GenCyber Cybersecurity Workshop

Network and Server Security, Ethical Hacking

Presented by

Andrew T. Garrity

Associate Database Administrator

Information Technology

Star Wars "Air Gap"

- Script writer Rian Johnson never connected his MacBook Air laptop computer to a LAN or network, never used it for email or online searching.

When he was not using the laptop, it was locked in a safe at the studio.

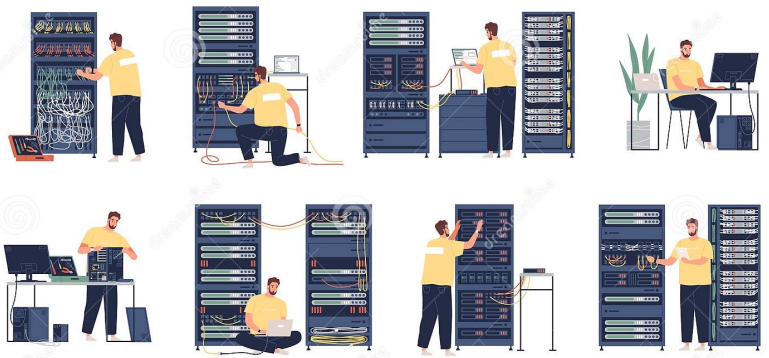
CompTIA Security+

- CompTia Security+ guidelines define three network security areas:
- **Network Security Appliances and Technologies.**
- **Cloud and Virtualization Security**
- **Wireless Network Security.**

Software

Some Departmental server software includes:

- **Accufund accounting system** for accounts payable and receivables
- **Student medical and immunization system** called Medicat for telehealth and mobile health system for touchless student check-ins. Medicat, going forward will include COVID screening app
- **Counseling Center** – teletherapy scheduling system
- **Burchfield Penney Art Center** point of sales CounterPoint system for the café and general store
- **Visix digital signage software** that integrates with our alerting system upon campus issues



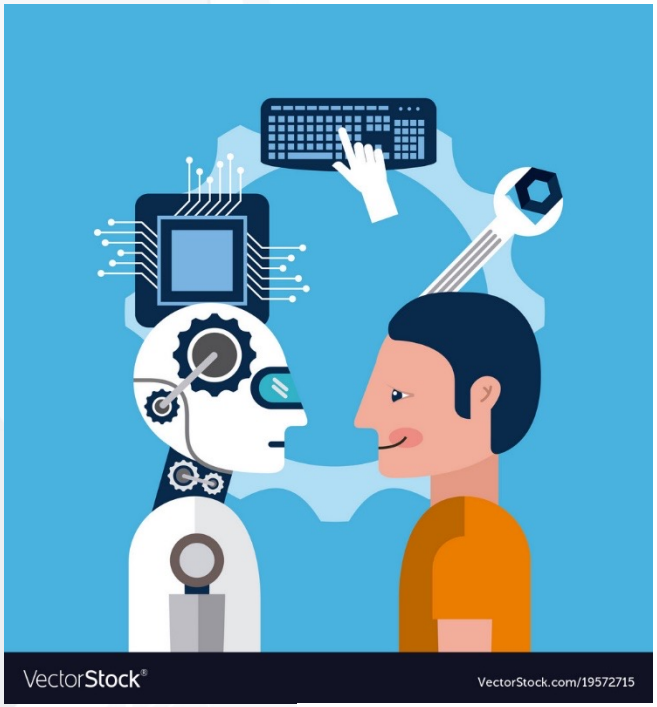
Levels of Security

Levels of security

- **Network level** - we have in place to safeguard around the perimeter of our network
- **VM Host level** - make sure our virtual hosts that houses our servers are secure
- **Server level** - make sure the OS is fully patched with firewall and antivirus enabled
- **Client level** - make sure the Windows client OS is fully patched with firewall and antivirus enabled
- **Database Security** – protecting and encrypting important data.
- **Application level on the servers** - make sure the updates are installed from the vendors of the products including Outlook email
- **Application level on the clients** - make sure updates are installed including Microsoft Office suite.

