How to Frustrate a Penetration Tester

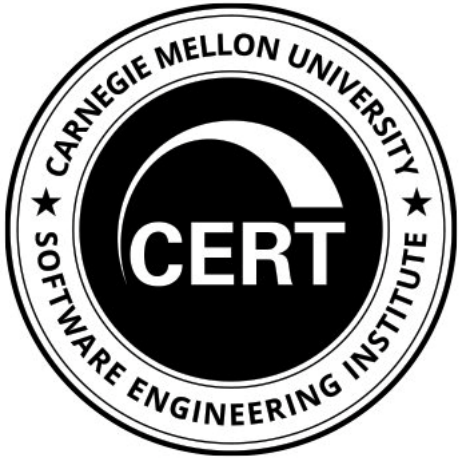
Justin Forbes

Disclaimer

- The statements expressed in this presentation are solely my own and do not represent my employer, university, government, or family
- If you can’t handle memes now is the time to leave
- Do not implement any suggestions without doing your own due diligence and getting organizational buy in, I don’t know your network you should
- I might swear

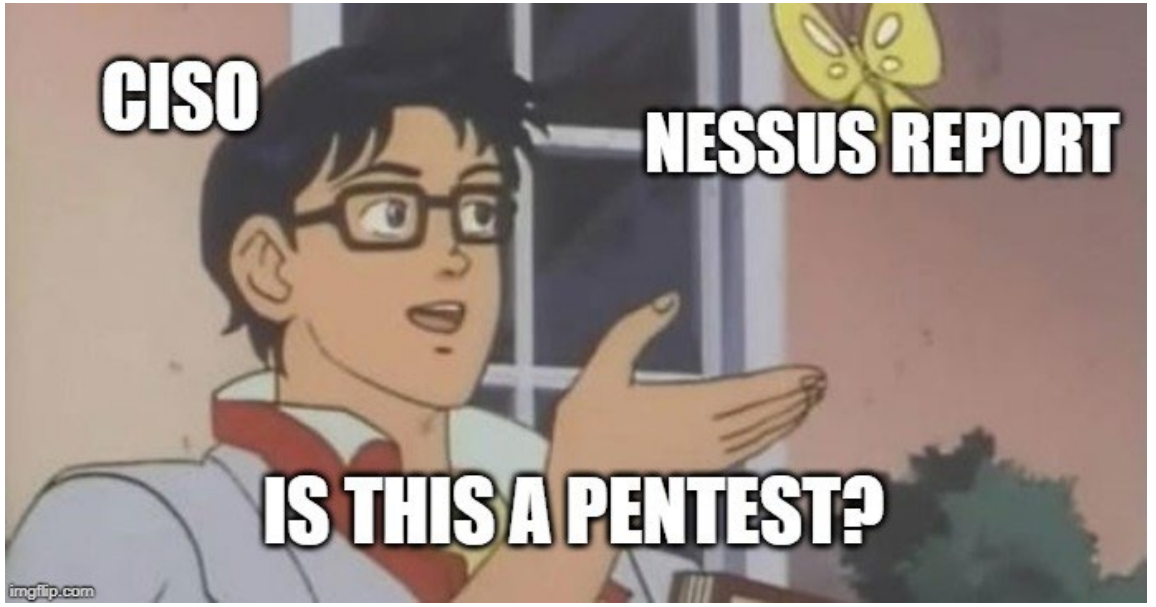
Who am I?

- ❑ Bachelors of Information Science from Pitt in 2008
- ❑ Masters of Telecommunications from Pitt in 2010
- ❑ Started at CERT/SEI/CMU in 2010
- ❑ Team Lead for Applied Network Defense Team
- ❑ Teacher for Ethical Penetration Testing class at CMU
- ❑ Led over 50 penetration tests
- ❑ 8 years of beard growth
- ❑ Still learning and failing everyday



What is a Penetration Test?

