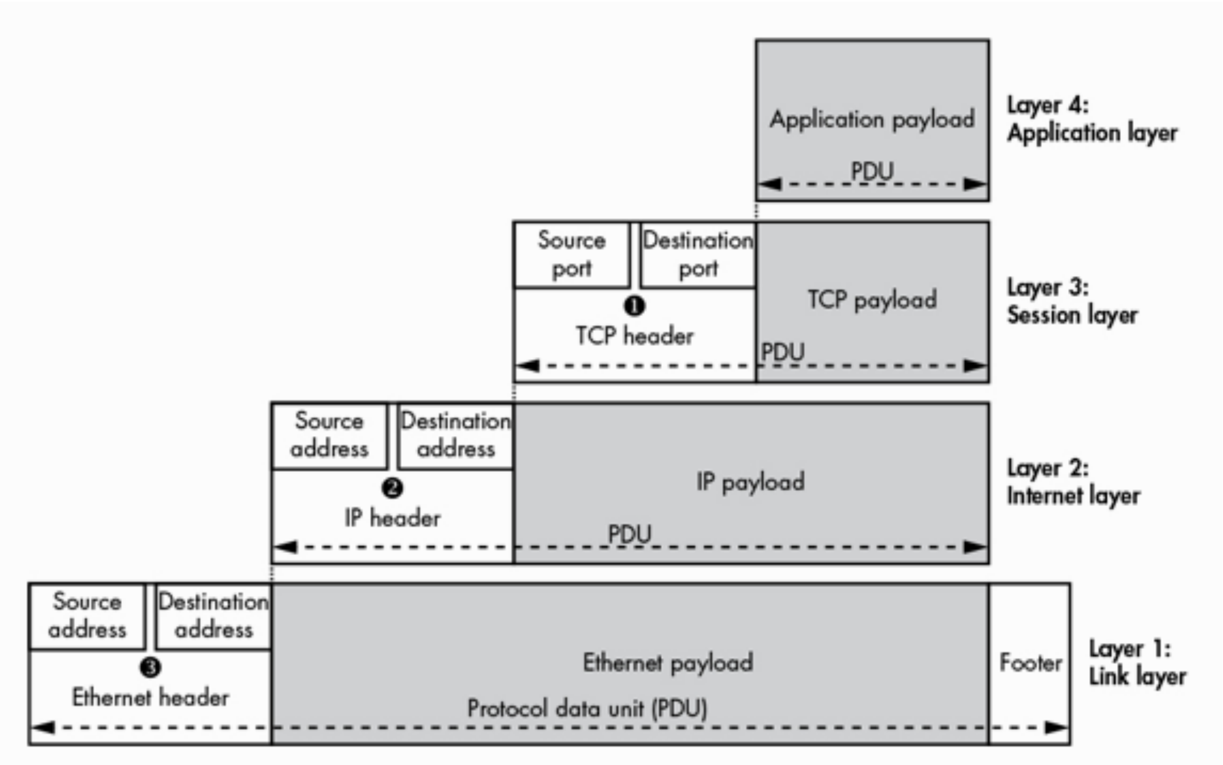
- Interpret network packets by analyzing their hearder, payload, and trailers.
- Understand the roles of network ports.
- Associate common protocols with assigned ports.
- Understand the OSI model.
- Capturing packets with wireshark.

Fundamentals

- Network Protocols
    - http
    - ftp
    - pap (authentication)
        - Two-way handshake
        - Accept / Reject
    - smb (windows)
    - netbios

- Clients and Servers exchange binary data.
- Network Packets
  - header (96 bits)
  - payload (660 bits)
  - trailer (32 bits)
- Common Ports
  - PORT 80 **HTTP**
  - PORT 443 **HTTPS**
  - PORT 21 **FTP**
  - PORT 22 **SSH**
  - PORT 25 **SMTP**
  - PORT 53 **DNS**




Application payload
PDU
Layer 4:
Application layer
Source port
Destination port
❶
TCP header
TCP payload
PDU
Layer 3:
Session layer
Source address
Destination address
❷
IP header
IP payload
PDU
Layer 2:
Internet layer
Source address
Destination address
❸
Ethernet header
Ethernet payload
Protocol data unit (PDU)
Footer
Layer 1:
Link layer

