Cybersecurity Club Minutes
4-12-22

5:30 meeting started

- Started with talking about paid research opportunities for undergraduates and working for the summer GenCyber program.
- Talked about cybersecurity in the news: There were cyberattacks targeting UPS backup power devices, the BlackCat ransomeware which is tied to the BlackMatter group, Microsoft obtaining a court order to take down domains targeting Ukraine, and SharkBot banking Trojan resurfacing in google play apps hidden behind antivirus apps

5:37 moved to talking about the resource Defend the Web

- Intro: Created accounts for defend the web
- Defend the Web is a similar resource to Over the Wire
- Completed Intro 1 level: ctrl u, look at source code for password
- Worked on the next levels of defend the web

6:00 meeting ended

Cyber Security Meeting 3-29-22

Meeting started at 5:30 pm

- Talked about cybersecurity in the news and how Hondas built between the years 2016-2020 are easily hackable. And it's not just Hondas either, it's a certain type of key fob that doesn't use encrypted signals for things like remote start.

5:40 pm played cybersecurity family feud
6:30 pm meeting ended

Cybersecurity Meeting 3-8-22

5:30 pm – meeting started and began with Cybersecurity in the news
- Dirty pipe: most severe linux vulnerability since 2016.
- Russia's Invasion kicks Senate into Cybersecurity Law Mode.

5:40 pm – moved into Web Scraping
- Data scraping is used for extracting data from websites.
- Can be done manually but most often done by a bot.
- Has several uses: web indexing, web mining, online price change monitoring, price comparison, product review scraping, research, and website change direction.
- You can scrape any website, however there are copyright laws you must follow.
- Showed an in person demo of web scraping

6:00 pm – meeting ended

Cybersecurity Club Minutes
3-1-22

5:30 pm meeting started

- Started with current news today: cyberattacks accompany Russian military assault on Ukraine, Moscow exchanged was downed by a cyberattack, anonymous attacked the Russian tv channels

5:33 pm moved to Network Configuration

- Introduction: is a process of assigning networks settings, policies, flows, and controls
- Network configuration deals with several things such as, maintaining a network, making configuration changes, relaunching devices, and track/report data
- Basic internet, the internet is made up of multiple networks that are communicated through protocols
    - Protocols define the format, order of messages sent and received between entities
- TCP and UDP are the most important protocols
- Protocols are essentially rules that describes how the software in a network will work
- Network security is essential to understand the data coming in and report possible data that is not supposed to be there.
- Road map, as a network admin there are several tasks that are involved.
- Network Topologies are different types of network configurations within the computer network. Describes how it is arranged.
- What makes up a network? Modem, router, firewall, switch, LAN cable/Patch Cable, access point, repeater, patch panel.
- Tools are a big asset in network configuration.
    - Wireshark, is an open-source network software that helps analyze network protocols that efficiently analyze network protocols and enhance security in real-time

6:00 pm meeting ended

Cybersecurity Club Minutes

2-22-22

5:30 pm Meeting Began
- Went over virtual machines, what they are and how to install them

5:35 pm Looked at specific Vms (Kali)
- Ran through basic commands
    - Whoami
    - /home/kali
    - Ls
    - Ls .l
    - Ls -a
    - Ls -r
    - Sudo nano .bashrc
    - Ls -t
    - Clear
    - Cd Documents/
    - Cat
    - History
    - History > history.txt
    - Nano history.txt

5:45 pm Creating a simple python script within the terminal and get it to run
- Writing it in the command line
- Using control S to save it
- Sudo apt install python3 for in case python is not updated or installed
- “Python3 sample.py” runs the program
- Can do that with other languages as well but with just different commands

5:50 pm Kali VM
- Has a lot of useful tools, especially in cybersecurity
- Man command
- Exit

6:00 pm Meeting ended

Cyber Security Club Minutes 2-8-22

5:30 PM Meeting was started

- Went over how NCAE Cybergames and how they split up the northeast competition
- May be moving the competition to next Feb 26
- Will be doing the world of bills sandbox
    - Watched the video
    - Launched the environment
    - Tried the sandbox

6:30 PM Meeting ended

1-25-22 cybersecurity meeting

5:30 pm started the meeting

- Went over the DoD Cyber Scholarship, how to apply, what you need, and what you will get out of it
- Went over the NCAE Cybergames and figuring out our team and who would like to compete
- Also watched videos from people who work for NCAE as well as past competitors on advice on how to prepare as well as what to do if you've never done them before.
- Then walked through one of the NCAE sandboxes given to users who hope to compete

6:00 pm ended the meeting

Cyber security meeting

10-12-21

5:30 pm: started the meeting and gave a quick brief current cybersecurity news

- Twitch was breached and 125GB files were posted
    - Was the first of several attacks
- Cyber security day is October 26th
    - Starts at 9 am

5:45 pm: dove into the topic of red team strategies

- Physical security
    - Red team physical penetration testers are hired to test the effectiveness of a company's security
    - One of the more important tactics keep computer systems secure
- What red team testers look for
    - Basics, attack, and a solution

6:00 pm: broke into two teams to do a red team vs blue team simulation

6:30 pm: meeting ended due to fire alarm

Red Team Strategies

GenCyber Summer 2021

Hackers: The Good, The Bad, and The Ugly

- When people typically think of “hackers” they typically think of what we call Black-Hat hackers
  - A hacker that breaks through computer security for their own gain, typically with malicious intent
  - Criminal / Illegal
- However, there are also legal, ethical hackers: Red Team hackers.
- Their job: legally hacking, either using physical or cyber means, into a company or building in order to expose the security weaknesses and help them get repaired.