Cylance Smart Antivirus Protection Technology

- **Cylance –** uses artificial intelligence (AI) based solutions that predict and prevent execution of advanced threats and malware at the endpoint.
- It provides a solution that is proven able to block emerging threats on average 25 months before they are first detected.
- Cylance uses AI approach – predicting and protecting against known and unknown malware and attacks.



https://www.cylance.com/en-us/why-cylance.html

Firewalls

- A computer firewall is designed to limit the spread of malware.
- A firewall uses bidirectional inspection to examine both incoming and outgoing network packets.
- Firewalls allow approved packets to pass through, but takes different actions when suspicious packets come through, based on *rules*.

Firewalls

- Specific examples of rules could be:
- "Allow traffic from 183.36.0.0/24 to port 22."

Firewalls can also apply content/URL filtering. The firewall can monitor websites accessed through HTTP to create custom filtering profiles.

Firewalls

- Hardware-based firewalls – specialized separate devices that inspect network traffic.
- Web-application firewalls – monitor HTTP connections.
- Virtual firewalls – are cloud-based and designed for public cloud environments.

Deception Instruments

- **Deception instruments** seek to direct threat actors away from valuable assets to something that has little value.

- Threat actors can be tricked into thinking that they have been successful and have something of value when they do not.

Honeypots and Sinkholes

- A **honeypot** is a server located in an area of limited security that serves as bait to threat actors.
-
- Deflect – direct attention away from legitimate servers.

- Discover – expose the techniques the threat actors are using. Security personnel can then determine if a production server could thwart a similar attack.

Sinkholes

- **Sinkholes** are software-based programs that steer traffic away from its intended destination to another device.

- **DNS sinkholes** are commonly used to thwart DDoS attacks.

Honeypots

- In one study 10 honeypots around the world were created to simulate the Secure Shell service SSH service. One honeypot started receiving login attempts just 52 seconds after it went online. After all 10 honey pots were discovered, a login attempt was made one each one every 15 seconds.

- After 1 month, over 5 million attacks had been attempted on the honeypots.

Cloud Security Concerns

Unauthorized access to data	Improper cloud configurations can leave data exposed.
Lack of Visibility	Organizations have no way to verify the security measures being taken
Insecure Application Programming Interfaces (API)	APIs can lead to system vulnerabilities.
Compliance Regulations	Organizations that have to know where its data is who can access it, and how it is protected will struggle with the lack of transparency.

Virtualization

- **Virtualization is** installing a hypervisor on server hardware and then creating Operating Systems on top of the hypervisor.

- A hypervisor can also be created atop a base Operating System in stall, with multiple OS installations on top of the type 2 hypervisor.

Hypervisor Security concerns

- If a hypervisor is compromised multiple virtual servers are at risk.
- Traditional security tools such as firewall and anti-virus software must be specifically written or configured for VM environments.
- VMs may be able to “escape” from the container environment and interact directly with the hardware.

Wireless Attacks

- Bluetooth Attacks
- Bluetooth is a Personal Area Network.

- **Bluejacking** – sending unsolicited messages to Bluetooth devices.

- **Bluesnarfing** - an attack that accesses unauthorized information from a wireless device through a Bluetooth connection.

RFID Attacks

RFID ATTACK TYPE	DESCRIPTION of ATTACK
Unauthorized tag access	A rogue RFID reader can determine the inventory on a store shelf to track the sales of specific items.
Fake Tags	Authentic RFID tags are replaced with fake tags that contain fictitious data about products that are not in inventory.
Eavesdropping	Unauthorized users could listen in on communications between RFID tags and readers.

Case Study

- Dennis Moran was 17 when he hacked into D.A.R.E, RSA Security and military bases' websites. He defaced several web pages and left his hacker name "Coolio" on several web pages.

- When he was 18 he was convicted in court, sentenced to 9-12 months in jail and ordered to pay $5,000 to three different victims.