OSI Model

Type	Layer	Protocol Data Unit	Function
Host	**7** Application	**User Data:** HTTP, FTP, IRC, SSH, DNS, SQL	High-level **APIs**, including resource sharing, remote file access
Host	**6** Presentation	**Syntax Data:** SSL, SSH, IMAP, FTP,MPEG, JPEG	Translation of **data between a networking service and an application**; including character encoding, data **compression** and **encryption/decryption**.
Host	**5** Session	**Port Data:** APIs, Sockets, Winsock	Managing communication **sessions**, i.e., continuous exchange of information in the form of multiple back-and-forth **transmissions between two nodes**.
Host	**4** Transport	**End to End:** Segment, Datagram, TCP, UDP	Reliable **transmission of data segments** between points on a network, including **segmentation**, **acknowledgement** and **multiplexing**.
Media	**3** Network	**Packet Data:** IPv4, IPv6, ICMP, IPSSec, IGMP	Structuring and managing a multi-node network, including **addressing**, **routing** and **traffic control**.
Media	**2** Data Link	**Frame Data:** Ethernet, PPP, Switch, Bridge, MAC	Reliable transmission of **data frames** between two nodes connected by a physical layer.
Media	**1** Physical Link	**Physical Structure Data:** Bit, Symbol, Coax, Fiber, Wireless, Hubs, Repeaters	Transmission and reception of **raw bit streams** over a **physical medium**.

Wireshark

- Filter method examples:
  - `http.request.method=="GET"`
  - `http.request.method=="POST"`

Bootcamp PPT#23

Session 8.3 Networking Fundamentals III

Tuesday October 27, 2020 / 6:30-9:30 PM
Zoom Link: https://zoom.us/j/2246200754
Zoom Password: 606132

Expectations

- Better understanding of Layers 2, 3, 4.
- Understanding ARP activity.
- Using `ping` and `fping`
- Using `traceroute`
- Understanding TCP and UDP.
- Anakyze TCP traffic with Wireshark.
- Analyze SYN scans.

Methods

- Enumeration Methods
  - physical addresses
- Media Access Control
  - physical machine address
- **Layer 2** (Data Link)
  - ARP Request & Reply
  - ARP Cache Timeout
    - dynamic addresses
- **Wireshark**
  - ARP Filter
    - Check Ethernet and ARP details.
    - **Request:** `arp.opcode  == 1`
    - **Reply:** `arp.opcode  == 2`
  - TCP Handshake
    - True = `1` , False = `0`
    - `tcp.flags.syn == <#>`
    - `tcp.flags.ack == <#>`
- `ping`
  - Packet inter-network groper.
  - Internet Control Message Protocol (IMCP)
  - Count: `-c`
- `fping`
  - Count: `-c`
  - Generate a target list from a supplied IP netmask: `-g`
- `traceroute`
  - Used ICMP and Time to Live (TTL)
  - TTL is an indicator of how long a packet lasts.

LAN, MAN, WAN

- A **LAN** (local area network) is a group of computers and network devices connected together, usually within the same building. By definition, the connections must be high speed and relatively inexpensive (e.g., token ring or Ethernet).
- A **MAN** (metropolitan area network) is a larger network that usually spans several buildings in the same city or town.
- A **WAN** (wide area network), in comparison to a MAN, is not restricted to a geographical location, although it might be confined within the bounds of a state or country. A WAN connects several LANs, and may be limited to an enterprise (a corporation or an organization) or accessible to the public. The technology is high speed and relatively expensive. The Internet is an example of a worldwide public WAN.

What is Transmission Control Protocol (TCP)?

- **TCP works on network layer 4 of the Open Systems Interconnection model**.
- **TCP handshake:**
  - **Setup:** SYN, SYNACK, ACK, Data
  - **Termination:** FIN, ACK, FIN, ACK
- Connection-oriented protocol that computers use to communicate over the internet.
- It is one of the main protocols in TCP/IP networks.
- TCP provides error-checking and guarantees delivery of data and that packets will be delivered in the order they were sent.

What is User Datagram Protocol (UDP)?

- **UDP works on network layer 4 of the Open Systems Interconnection model**.
- Connectionless protocol that works just like TCP but assumes that error-checking and recovery services are not required.
- UDP continuously sends datagrams to the recipient whether they receive them or not.

What’s the difference?

- TCP and UDP have many differences and similarities.
- They are the most commonly used protocols for sending packets over the internet.
- They both work on the transport layer of the TCP/IP protocol stack and both use the IP protocol.