Red Team vs Blue Team

RED TEAM

- Offense
- **Detect Weaknesses in a company's** security
- Penetration Testing
- Social Engineering/Phishing
- Physical Security Access

BLUE TEAM

- Defense
- Incident Response
- Maintaining the network
- Risk Assessment

Physical Security in Cyber Security

- One of the most important tactics in keeping a computer system secure is ensuring its physical security.
- Red Team physical penetration testers are hired to test the effectiveness and sustainability of a company's physical security
    - They hack into the building as well as the cyber systems and then report their findings to the company.
- Physically Protected Spaces keep a company's data and computer network secure

Physically Protected Space (PPS)

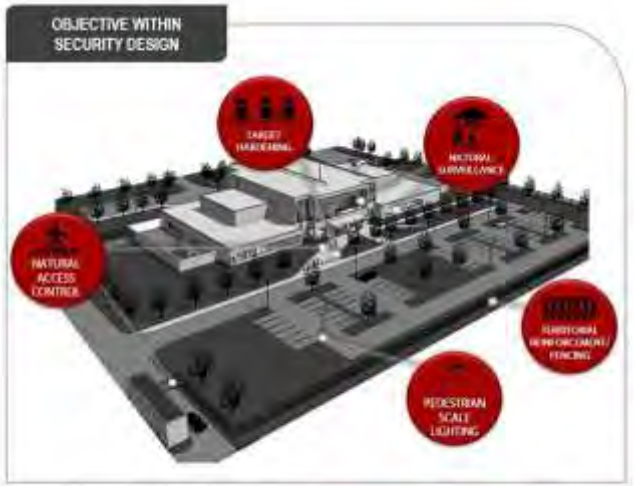
- An area that is guarded from those with malicious intent to access it
- Usually contains multiple layers of security
- Takes CPTED and applies it to a real life situation
- Example: the Google Data Center
  - Six Layers of Security
    - 1. Signs, Fences, road, etc.
    - 2. Smart Fencing, Guard patrols, cameras
    - 3. Building Access: Card access, Iris Scanning
    - 4. Security Operations Center: 24/7 Observation of Cameras, Scanners, etc.
    - 5. Data Center Floor: Massive server room with only as-needed access
    - 6. Disk Erasion Room: Room that destroys hard disks. Two-way locker system so that only few designated workers are allowed to erase the drives.

Google Cloud

For more info: https://www.youtube.com/watch?v=kd33UVZhnAA (6 min)

Crime Prevention Through Environmental Design (CPTED)

- Also known as Design Out Crime
- Multi-disciplinary approach to preventing crime
- Planning the layout of an environment with security in mind



CPTED Site Considerations

Image is property of Ross & Baruzzini

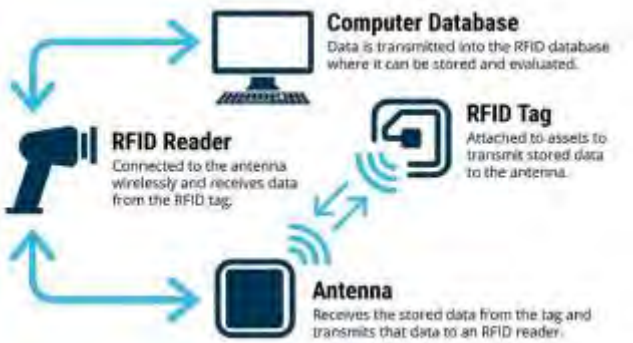
Four Principles of CPTED

1. Natural Surveillance
    a. Visibility
    b. Placement of both physical and social features
    c. Ex: windows, no blind corners, support desks, etc.
2. Natural Access Control
    a. Restricting and encouraging movement in different parts of the building
    b. Ex: clear and limited entrances, security checkpoints, etc.
3. Territorial Reinforcement
    a. Publicly distinguished security areas
    b. Ex: restricted areas, gates, security level access requirements, etc.
4. Maintenance
    a. Well maintained grounds to show that structure is well-kept and being used

What Red Team Physical Pen-Testers Look For...

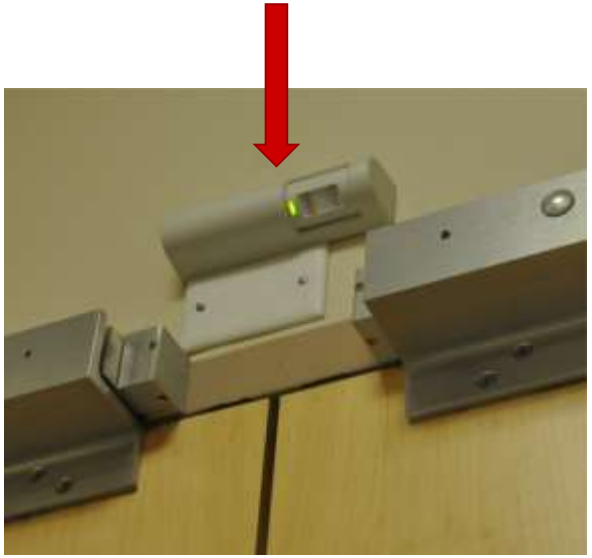
Common Security Components
RFID (Radio-Frequency Identification)

- Basics
  - RFID systems consist of a tag (RFID label), a reader, and an antenna
  - Often used for physical security components like door access/locks
- Attack
  - RFID tags can be cloned if an attacker can pick up and read signals from the card to reader
  - Once cloned, a hacker can recreate the RFID tag
- Solution
  - Use an RFID system with mutual authentication or stronger security measures (like Smart Card chips or Biometrics)



Common Security Components
REX (Request-to-Exit) Sensors

- Basics
  - Simple passive thermal sensors detect people exiting and unlock the door
  - Commonly used sensors do not detect heat change, but rather anything different in the area
- Attack
  - Blowing cloud of gas through door to trip sensor
- Solution
  - Dual-technology REX sensor
    - Uses both passive infrared and radar technology
  - The sensor will trip once a heat change AND human-sized object is detected