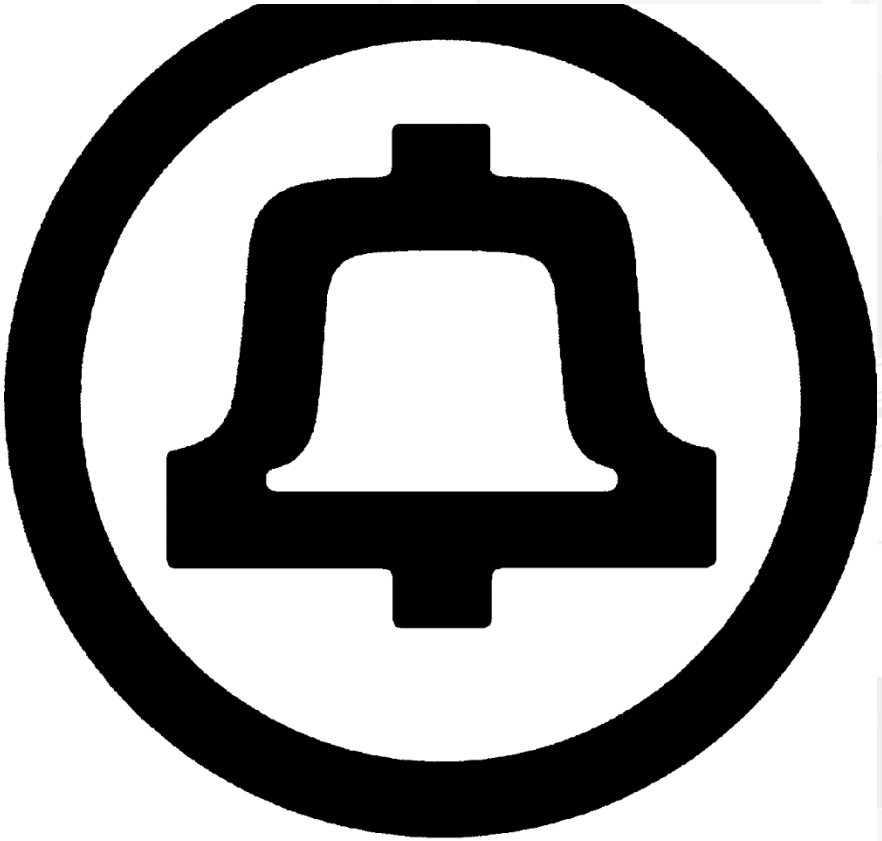
Case Studies

- Robert Morris, jr. was attending MIT when he created a worm that got out of control during the testing phase. This exploit caused damages in the tens of thousands.

- He was sentence to 3 years probation, 400 hours of community service and a fine of $10,050.

Questions

- Should someone under the age of 18 be able to serve prison time for a cyber-crime? Why or why not?
- • Should teenagers be tried as adults and serve prison time even if they were 17 when they committed the crime? Why or why not?
- • Was Moran's punishment fair, or should it have been more or less harsh?
- • Should Morris have been convicted for affecting systems he did not purposely infect? Why or why not?
- • Morris's worm caused more damage than Moran affected websites; should Morris have received prison time like Moran received? Why or why not?



The Bell Telephone Company

Hackers

The phone company had “hackers” working for them, appropriating computer languages and mainframe computers to create new technology.

The phone company also had “hackers” outside the company that were using technology such ”tone generators” to make free phone calls, and were intent on learning how the phone system worked.

UNIX and the B Programming Language

- In 1969 the first version of the operating system **UNIX** is released. UNIX is a multi-tasking, multi-user operating system developed by Ken Thompson, Dennis Ritchie, Brian Kernighan, Douglas McIlroy, Michael Lesk and Joe Ossanna, while they were working for AT&T laboratories. Ken Thompson created a programming language called "B" named after Bell laboratories or his wife Bonnie. The B language was based on an even earlier language called BCPL (**B**asic **C**ombined **P**rogramming **L**anguage).

Phone Phreaks and Hackers

- Outside of the Bell phone company existed a group of technology enthusiasts that would come to be known as “Phone Phreaks” or “Hackers.” John Draper known as “Captain Crunch” was the most famous Phone Phreaker.
- The original meaning of the word “hacker” was someone who liked to take things apart, find out how they worked, improve them or modify them to their own needs.
- People began exploring the Bell telephone network because it was the most complex system in existence at the time.

Hacking

- Phone phreaking would also attract the attention of Steve Jobs and Steve Wozniak who would later go on to form Apple computer.

Certified Ethical Hacker

- Certified ethical hackers look for weaknesses and vulnerabilities in computer systems.

- They used to be called “white hat” hackers, a nod to old Western movies where the good guy would wear a white hat and the villain would wear a black hat.

Vulnerability Assessment and “pen” or Penetration Testing:

Log reviews

Test or “synthetic” transactions to the the system, especially security.

Software vulnerability assessment – code review

Misuse case testing.

- Test case assessment
- Risk, Threat and Vulnerability Assessment

Certified Ethical Hacker

- **NVD – National Vulnerability Database.** Security measurement and compliance.

