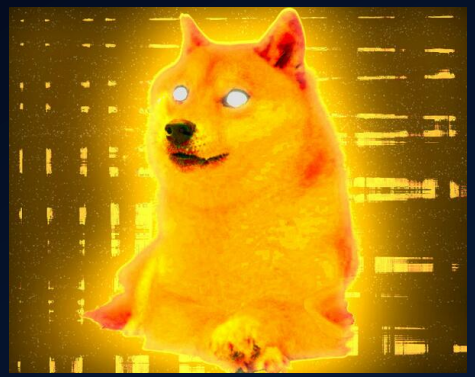
UMBC Cyber Defense Team

FIRST MEETING PRESENTATION
2016-2017

Welcome to the UMBC Cyber Defense Club!

- Also called the UMBC Cyber Dawgs!
- A student run organization since 2009.
- We're a group of students that share a passion for-and recognize the importance of-computer and network security

such hack



much cyber

Some Introductions

- President: Bryan Vanek
  - Comp Sci & Math, Spring 2018
  - Firewalls, Secure Programming
- Vice President: Anh Ho
  - Computer Science, Spring 2017
  - Windows Administration
- Secretary: Zack Orndorff
  - Computer Science, Spring 2019
  - Linux Administration
- Treasurer: Christian Beam
  - Computer Science, Spring 2019
  - Computer Networking, SDN
- Historian: Jacob Rust
  - Computer Science, Spring 2017
  - History, Awesome Hype Man
- Technical Advisor: Chris Gardner
  - Comp Sci & Math, Spring 2018
  - Offensive Security, Forensics

So…what is cyber security?

- The protecting of computers, networks, programs and data from unintended or unauthorized access, change or destruction
- Basically keeping the bad guys out, while keeping everything up and running
- Several different types of cyber security
  - Application Security
  - Network Security
  - Information Security
  - Recovery/backup security
  - Offensive Security
  - And much, much more!!

Why is Cyber Security Important?

- Highly sensitive data is accessed, stolen, and/or used every day
- Over 480 million records leaked in 2015-and those are just the big, well-known hacks
- A lot of these hacks could have been mitigated with proper training and good practices
- In other words, people's lives get ruined because of this, and most (if not all) of it is preventable

Who Should Use Cyber Security?

- EVERYONE!!!! Not just limited to IT professionals
  - Hospitals
  - Large and small commerce + financial institutions
  - ALL government agencies
- The need for cyber security is crucial-from enterprise to mom & pop shops!
- Job market is always looking for cyber security experts
- Oh, AND it's suuuuuper fun to learn about.

How Do the Cyber Dawgs Approach This?

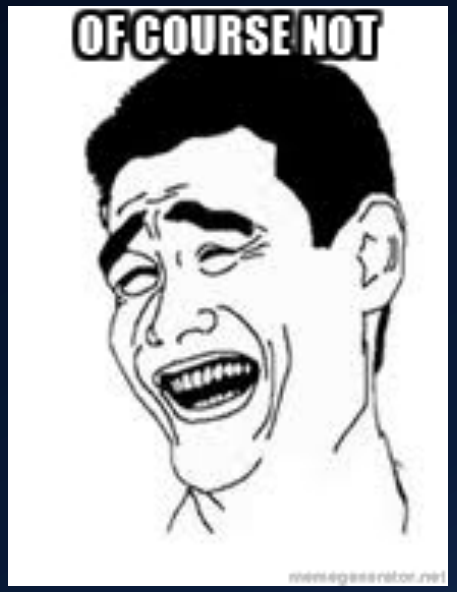
- There are lots of ways to learn about cyber security…
- …but we believe in approaching it through multiple tracks.
- We have three main tracks that we follow throughout the year:
  - Education + Hands-on
  - Competition Participation
  - Industry Exposure

Track #1: Education and Hands-on

- Our regular club meetings: every Wednesday from 7-9 in ITE233
- We go over lots of relevant and important topics pertaining to cyber security
- We have a schedule for this semester!
  - Check it out on our website: http://umbccd.umbc.edu/
- Some stuff we'll be covering this semester:
  - Hashing and cracking tools
  - Website Exploitation
  - Networking + Network Forensics
  - Firewall Security

This all sounds super cool…but do I need to have experience coming in?