Designing Your Own Secure Building

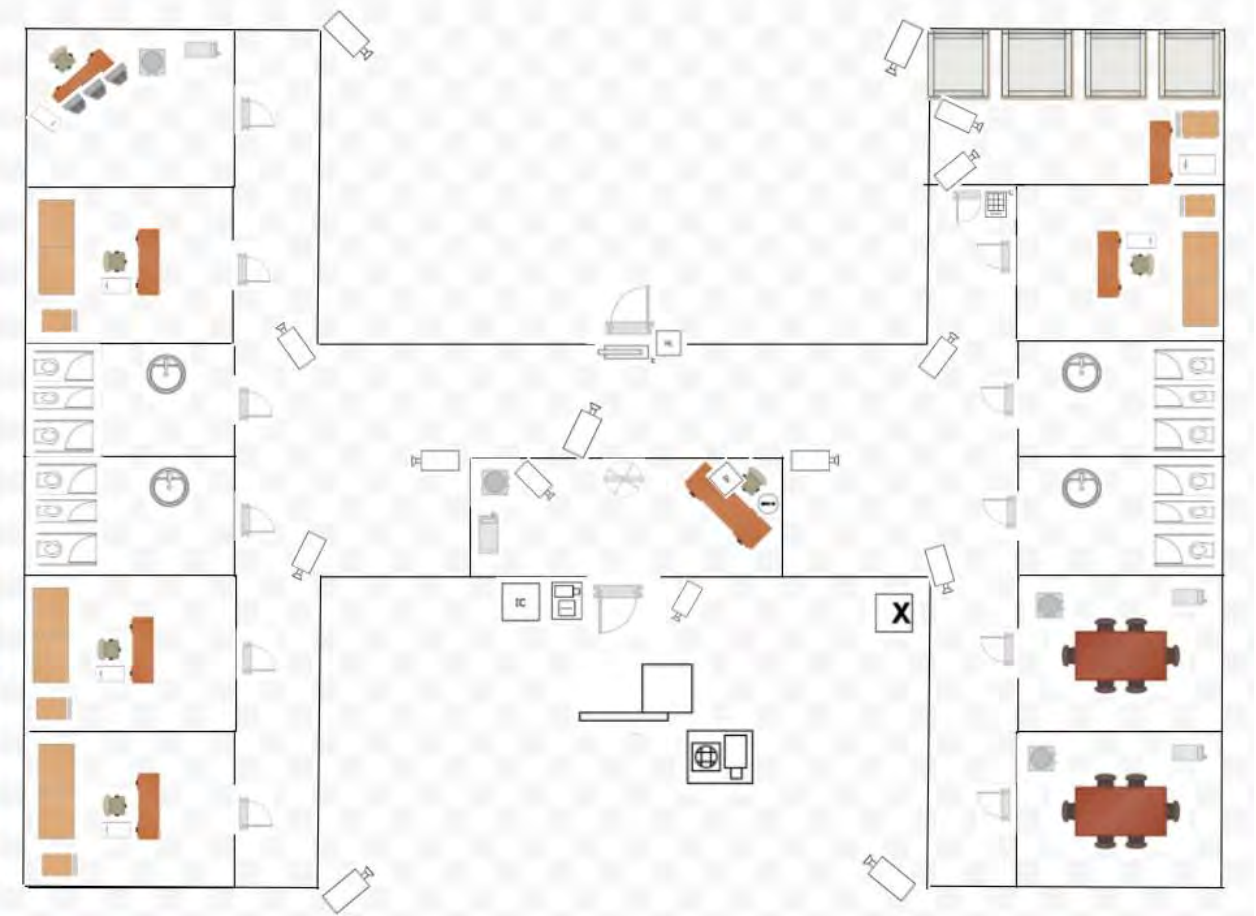
Instructions

- Use the link provided in your breakout room to enter Google Drawings
- As a team create a secure building based on the previous requirements
- Be prepared to have your final copy shared at the end
- If you would like to discuss or explain your floorplan there will be time for that as well

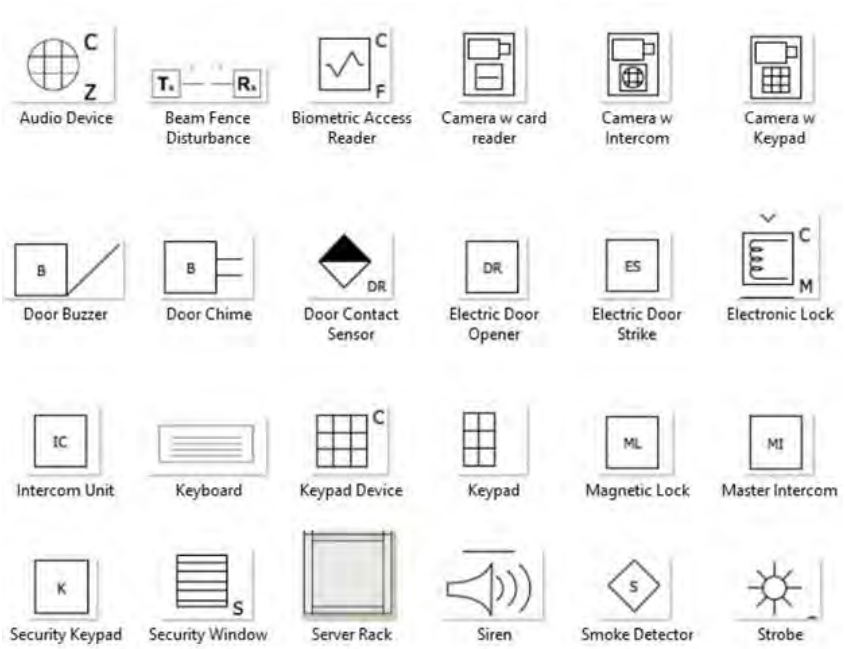
Requirements

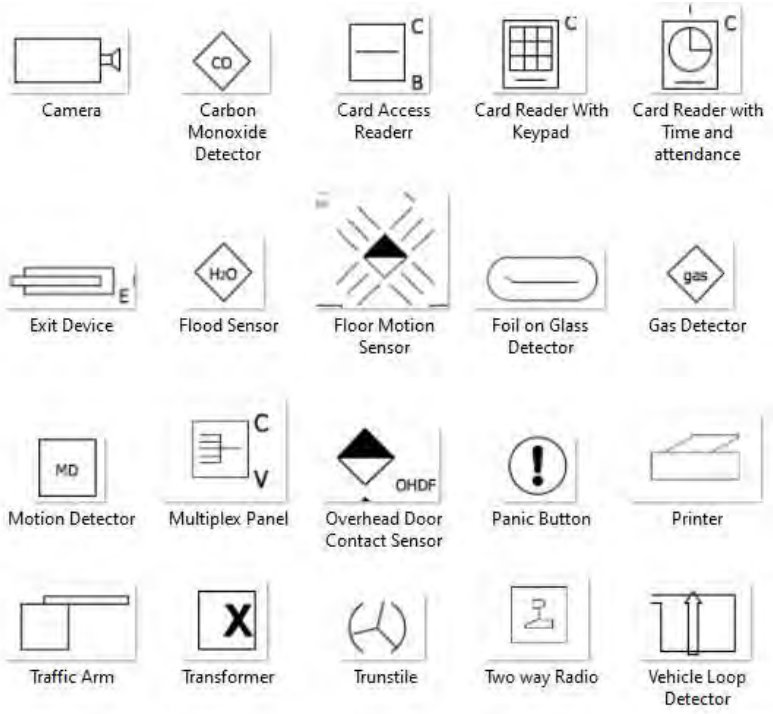
- Building must be in the shape of the letter H
- The building needs to have at least 6 rooms
- One room must be a secure server room
- One room must be the security guard office
- You may not have any empty rooms

EXAMPLE FLOOR PLAN



Example of Key





Tips

- Helpful symbols can be found in the Red Team Strategies folder
- The requirements for the activity can be found alongside the key in the file named “Required-Key”
- You are not limited to supplies given to you
- If you have an idea and would like to use items feel free to use your own!