- **CVE – Common Vulnerabilities** and Exposure database.

Automated, passive testing of security controls.

Identify vulnerabilities, lapses in security controls and identify system misconfigurations.

Explicit Emails

Explicit emails use information bought cheaply on the dark web to send out emails with explicit user details, such as old passwords.

This really gets the attention of the person who received the email since passwords are often re-used on different sites or changed only slightly.

Threat Actors

- **Threat actor** – an individual or entity responsible for cyber incidents against the technology equipment of enterprises and users.

Cyber Attack Types

- **Physical impersonation** – dressing up like a security guard, janitor or other employee to gain entry to a site.
- **Zero Day attacks** – exploiting a vulnerability in computer code before it becomes known to the general IT community.

Cyber Attack types

SPIM – SPAM messages targeting Instant Message (IM) users.

Pharming – redirecting a web site's traffic to another website.

Phishing – asking for user credentials.

Social Engineering

- **Social engineering** is the deceptive methods that malicious individuals use to compromise computer systems using the inherent weaknesses of the system's operators.

- Cheaper
- Less Complicated
- Readily available
- Safer

Cyber Attack Types

Shoulder surfing – looking over someone's shoulder to get a password or pin.

Dumpster diving – looking through someone's trash for information.

Tailgating – gaining physical entry to a site by following an employee through a gate or a door.

Pretexting

- A malicious attacker will pretend to be someone else to gain access to sensitive data.
- A person will pretend to be from the Help Desk or someone in a position of higher authority using the phone, text, or email.
- Email Spoofing – email appears to be from a legitimate source.
- Pretexting takes advantage of a willingness to help and gullibility.

Pretexting

- Employees may be hesitant to challenge an individual out of fear of offending that person or being disrespectful.
- Tailgating or “piggybacking” can be mitigated using identity badges, access cards and biometrics.

Shoulder Surfing

A malicious person acquires sensitive data using a surveillance method.

Surveillance can range from peering over a person's shoulder, using hidden cameras, keystroke loggers or ATM skimmers.

The objective is to steal login credentials or credit/debit card details.

Shoulder surfing takes advantage of a sense of security and inattentiveness.

Dumpster Diving

A Malicious person looking through disposed items (like garbage) to find sensitive data that was not disposed of properly.

- ❑ Documents that were not properly shredded.
- ❑ Hardware devices that were not overwritten or “blanked out.”

Dumpster Diving

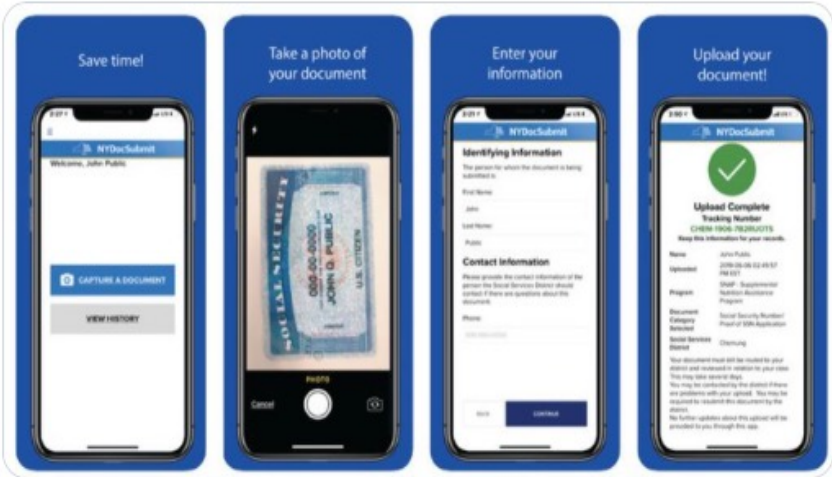
DUMPSTER DIVING TAKES ADVANTAGE OF A FALSE SENSE OF SECURITY AND NEGLIGENCE.

PEOPLE FIGURE NO ONE WILL TAKE THE TIME AND EFFORT TO GO THROUGH THE GARBAGE.

Dumpster Diving

There is new threat of “virtual” dumpster diving as government and businesses increasingly use e-forms to take the place of paper forms and manual submissions.

The @ECSocServices is pleased to announce the launch of Mobile Document Upload for Temporary Assistance, SNAP (food stamps), Medicaid, and HEAP clients. Clients can now photograph documents and submit them to ECDSS from their Apple or Android device. More: www2.erie.gov/socialservices...