- No experience required!
- Schedule is tailored for beginners and veterans alike.
  - Having trouble/can't find a solution? Ask us!
  - Want to learn about something else? ASK US!
  - Bored/already know it? ASK US!!!
- Office hours: Wednesdays in ITE366 during free hour (from 12-1)
- We're building a resources page for everyone too!
- Also, we're working on a curriculum for a potential spring course (for credit), and we're looking for feedback through the semester! SO DO THAT!!



Track #2: Competition Participation

- What the club was founded on
- We encourage EVERYONE to do at least one competition while they're part of the cyber dawgs
- Lots of different types of competitions available!
  - Defensive Competitions
  - Offensive Competitions
  - Mixed Style Competitions

Some Upcoming Competitions

- NSA Codebreakers: Starts September 9th!
  - Registration available at https://codebreaker.Ltsnet.net (use your UMBC email)
- CSAW CTF (Cyber Security Awareness Week): Qualifiers begin September 16th!
  - We'll have our own teams-speak with us if you're interested!
- NCL (National Cyber League): Registration up until October 3rd!
  - http://www.nationalcyberleague.org/
- Others: Kaizen, MITRE, PICO, CCDC (will post as details become available)
- We also have a coach for this year's CCDC competition!

Oh…and WE are hosting our own CTF!

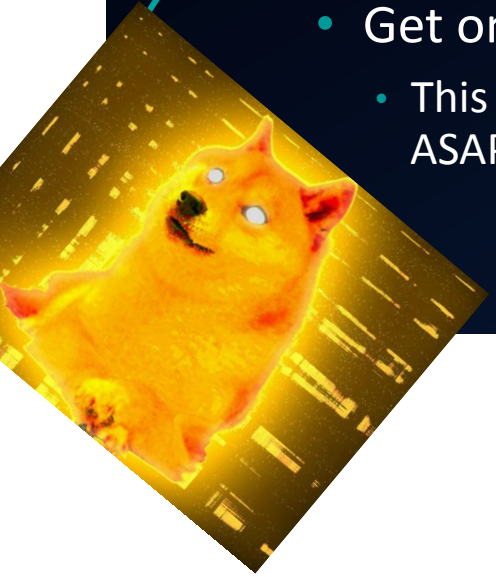
- The DawgCTF; tentatively scheduled for 3/4/17
- Jeopardy style CTF open to the entire UMBC campus!
- A great event for first timers!
- Topics will include (but are not limited to)
  - Network Forensics
  - Reverse Engineering
  - Cryptography
- There will be prizes for top performers!!!
- There will also be some companies to network with!
  - Parsons
  - Splunk
  - More to come!

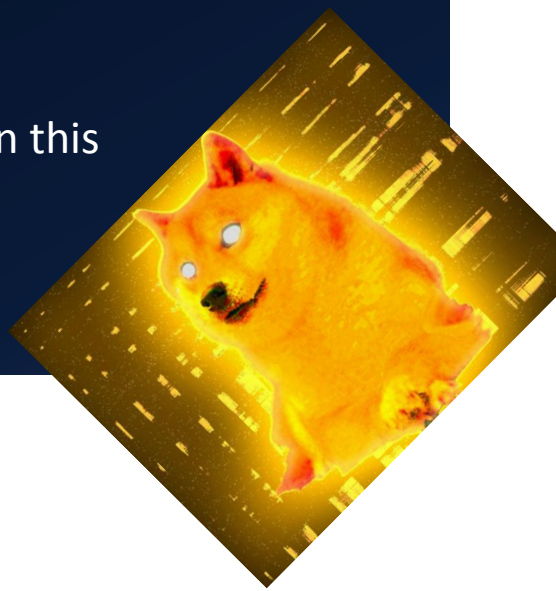
Track #3: Industry Exposure

- The fields of IT, CS, IS, and cyber security is ever changing
- It's important to know what industry is using today!
- We'll have some industry folks come in and give talks, demos, and labs!
  - NSA Codebreakers: Details + Tips & Tricks with Dan Guernsey
  - Parsons: The Farm Initiative with Brett Hite
  - Splunk: More than a SIEM (Security Information and Enterprise Management) + Security Enterprise with Sabrina Lea
- Dates + Times will be released as they become available!

