Cyber Defense Recap

Module 17

Module 17 Agenda

- School Spirit
- Recap of each topic covered
- Jeoparty!

Do You Have School Spirit?!

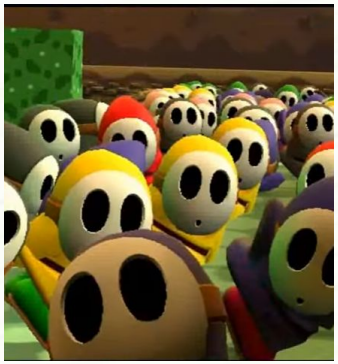
Let's get creative!

- Come up with a team name for your school. Otherwise your default name is simply your school number.
- As a school, create an emblem or logo to represent your team during the cyber defense competition.
- You may use any appropriate logo/emblem that is not directly affiliated with any company/organization.
- Use of graphic design or photo editing software is encouraged. Submit before cyber defense competition.

Do You Have School Spirit?!

Some cheesy examples to inspire you…

The Peacekeepers



Shy Squad

You will be able to use these team names and logos when your register your team into IScorE

Topics Covered

- IT Environments
- Virtual Machines
- Internet
- Passwords
- File Permissions
- Network Tools
- DNS and Packages
- Email
- Firewall
- 7 Layer of Cyber Security
- Vulnerabilities/Malware
- Scanning
- Physical Security
- Social Engineering
- Auditing
- Remediation

IT Environments

IT Environments:

- Communities of technology that have a purpose whether personal, home, business, or school use.
- The components includes…
  - Computers, Server, Applications/Web Apps, Connectivity (WiFi, Cellular, Wired Ethernet), and Security Measures (firewalls, intrusion detection systems)
- ISEAGE is the protected IT Environment used for the Cyber Defence Venue

Virtual Machines

VMs:

- VMs is a cloud like computer that run on top of a computer through the Internet (your team machines in ISEAGE).
- The four components of a computer are…
  - user: who operated the computer
  - applications: installed on computer (word, email, web browser, etc)
  - operating system: controls of interaction with computer (Linux, Windows, Mac OS X)
  - hardware: Physical components (hard drive, mouse, monitor, keyboard, etc.)

Internet

Internet:

- The internet is a collection of computer interconnected by networks.
- Internet Service Providers (ISPs) are the "back of the Internet"
  - ISPs manage networks
- Each computer has an Internet Protocol (IP) Address.
  - Composed of two parts: network and host

    Ex/ 253.782.2.15

Passwords

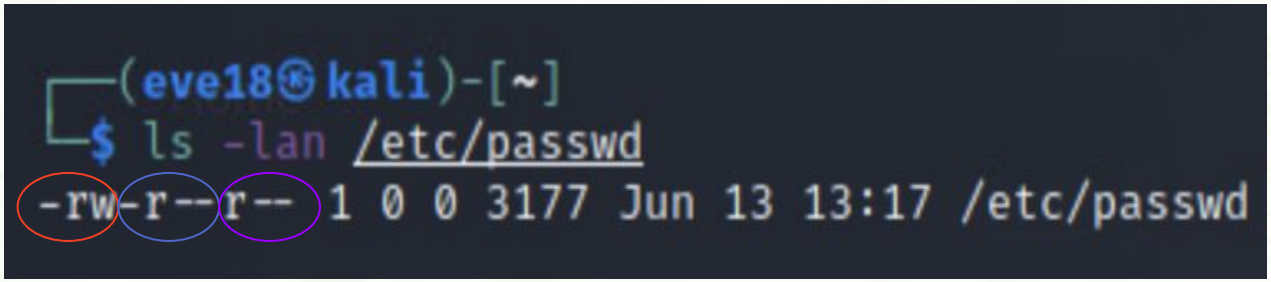
Passwords:

- Way of authorization to prove identity to login into computers, phones, emails, school accounts, bank accounts, and websites.
- Stored as hash values :
  - Hash functions convert passwords into encrypted code called hash values
  - Hash values are stored in password files
- It is crucial to create strong passwords to protect your data.