Rogue Access Points

Access points are wireless connections to computer networks.

If a user sees a network such as “TellMyWiFiLoverHer” without the lock symbol signifying WEP, WPA, WPA2 wireless protocols, it may be a “rogue access point.”

Browsing history, user details and sensitive information can be intercepted using these bogus access points.

Phishing

Phishing – the act of acquiring sensitive data through electronic communications by pretending to be a credible source

Phishing

"Hackers commonly replace the letter *f* with *ph*, a nod to the original form of hacking known as phone phreaking. Phreaking was coined by John Draper, aka Captain Crunch, who created the infamous Blue Box that emitted audible tones for hacking telephone systems in the early 1970s."

Phishing

MOST PHISHING IS DONE USING EMAILS. IT IS RELATIVELY SIMPLE TO SPOOF A LEGITIMATE ORGANIZATION'S LOGO AND CREATE AN EMAIL ADDRESS THAT LOOKS CONVINCING.

GENERIC OR MISSING GREETING.

DECEPTIVE EMAIL ADDRESS.

REQUEST TO VERIFY ACCOUNT

SENSE OF URGENCY

ATTACHMENTS

STRANGE LOOKING LINKS

Phishing – things to look for

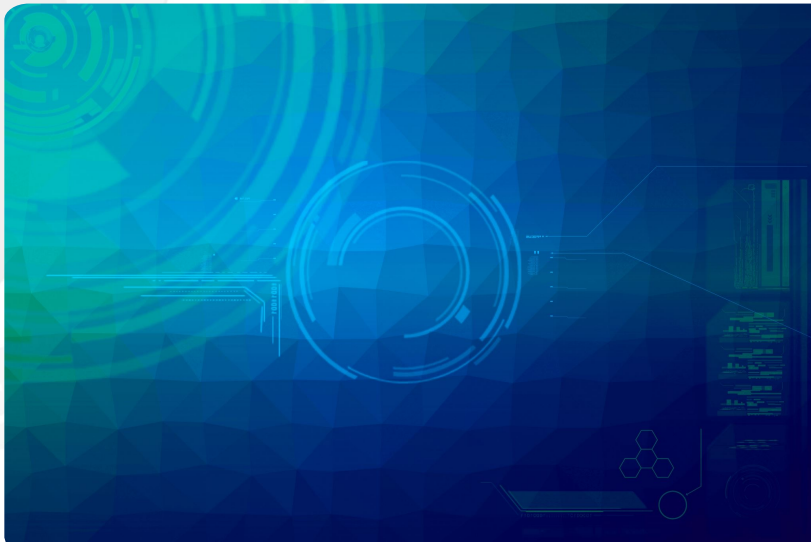
PRIZE OR AWARD NOTIFICATION

MISSPELLINGS, GRAMMAR MISTAKES OR ODD WORDING.

Phishing

Older users will often say "How can they know all of this information?"

While younger users will just assume that they don't in fact have any privacy in this digital age where there is so much information online.



Twitter

Phishing attempts often ask for payment in Bitcoin or other cryptocurrencies to avoid being tracked.

Spear Phishing

- Sending targeted
  recipients prete
  sted source.
  empts are
  contain
  makes
  timate

Recent Phishing Trends

- More personalization. Personal and company details are including in the subject and text of the emails.
- Multi-platform – phishing attacks are showing up in texts.
- HTTPS usage. Many malicious links are never using secure server URLs.
- BEC Business Email Campaigns.

Phishing – more complicated examples

Redirection using Local Host

Local Host – the default name of the computer. IP address 127.0.0.1

Using web server software and a fake web page along with a bit of PHP code, a user can be "redirected" to what appears to be a legitimate web site. The user is then prompted to enter their credentials which are sent to a text file.

Look at Windows Defender Firewall

- At the Windows start box type →

  Windows Defender Firewall

Is there a domain network, private, guest or public network?

What is the firewall state for inbound connections?

Create an .exe file

Using a compiler on Mac OS terminal or a Windows compiler create a simple "Hello World" program and try to mail that to classmates.

Try to create an Excel macro and email that to classmates. Or just try to email a regular Excel file.

Using Notepad create a text file, save it "all files" and give it a random three letter extension, such as "xyz". See if you can email it.