- ❑ Can scale in complexity based on an organization's maturity
- ❑ Value of the test corresponds to the scope
- ❑ Not looking for every possible vulnerability
- ❑ Identify risk and show impact



Vulnerability Assessment → Traditional Penetration Testing → Threat Emulation → Red Team Assessment

Frustration is Good

- Penetration testers love a challenge
- Frustration spawns new tools, techniques, and tactics
- We only want to work as hard as we have to, just like an “APT”
- Good frustration vs Bad frustration

Source: https://www.sustainableman.org/wp-content/uploads/2018/12/shutterstock_261667859-1024x734.jpg

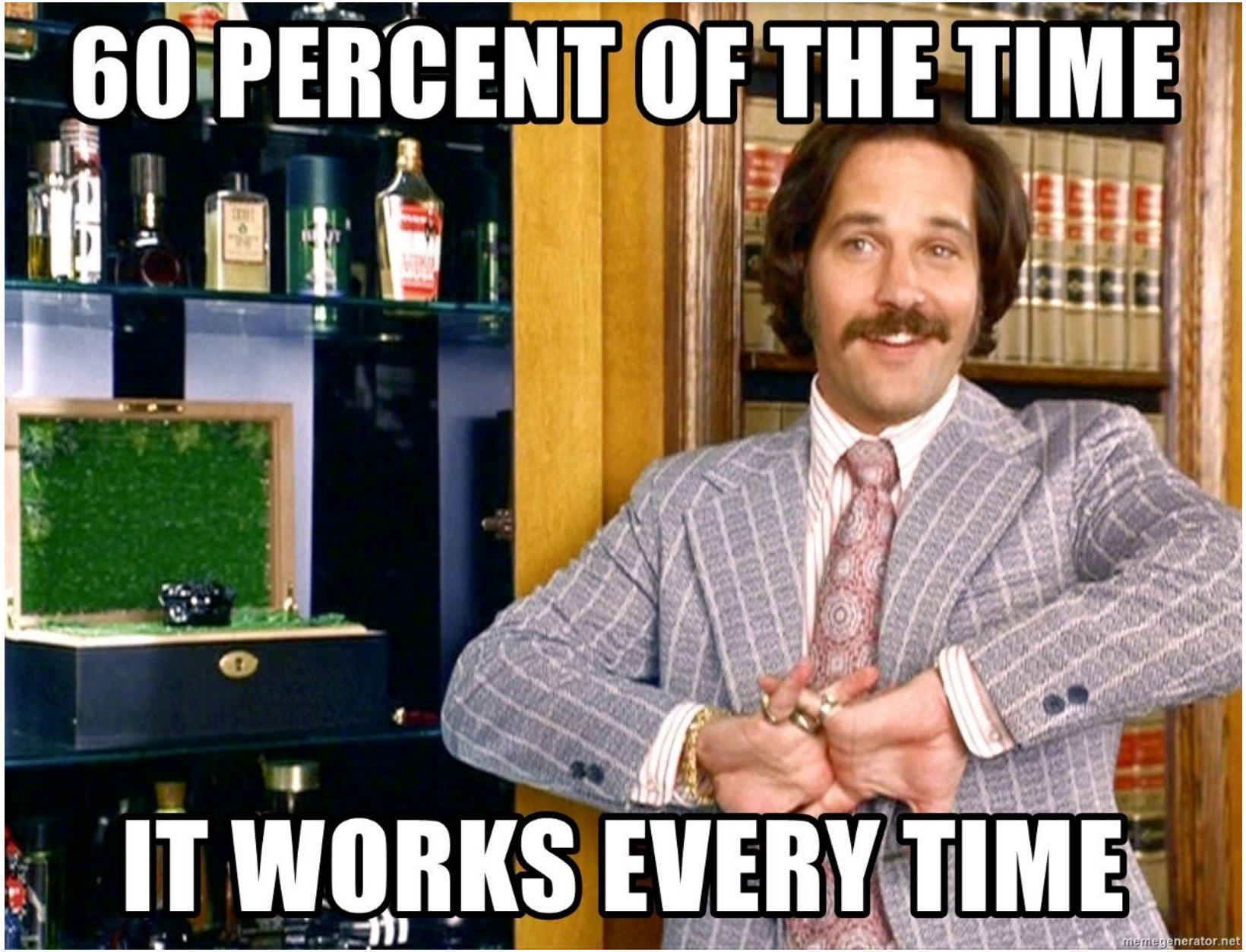
The Current State of Penetration Testing

Source: https://www.memecreator.org/static/images/memes/4647173.jpg

How Does It Happen?