Cyber security meeting

10-5-21

5:30 started the meeting and gave a quick brief about the topic of social engineering

- It is the use of deception to manipulate individuals into giving up information for fraudulent purposes
- Internal threats: example, July 2020 hacker gained access to 130 private and corporate twitter accounts
- How to categorize internal threats

5:45 Started the sock puppet activity trying to find the real identity of jack manser
6:30 Concluded the meeting

Social Engineering and Internal Threats

By Daniel Saylor

Based off research conducted and presented by Jayson Street

SOCIAL ENGINEERING 101

- *"The use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes."*
- The problem with social engineering is that it cannot be combatted by traditional security solutions
  - Technical Solutions already fail to catch some mass campaign attempts
  - Spear phishing is so unique/tailored it is hard to detect
  - Victims are often unaware they are being attacked

Internal Threats

- In July 2020, hackers gained access to 130 private and corporate twitter accounts with at least a million followers each.
  - Barack Obama, Elon Musk, Bill Gates,
- Posted a phishing tweet promoting a bitcoin scam
- Twitter admins were fooled into thinking the attacker was Twitter's own IT department and gave attackers access to administration tools
  - cost Twitter 4% of it's stock price and lost users nearly 300,000$ in bitcoin currency.

Categorizing Internal Threats

- Social engineering should not by itself be considered the only threat vector.
- Internal threats are the real problem in a social engineering attack
  - *The social engineering is going to occur and by itself cannot compromise security. Rather, an internal user must initiate the compromise on the attacker's behalf. Thus, we must also address internal threats.*
- *Types of internal threats:*
  - *Inadvertent*
    - *Just trying to do their job*
  - *Negligent*
    - *Carelessness/should've known better*
  - *Malicious*
    - *Intentionally trying to disrupt the business from the inside knowingly and willingly*

WHAT IS FAILING?

- Most employees do not care about your data
- Security staff become complacent in violating procedure over time
- On perimeter security for small/medium businesses often hinge on a front desk/receptionist
  - Average glass door requirements are *high school diploma and good communication skills*
- Employees not empowered to question the unusual
  - There is only one thing that is more dangerous then no security: ***a false sense of security***

Security Complacency

- Security Staff are Human beings
- Common security knowledge that humans dull with repetitiveness
  - A guard at the gate of a facility
- In 2019, 2 civilians breached an air force base
  - Only found when one told airmen she had been kidnapped.
- *"The vehicle did not stop to have their credentials checked [at the main gate]. The [security force] sentry failed to stop the vehicle or initiate gate runner procedures which allowed the vehicle to successfully breach the installation."*
- ***Protocols were not followed because the security staff did not have a respect for the protocols in place.***

SCENARIO

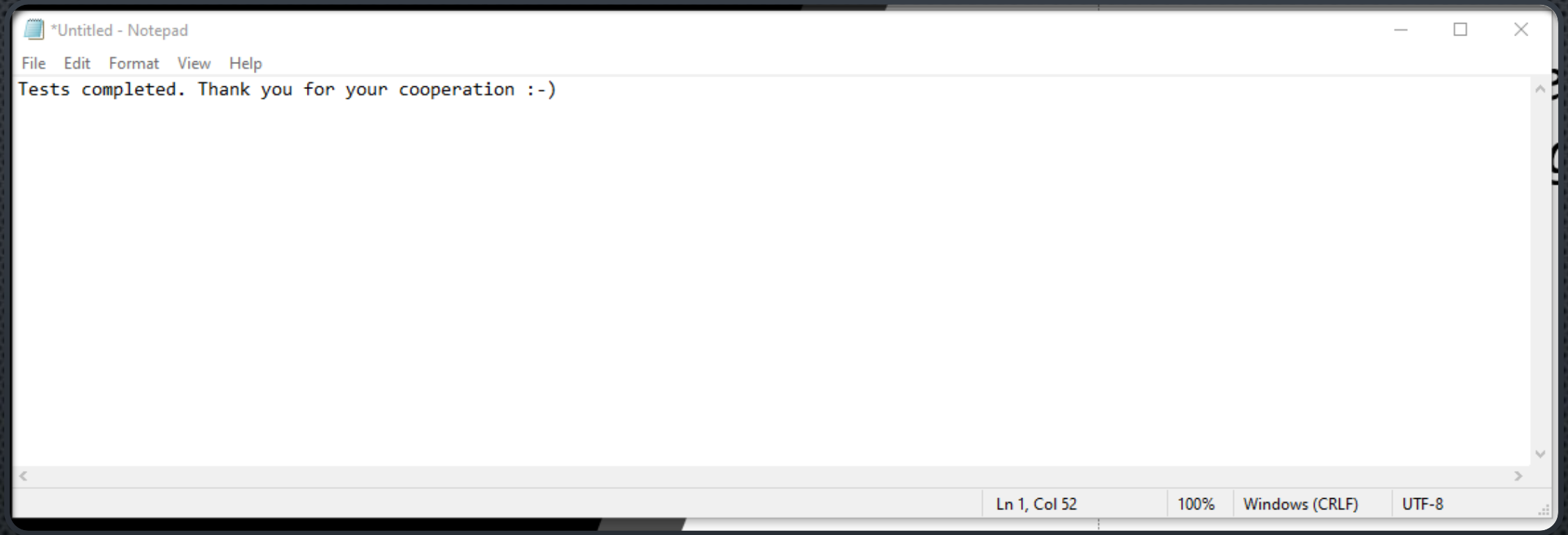
- *An individual approaches your cubical in a corporate building wearing a collared shirt. They claim to be from Regional IT. You have seen them walking around the office earlier in the day but do not recognize them. The office has a receptionist desk and badge-reader secured doors.*

SCENARIO

- *The individual notifies you that they are doing a permissions right's check to make sure your USB ports are not allowing cell-phones to be plugged into your computer.*

SCENARIO

- *The individual plugs in a USB into the port and multiple command prompts appear and disappear on the screen*



SCENARIO

A TEXT DOCUMENT OPENS ON THE DESKTOP:

Building internal resistance

- Lunch and learn
- teach employees how to protect their own data at home so they will protect yours
  - If someone practices something at home, they are far more likely to practice it at work
- Make it fun
  - "where's waldo" badge hunting.
- Re-enforce by trainings and protocols
  - implementation of trainings/protocols alone is generally ineffective, unproductive, and generally a waste of time and money.
  - Policy should describe punishment and procedure when a staff member leaks information

THE MAIN POINTS

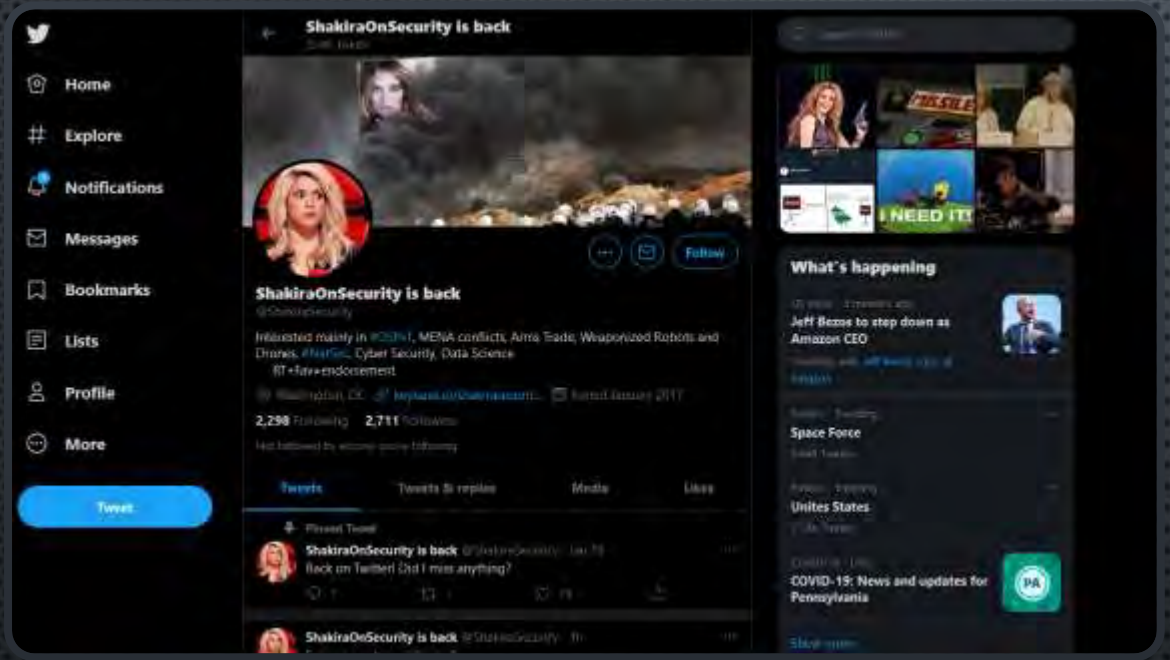
- *Social engineering attacks need to combatted internally by your business employees, not solely through products and solutions*
- *Security lapses are a threat to modern businesses and is the job of every employee regardless of title.*
- *Building internal resilience to threats is not about hunting a secret agent, but training staff in a way they want to learn.*

PART 2: SOCK PUPPET STAGE

Social Engineering in Practice

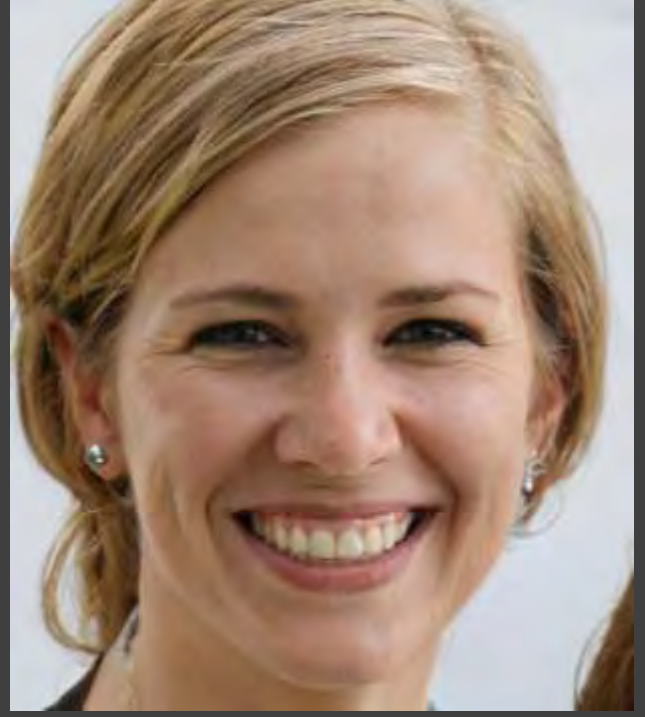
Daniel Saylor

WHAT IS A SOCK PUPPET?



ALTERNATIVE IDENTITIES IN CYBER SECURITY

- SECURITY PROFESSIONALS: OFFENSIVE OPERATIONS/PENETRATION TESTS
- CRIMINALS: ANONYMIZE AND LEAD ON POLICE/INVESTIGATORS


FALSE FLAG OPERATIONS

- WITH MODERN TECHNOLOGY, THE ABILITY TO CREATE A TOTALLY DIFFERENT IDENTITY IS STARTINGLY EASY.
- RANDOMIZED RESULTS: AI GENERATED PROFILE PHOTOS, PRIVACY GUARANTEED SERVICES AND MIDDLEMAN SERVICES ALLOW FOR THE CONSTRUCTION OF A FAKE IDENTITY FOR CHEAP

VERIFYING POORLY MADE IDENTITIES

- Email Address Lookup/Verify
  - Hunter.io - https://hunter.io/
  - Phonebook.cz - https://phonebook.cz/
  - VoilaNorbert - https://www.voilanorbert.com/
- Verifying Email Exists
  - Email Hippo - https://tools.verifyemailaddress.io/
  - Email Checker - https://email-checker.net/validate
  - Clearbit Connect - https://chrome.google.com/webstore/detail/clearbit-connect-supercha/pmnhcgfcafcnkbengdcanjablaabjplo?hl=en

OTHER TOOLS

- Creating an Effective Sock Puppet for OSINT Investigations – Introduction - https://jakecreps.com/2018/11/02/sock-puppets/
- The Art Of The Sock - https://www.secjuice.com/the-art-of-the-sock-osint-humint/
- Reddit - My process for setting up anonymous sockpuppet accounts - https://www.reddit.com/r/OSINT/comments/dp70jr/my_process_for_setting_up_anonymous_sockpuppet/
- Basic Starter
  - Fake Name Generator - https://www.fakenamegenerator.com/
  - This Person Does not Exist - https://www.thispersondoesnotexist.com/
- Private Credit Cards
  - Privacy.com - https://privacy.com/join/LADFC - *Referral link. We each get $5 credit on sign up.