Zoom statistics

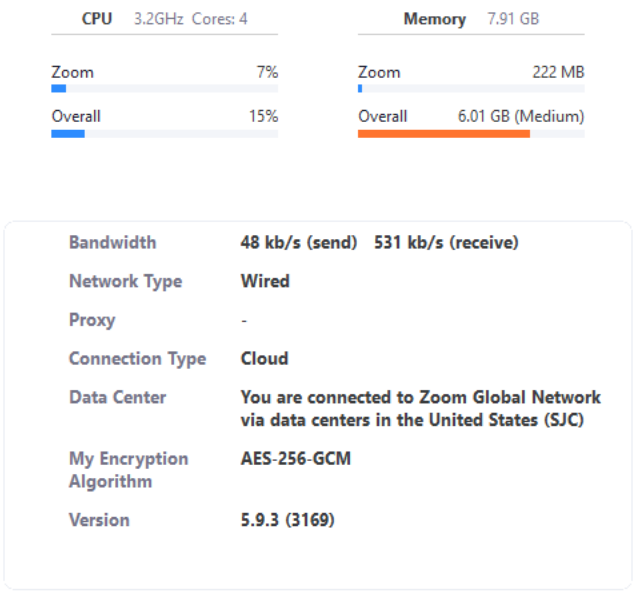
During a Zoom meeting , capture the statistics

Go to “meeting information” → “statistics”

What is the bandwith? What is the network type?

What is the connection type?

What is the encryption algorithm?



Duckduckgo

- Duckduckgo is a web browser that is supposed to be completely private. It doesn't **use filter bubbles, personalized search results** or show search results from **content farms**, if you use it as browser extension instead of just navigating to duckduckgo.com.

Sandboxing

- **Sandboxing** is creating an isolated environment where suspicious software is tested to see if and how it replicates, what happens to existing files, what new file, directories and executables are created and spread.

- **Sandboxing** in a classroom setting means setting up a temporary desktop environment that mimics a computer's operating system and hardware resources for training. Once the training is completed that particular instance is saved or destroyed.

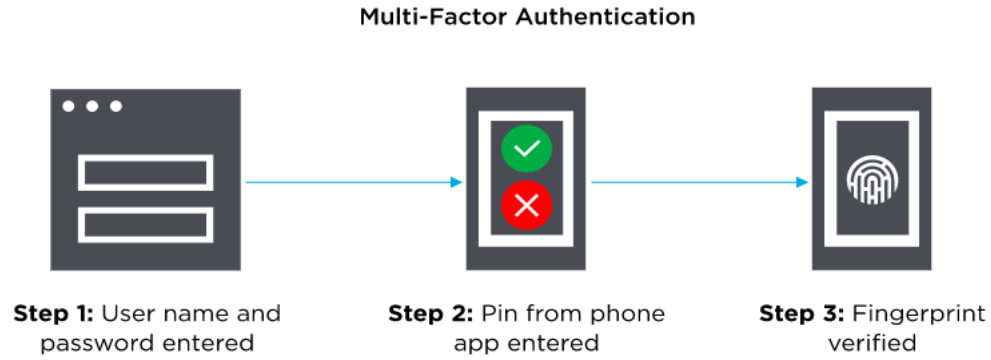
Phishing Simulators

- These allow you to create and send at least one phishing email to a real user.
- Many free and open-source options are available online, such as Infoseq IQ, Gophish and LUCY.

Retrieve “deleted” files.

- Create and delete a simple text file using a USB.
- Using Disk Drill app try to recover that file after it has been deleted. What happened?

Multifactor Authentication (MFA)



What is Multi-Factor Authentication (MFA)?

Multi-factor Authentication (MFA) is an authentication method that requires the user to provide two or more verification factors to gain access to a resource such as an application, online account, or a VPN. MFA is a core component of a strong identity and access management (IAM) policy. Rather than just asking for a username and password, MFA requires one or more additional verification factors, which decreases the likelihood of a successful cyber attack.

Multifactor Authentication (MFA) Importance

Why is MFA Important?