File Permissions

File Permissions:

- The set of rules accessed to files; Controls who has permissions to read, edit, or run files.
- Can view permissions **ls-lan <filepath>** command.
  - r: read, w: write, x: execute



First 3: User permissions Second 3: Group permissions Last 3: World permissions

File Permissions

File Permissions Cont.:

- Edit permissions using **chmod <###> <filename>** command.
  - read [r]: 4, write [w]: 2, execute[x]: 1
  - First # is the user, then group, then world permissions.
  - Ex/ **chmod 757 file2** changes the user permissions to xrw, group permissions to xr-, and world permissions to xrw.

1+2+4=7 1+4=5, 1+2+4=7

Network Tools

Network Tools:

- **ping**: sends echo-request packets to network hosts
- **dig**: names domain name to IP addresses
- **whois**: returns information about a domain
- **traceroute**: trace the network packet path
- **netstat**: helps figure what ports/servers are open on a machine
- etc.

DNS

DNS:

- The telephone directory of the web.
- A domain name server converts domain names (www.google.com) to IP addresses.
- Composed of the…
  - Resolving name servers: Internet provider, first phase, searches its list (cache) for the IP addresses.
  - Root name servers: Second step. Stores top level domains (.com, .edu,.gov). Guides the DNS to where the TLD server is located.
  - Authoritative name servers: Leads to the domain name provider and stores the full IP addresses

Packages

Packages:

- Small programs that helps manage other computer programs.
- Helps install, remove, and update softwares within our machines.
- “apt” commands
  - **apt install <package>**
  - **apt remove <package>**
  - **apt update**
  - **apt search**
  - **apt show <package>,** Etc**.**

Email

Email:

- The Email system is composed of
  - Message Transfer Agent (MTA): Stores and transports messages
    - communicate with other MTAs through the Simpler Mail Transfer Protocol (SMTP)
  - User Agent (UA): supports user interactions between the user and MTAs (read, write,send, and manage emails)
    - Private/application based: outlook, thunderbird, iMail
    - Web based: Gmail, AOL, Hotmail, Yahoo!

Firewall

Firewall:

- Softwares that are used to protect computer systems for hackers outside of the network.
- Can be seen as a filter that weeds out suspicious addresses from entering a computers systems network.

7 Layers of Cyber Security

7 Layers of Cyber Security:

- Mission Critical Assets: the computer system/data being protected
- Data Security: backups and authorization encryption
- Application Security: adding, testing, updating applications to avoid vulnerabilities
- Endpoint Security: use of antivirus software, web content filtering, application control

7 Layers of Cyber Security

7 Layers of Cyber Security:

- Network Security: configuring user permissions within network
- Perimeter Security: preventing suspicious being from entering network by using firewalls, anti-virus softwares, and data encryption
- Human Layer: being aware of human threats like spamming, phishing, and social engineering

Vulnerabilities/Malware

Vulnerabilities/Malware:

- Vulnerabilities are potential entry points for hackers and malware
  - Malware: files/programs that aim to deceive, manipulate or spy on targets
- Types of vulnerabilities include:
  - Design Vulnerabilities
  - Implementation Vulnerabilities
  - Configuration Vulnerabilities
  - Web Vulnerabilities

Scanning

Scanning:

- Tool used to by both hackers and companies to find devices, entry points, and weaknesses within a network.

- Broken down into…
  - Network/Host Scanning
  - Port Scanning
  - Vulnerability Scanning

Physical Security

Physical Security:

- The physical measures used to protect an organization' assets
  - Easy to forget, but it is necessary to secure the physical location of our computer system
  - Examples:
    - Doors
    - Gates
    - Locks
    - Codes
    - Badges
    - Senors

Physical Security

Social Engineering:

- The act of manipulating important people to try and gain access.
  - Examples:
    - Baiting
    - Phishing
    - Whaling
    - WiFi Phishing
    - SMSising
    - QR Code
    - TinyURL

Auditing and Remediation

Auditing:

- IT/cyber security auditing is the examination of a computer system to make sure everything is clean and up to date.

Remediation:

- Remediation is the process of stopping and treating a data breach.

Questions?

Contact IT-Adventures support staff!

email:
ita@iastate.edu