YEEHAW!!! I'M TOTALLY HOOKED!

- Remember: our regular club meetings are Wednesdays from 7pm-9pm in ITE233.
- Check out our website to see our schedule, resources page, and link up with the group at http://umbccd.umbc.edu/
- Subscribe to our mailing list: send an email to umbccd-subscribe@lists.umbc.edu to join
- Get on our slack channel! https://umbccd.slack.com
  - This is really the best way to communicate with us, so get on this ASAP!





Now, a few more things to note (courtesy of our previous president, Julio Valcarcel)

- Learning cyber security is hard
  - Meetings are a starting point
  - Requires dedication and time
  - Don’t hesitate to ask questions-we are here to help!
- If you have suggestions for talks, let us know!
- When replying to mailing list make sure it has the person’s email not the mailing list email address
- Don’t reply to umbccd@lists.umbc.edu unless it is for the whole list

OH…AND THIS IS IMPORTANT

- While we are a cyber defense team, the tools and techniques we will be going over are used to break into a system/network
- So unless it is YOUR server, computer, virtual machine, or service, or unless you have EXPLICIT and COMPLETE permission to do so…
- DO NOT USE ANY OF THESE TOOLS OR TECHNIQUES ON A SYSTEM THAT YOU DON'T HAVE COMPLETE AUTHORIZATION TO DO SO
- If you don't adhere to this, some of the legal ramifications include-but are not limited to-the following:
  - Expulsion from UMBC
  - Being charged for either a misdemeanor or a felony, depending on the severity
    - Fines up to $100,000 for misdemeanors, up to $250,000 for felonies
    - Jail time up to 1 year for misdemeanors, up to 10 years for felonies
  - AND THIS IS JUST THE FEDERAL LEVEL.


UMBC
CYBER DEFENSE
ANY QUESTI
ALRIGHT, NOW IT'S TIME FOR SOME AWESOMENESS
COURTESY OF OUR HISTORIAN, JACOB RUST!!

So…let’s talk about some recently reported hacks…

The DNC Hack

- Discovered by Crowdstrike on June 14tt, corroborated by Fidelis Cybersecurity and Mandiant
- Two separate Russian intelligence-affiliated adversaries present in the DNC network
  - One group had access for more than a year
- Methods of attack included gaining root access through malware (originated from Russian military intelligence-identical SSL certs)
- Results? Resignations (Debbie Schultz), disclosure of countless communications/emails, PII
- A complicated, planned attack…but this isn't always the case

Social Engineering

- Successful infiltration/hacking mainly comes from something called Social Engineering
  - Psychological manipulation to get access to confidential information
- People who were recently ‘engineered’
  - Mark Zuckerberg (Facebook CEO): Twitter & Pinterest hacked (password was ‘dadada’)
  - Sundar Pichai (Google CEO): Quora + Twitter
  - Leslie Jones (Actress): iCloud revealed passport, driver’s license, phone number

The reason I'm telling you this?

- Hacking and infiltration take on many different forms
- Whether you're a public figure or the most private individual ever, if someone is motivated enough and has enough time, they WILL get your information
  - Truly, in today's society, it's not a matter of 'if,' but a matter of 'when'
- You are only as secure as your weakest point of entry
  - One weak password or one missing piece of software can lead to a cascade of infiltrations and breaches
- So as you learn with us this semester, always keep this in mind: WE ARE NOT JUST HERE TO LEARN-WE ARE HERE TO EDUCATE

Alright, enough chit chat
LET’S SHOW YOU GUYS SOME COOL STUFF YOU CAN DO WITH WHAT YOU LEARN HERE!