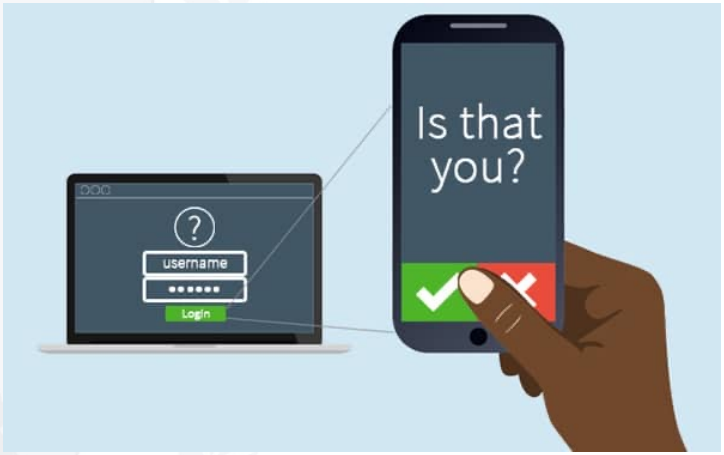
The main benefit of MFA is it will enhance your organization's security by requiring your users to identify themselves by more than a username and password. While important, usernames and passwords are vulnerable to brute force attacks and can be stolen by third parties. Enforcing the use of an MFA factor like a thumbprint or physical hardware key means increased confidence that your organization will stay safe from cyber criminals.

Multifactor Authentication (MFA) How does it work?

How Does MFA work?

MFA works by requiring additional verification information (factors). One of the most common MFA factors that users encounter are one-time passwords (OTP). OTPs are those 4-8 digit codes that you often receive via email, SMS or some sort of mobile app. With OTPs a new code is generated periodically or each time an authentication request is submitted. The code is generated based upon a seed value that is assigned to the user when they first register and some other factor which could simply be a counter that is incremented or a time value.

(show web outlook)



Multifactor Authentication (MFA)
3 Main Types

Three Main Types of MFA Authentication Methods

Most MFA authentication methodology is based on one of three types of additional information:

1) **Password or PIN** - Message or code sent via text or email
2) **ID badge or smartphone** - Answers to personal security questions
3) **Biometrics** - Fingerprints, facial recognition, voice, retina or iris scanning or other Biometrics

Examples of Multi-Factor Authentication include using a combination of these elements to authenticate

Multifactor Authentication (MFA) Differences

What's the Difference between MFA and Two-Factor Authentication (2FA)?

MFA is often used interchangeably with two-factor authentication (2FA). 2FA is basically a subset of MFA since 2FA restricts the number of factors that are required to only two factors, while MFA can be two or more.

Web references:
https://www.onelogin.com/learn/what-is-mfa

Fun Activities

Fun activities: Go to **Start** and type **cmd** in the search field to open the command prompt. Or go to *Start > Run type cmd or command*

netstat - The network statistics, is a Command Prompt command used to display very detailed information about how your computer is communicating with other computers or network devices

- Example: **netstat -a** command would give the extended result of ports opened on the server and established connections and their current state for both TCP and UDP connections.
- **netstat -an** command would only show the remote server IP addresses where netstat -a would try to resolve the name for that IP address. Thus netstat -an would be faster than the netstat -a

More fun activities

Fun activities:

- nslookup - used for querying the Domain Name System to obtain domain name or IP address mapping, or other DNS records. The name "nslookup" means "name server lookup".
- Example: nslookup google.com
- nslookup (your device name.com)

Even more fun activities

Fun activities:

- Ping- command used to troubleshoot connectivity, reachability, and name resolution.
- Example: ping google.com
- Ping (your device name)
- Ipconfig - Displays all current TCP/IPnetwork configuration values and refreshes Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) settings
- Example: ipconfig or ipconfig/all

Additional resources use for the classrooms

Cyber.org (need to get a Free account if you do not already have one) has some great resources including lesson plans and PowerPoints. Course material associated with Ethics is available in their Cyber Society course area:

https://cyber.instructure.com/courses/6

And more technical cybersecurity information including a lot of information about hacking is available in their Cybersecurity course area:

https://cyber.instructure.com/courses/100

Teach Cyber (need to get a Free account if you do not already have one) also has a great set of lessons in their Intro to the Challenge of Cybersecurity class (8 units):

https://teachcyber.org/cybersecurity-teaching-resources/lessons/intro-to-cybersecurity/

Contact Information

Andrew T. Garrity

garritat@buffalostate.edu

https://it.buffalostate.edu

https://gencyber.buffalostate.edu/

https://cs4hs.buffalostate.edu/

BUFFALO STATE COLLEGE 1871–2021

150

believe. inspire. achieve.

Questions/ Comments

THANK YOU!