TCP is best suited to be used for applications that require **high reliability** where **timing is less of a concern**.

- World Wide Web (HTTP, HTTPS)
- Secure Shell (SSH)
- File Transfer Protocol (FTP)
- Email (SMTP, IMAP/POP)

UDP is best suited for applications that require **speed and efficiency**.

- VPN tunneling
- Streaming videos
- Online games
- Live broadcasts
- Domain Name System (DNS)
- Voice over Internet Protocol (VoIP)
- Trivial File Transfer Protocol (TFTP)

Address Resolution Protocol (ARP)

- Procedure for mapping a dynamic Internet Protocol address to a permanent physical machine address in a local area network.
- The physical machine address is also known as a Media Access Control.
- The job of the ARP is essentially to translate 32-bit addresses to 48-bit addresses and vice-versa.
- This is necessary because in IP Version 4 (IPv4), the most common level of Internet Protocol use today, an IP address is 32-bits long, but MAC addresses are 48-bits long.
- **ARP works between network layers 2 and 3 of the Open Systems Interconnection model**. The MAC address exists on layer 2 of the OSI model, the data link layer, while the IP address exists on layer 3, the network layer.
- ARP can also be used for IP over other LAN technologies, such as token ring, fiber distributed data interface (FDDI) and IP over ATM.
- In IPv6, which uses 128-bit addresses, ARP has been replaced by the Neighbor Discovery protocol.

How ARP works

- When a new computer joins a LAN, it is assigned a unique IP address to use for identification and communication. When an incoming packet destined for a host machine on a particular LAN arrives at a gateway, the gateway asks the ARP program to find a MAC address that matches the IP address. A table called the ARP cache maintains a record of each IP address and its corresponding MAC address.
- All operating systems in an IPv4 Ethenet network keep an ARP cache. Every time a host requests a MAC address in order to send a packet to another host in the LAN, it checks its ARP cache to see if the IP to MAC address translation already exists. If it does, then a new ARP request is unnecessary. If the translation does not already exist, then the request for network addresses is sent and ARP is performed.
- ARP broadcasts a request packet to all the machines on the LAN and asks if any of the machines know they are using that particular IP address. When a machine recognizes the IP address as its own, it sends a reply so ARP can update the cache for future reference and proceed with the communication.
- Host machines that don't know their own IP address can use the Reverse ARP (RARP) protocol for discovery.

- An ARP cache size is limited and is periodically cleansed of all entries to free up space; in fact, addresses tend to stay in the cache for only a few minutes. Frequent updates allow other devices in the network to see when a physical host changes their requested IP address. In the cleaning process, unused entries are deleted as well as any unsuccessful attempts to communicate with computers that are not currently powered on.

DNS Spoofing

- Domain Name Server (DNS) spoofing (a.k.a. DNS cache poisoning) is an attack in which altered DNS records are used to redirect online traffic to a fraudulent website that resembles its intended destination.

DNS cache poisoning example

The following example illustrates a DNS cache poisoning attack, in which an attacker (IP 192.168.3.300) intercepts a communication channel between a client (IP 192.168.1.100) and a server computer belonging to the website **estores.com** (IP 192.168.2.200).

In this scenario, a tool (e.g., arpspoof) is used to dupe the client into thinking that the server IP is 192.168.3.300. At the same time, the server is made to think that the client's IP is also 192.168.3.300.

Such a scenario would proceed as follows:

1. The attacker uses arpspoof to issue the command: arpspoof 192.168.1.100 192.168.2.200. This modifies the MAC addresses in the server's ARP table, causing it to think that the attacker's computer belongs to the client.
2. The attacker once again uses arpspoof to issue the command: arpspoof 192.168.2.200 192.168.1.100, which tells the client that the perpetrator's computer is the server.
3. The attacker issues the Linux command: echo 1> /proc/sys/net/ipv4/ip_forward. As a result, IP packets sent between the client and server are forwarded to the perpetrator's computer.
4. The host file, 192.168.3.300 estores.com is created on the attacker's local computer, which maps the website **estores.com** to their local IP.
5. The perpetrator sets up a web server on the local computer's IP and creates a fake website made to resemble **estores.com**.
6. Finally, a tool (e.g., dnsspoof) is used to direct all DNS requests to the perpetrator's local host file. The fake website is displayed to users as a result and, only by interacting with the site, malware is installed on their computers.