How are sock puppets being combatted?

- Both criminals and professionals use sock puppets
- Typical preventative methods:
  - Anonymizer active during signup
    - Tor
    - VPN
  - VoIP Phone numbers
  - Google Numbers
  - Flagged Email Extensions (10 minute mail, ect)
- Money as a Barrier

Activity Scope

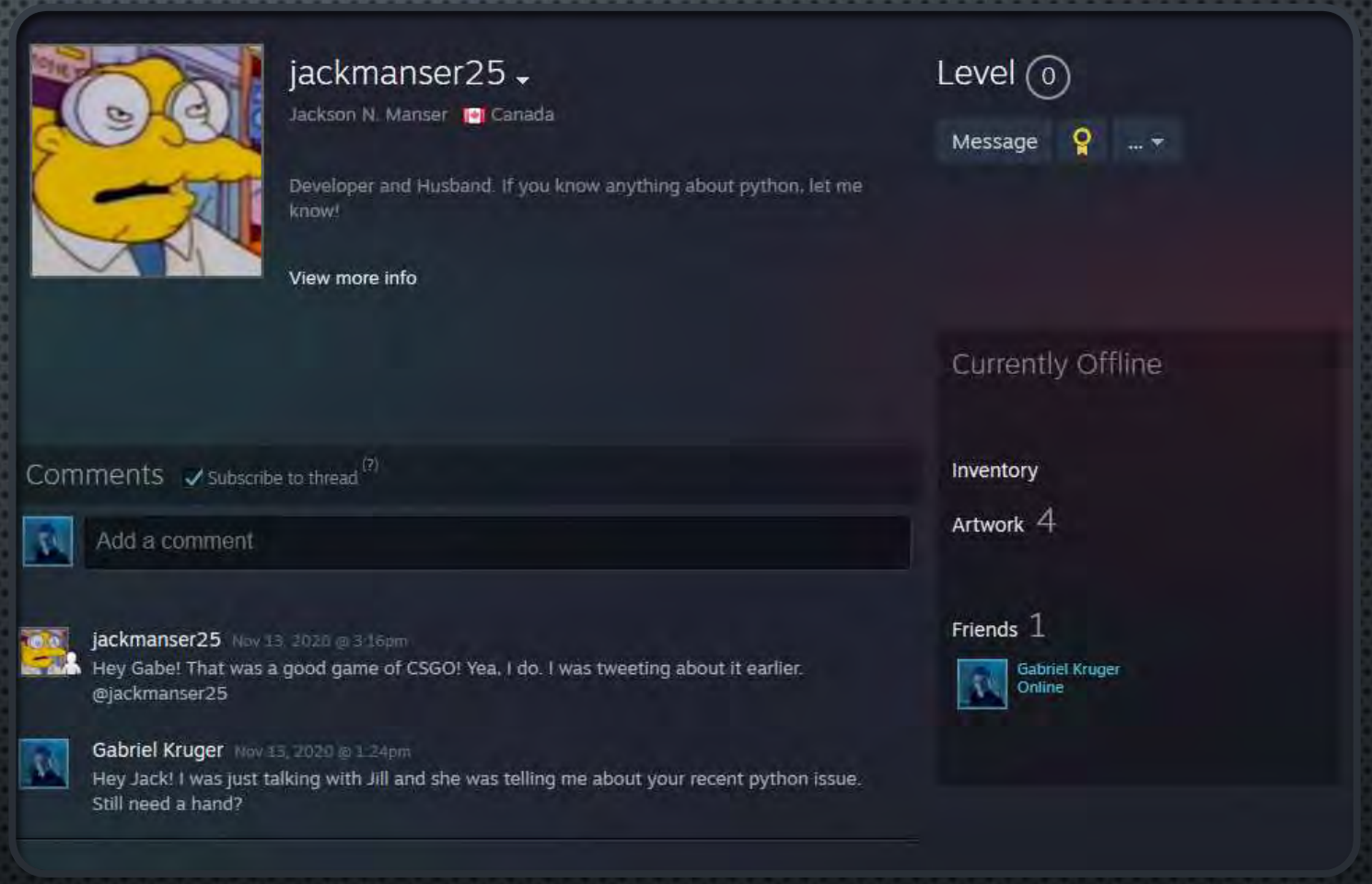
- While this project has been designed to give you as much freedom as possible to conduct your investigation, straying from the target is always a risk. Activities that fall within the boundaries of the assignment are called 'in scope,' and everything else is considered 'out of scope.' Therefore, the scope has been defined as follows:
- The following URLS are valid and can contain information/flags: *steamcommunity.com*, *Twitter.com*, *Tumblr.com*, *Github.com*, *Facebook.com*, *drive.google.com*, and *pastebin.com*.
- The following URLS can contain useful information for research and solving puzzles: *cryptii.com*, *crypto.interactive-maths.com*
- *The user Gabriel Kruger is out of scope*

Rules of Engagement

- **Rules Of Engagement:** Because of the nature of this activity, the rules of engagement are as follows:
  - Under no circumstances 'follow' or 'friend' the target.
  - Under no circumstances log in to any account during the investigation.
  - Under no circumstances attempt to contact the target through direct messaging, commenting or any other means.

TIME TO HUNT

- *HTTPS://STEAMCOMMUNITY.COM/ID/JACKMANSER25/*



Cyber security meeting

9-28-21

5:30 started the meeting and went over current news events regarding cybersecurity
- More specifically the Outlook bug and the data leak and lost money in result
- There is a new malware targeting android users in the US and Canada, occurred through SMS messages

5:35 Went over the capture the flag topic of the meeting
- Two specific categories: jeopardy and attack-defense
- Jeopardy: completing specific categories such as programming, applications, networking, forensics, and cryptography
- Attack-Defense: protecting or attacking a vulnerable computer system, and to gain points the team needs to maintain possession of as many systems as possible versus other competitors
- The history of CTF: first occurred in 1996, it serves as a steppingstone to jumpstart your career while introducing you to new tools and concepts regarding cybersecurity. It also familiarizes you with situations that occur in the real world.

5:40 2019 CAE-NE Hackathon
- IUP participated in 2019 against 8 different schools around our area. It ran from around 9 am to 4 pm. We were then provided resources for this event. Discussed who would want to participate if IUP were to join this event again.

5:50 OverTheWire Simulation
- Participated in a hands-on simulation playing bandit on OverTheWire

6:30 Concluded the meeting

CYBER SECURITY CLUB 9-28-21

FRANKLIN MAY

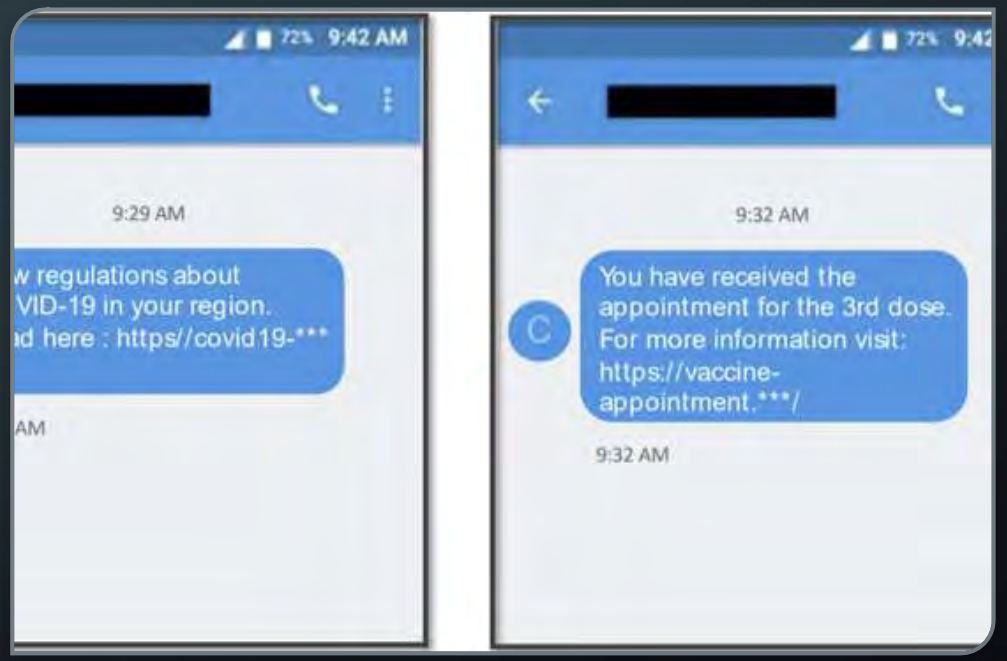
CYBER SECURITY IN THE NEWS

- Exchange/Outlook Autodiscover Bug
  - Leaks $100K+ Email Passwords
  - When adding a new Microsoft Exchange account to Outlook via the auto account setup
  - Autodiscover attempts to put together a URL to get configuration data based on the email domain
  - If it cannot find a domain, such as this it will attempt to build a URL using Autodiscover.com which means that the person who owns this domain will receive any of these xml documents containing log in information

- https://Autodiscover.example.com/Autodiscover/Autodiscover.xml
- http://Autodiscover.example.com/Autodiscover/Autodiscover.xml
- https://example.com/Autodiscover/Autodiscover.xml
- http://example.com/Autodiscover/Autodiscover.xml

NEW ANDROID MALWARE TARGETING US AND CANADIAN USERS

- Emerging malware called “TangleBot”
- Called this because the malware has many layers of control over different device functions
- Such as contacts, SMS, call logs, internet access, camera
- Starts as an SMS message claiming to contain new information on the COVID-19 vaccine



CAPTURE THE FLAG

DIFFERENT FORMATS

- Jeopardy
  - Complete as many categories from a given section
  - Common categories include, but are not limited to: programming, applications, networking, forensics, mobile, cryptography, and reverse engineering
- Attack-Defense
  - Team must either defend or capture vulnerable computer systems
  - To gain points teams need to maintain possession of as many systems as possible while keeping competitors out

HISTORY OF CTF

One of the first prominent CTFs occurred during DEF CON 1996

DEF CON and other Computer Security conventions have consistently held various forms of Capture the Flag since

CTF is an example of a wargame coined from the movie WarGames (1983)

Used to teach the basics of web attacks and web security

WHY PARTICIPATE IN A CTF COMPETITION?

2019 CAE-NE HACKATHON

- CTF held remotely by CAE-NE
- Hybrid CTF using both Jeopardy style and Attack-Defense style
- Separated into two sections one working on each portion
- Ran from around 9AM to around 4PM along with a few hours for set up the night before
- Competed against 8 different colleges around the area

Cyber Security meeting

9/14/21

5:30 PM: Started the meeting with some brief cyber security in the news

5:45 PM: Began presentation on phishing scams. Learning how they work, why they are so dangerous, and how they are made.

6:00 PM: Began creating our own phishing scam where we took the Facebook log in page, and edited the HTML code so that rather than logging in the Log In button will take the user to “Never Gonna Give You Up” by Rick Astley

6:30 PM: Concluded the meeting

Cyber Security Club 9-14-2021

Franklin May &

Ethan Buhl

Cyber Security In The News

- FTC is warning the LGBTQ+ community about extortionists on dating apps
  - Scammer on apps such as Grindr and Feeld
  - They will send explicit phots, and ask the target to reciprocate
  - They will then blackmail their target into paying a ransom
  - Some scammers will also out ‘closeted’ individuals found on these apps
  - FTC warns that users should not share explicit photos on these apps as there has been a massive increase in ‘sextortion’ attacks since January 2021

Cryptominers Hiding Logic Bombs in Python Packages

- Researchers discovered a logic bomb attack in the Python Package Index (PyPI)
- PyPI is a code repositor for Python developers
- Aim was to get honest software developers to deliver these bombs
- It is believed that the payloads included have been downloaded around 5,000 times
- The purpose of this is to hijack these systems for cryptomining

Python Packages cont.

- Complex event due to multiple different kinds of attacks
- Logic bombs
  - A set of instructions incorporated in a program that will carry out when a certain condition is met
- Cryptojacking
  - Malicious cryptomining by hacking into a computer to install software to mine cryptocurrencies
- Software Supply Chain Attacks
  - When a threat actor infiltrates a software vendor and employs malicious code before the vendor sends it to their customer

Phishing

Ethan Buhl

What is phishing?

“The fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.”

- Type of Social Engineering

History

- 1995
- Didn’t get popularized till 2000
- ILOVEYOU
- Destroyed files
- $5.5 – $8.5 Billion in damages

(Not so) Fun Facts

- 32% of data breaches
- 88% of companies experienced spear phishing
- New phishing site very 20 seconds

Types of Phishing

- Spear Phishing
  - Specifically tailored
- Phone Phishing
  - Scam Calls
- Phishing Website
  - Slightly varied URL
  - Ex. www.paypa1.com instead of www.paypal.com

How to defend?

- Traditional defenses won’t work
- Training Employees
- Err on the side of caution
- Being diligent

Questions or Discussion?

Simple Phishing Attack

Cyber Security Meeting

9-7-21

5:30 PM: Started the meeting with a presentation going over the club, and what the club has done in the past

5:50 PM: Completed elections for club officers ended with

- President
    - Franklin May
- Vice President
    - Ethan Buhl
- Secretary
    - Jacey Henderson
- Treasurer
    - William Franklin

6:15 PM: Meeting End

CYBER SECURITY CLUB 9/7/21

FRANKLIN MAY

CYBER SECURITY IN THE NEWS

- Howard University internet outage due to ransomware attack
  - This past Friday Howard University's IT team detected unusual activity on the network
  - The school's Enterprise Technology Services (ETS) intentionally shut down the network to investigate
  - Has been announced that this was dur to a ransomware attack, and are actively restoring operations
  - Classes canceled for today 9/7/2021

NEWS CONT.

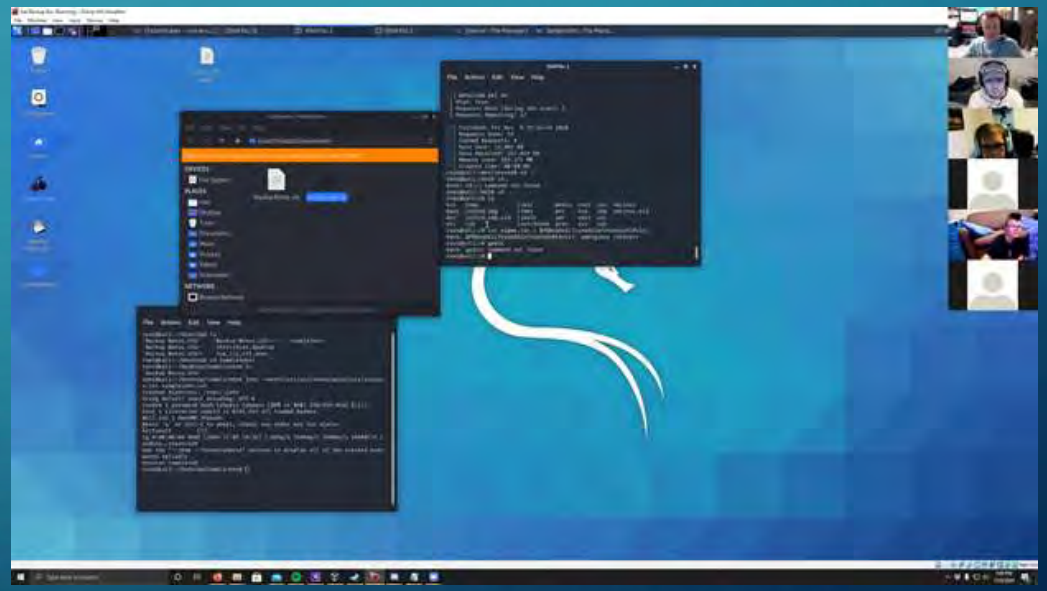
- Malicious Office documents make up 43% of all malware downloads
  - Millions use Microsoft Office documents daily
  - Researchers at Atlas VPN
  - EMOTET is most widely used
  - EMOTET injected into word files allowing the installation of other malicious software

CYBER SECURITY CLUB ACTIVITIES

- 2019 CAE-NE Hackathon
- CTF portion
- Blue Team portion
- Conducted remotely
- First Place for IUP

CYBER SECURITY CLUB ACTIVITIES CONT.

- 2020 Hackathon
- Conducted over zoom due to COVID
- Hosted by IUP
- Connect to VPN in order to attack vulnerable machine
- Goal was to obtain root access



CYBER SECURITY CLUB ACTIVITIES CONT.

- Hack the Box
- Overthewire.org
- Introductions of topics such as Ransomware, Keyloggers, Memory Acquisition/Analysis, and Enumeration

CYBER SECURITY CLUB ACTIVITIES

Interested in Cybersecurity?

Expose yourself to new experiences and activities

- Collaborate with others
- Build up your rsum
- Learn new security advances
- Discuss cutting-edge topics
- Bring your ideas to the table

Club Meetings

Every other Tuesday evening from 5:30 p.m. to 6:30 p.m. via Zoom

Who We Are

The Cyber Security Club is a student-run club with the goal of providing outside-of-class activities relevant to the industry. Attendees will leave with valuable experience proven to be useful during interviews and jobs. The club is open to everybody at IUP no matter what experience level or major you are. Our goal is to expand our knowledge of cybersecurity and information security through hands-on experience and direct interaction with professionals in the field.

Our club competed in the 2019 CAE-NE Hackathon and placed first. This opportunity provided hands-on experience in combating real-life cyber threats. No prior experience is required to participate in a hackathonyou learn as you compete. More info on this competition can be found in this news post about the Hackathon. Stop by our next meeting to learn more about future activities.

Recently, the Club members organized the first IUP Hackathon event on November 7, 2020. That competition was opened to IUP students and members of the community. For details on that event, please visit its page.

WHAT WOULD YOU LIKE TO SEE

ELECTIONS

President	Vice President	Secretary	Treasurer
• Provides leadership to officers and members • Leads/teaches majority of meetings	• Plans/coordinates meetings in cooperation with the President • Leads/teaches meetings in the President's stead	• Takes Meeting Minutes • Sends meeting announcement emails	• Takes care of financial decisions made by the club

REFERENCES

- https://wjla.com/news/local/howard-university-investigates-alleged-ransomware-attack?&web_view=true
- https://www.hackread.com/malicious-office-documents-malware-downloads/?web_view=true
- https://www.hackthebox.eu/
- https://overthewire.org/wargames/
- https://www.iup.edu/cybersecurity/activities/cyber-security-club/