- ❑ **Phishing**
- ❑ **Lack of Cyber Hygiene**
- ❑ **Password Hashes**
- ❑ **Active Directory Misconfigurations**

Phishing

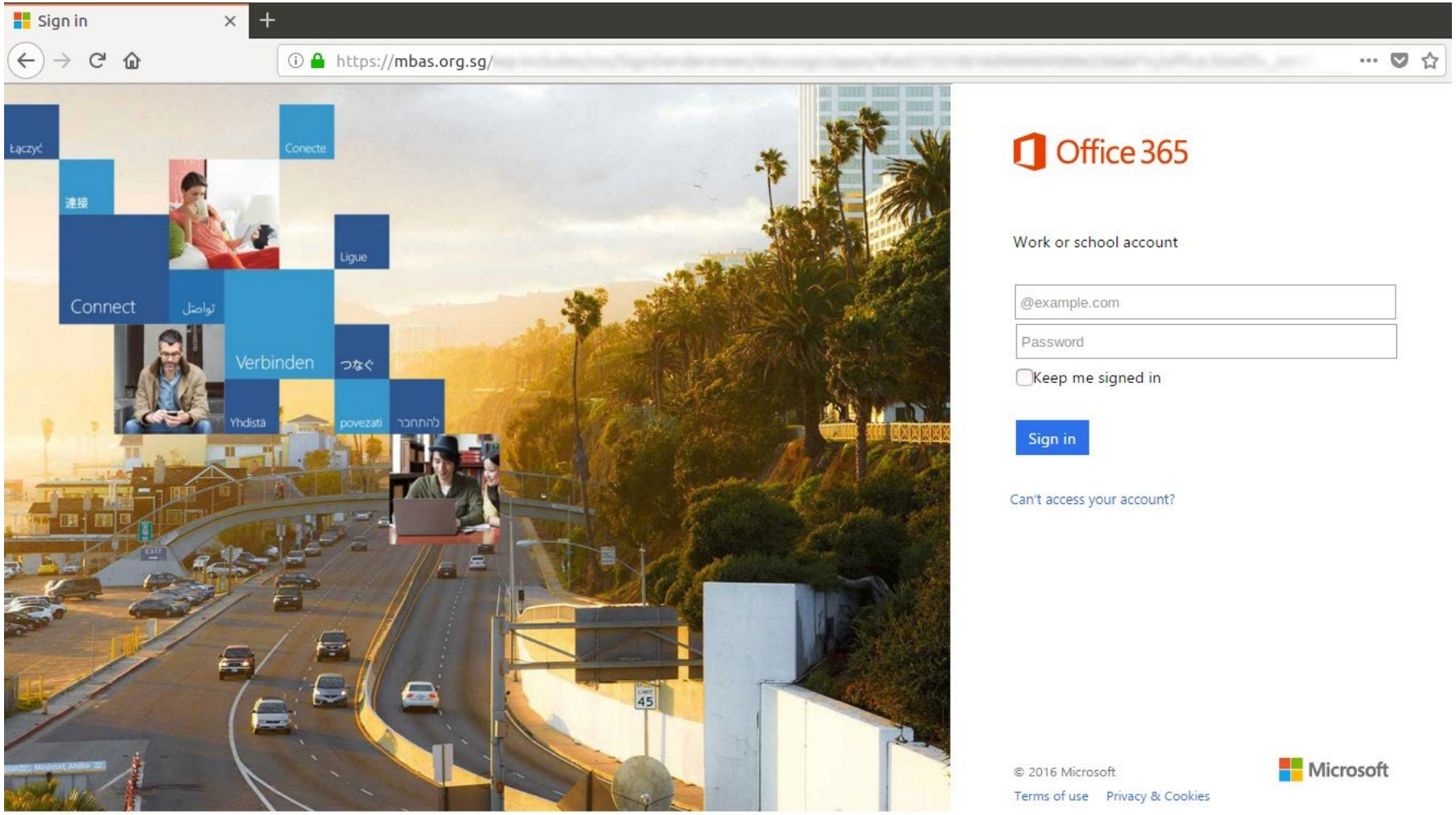


Source: https://cdn-images-1.medium.com/max/1250/1*bEhPyKq9ckEHMrJlUm8xNg.jpeg

Two Main Goals of Phishing Emails

- Phishing for credentials
  - Attacker clones a login page and attempts to trick a user
  - Attacker directly asks the user for credentials in the email
- Phishing for access
  - Attacker is attempting to execute code on the targeted system
  - Payloads are delivered either as attachments or as links within the email

Stealing Credentials



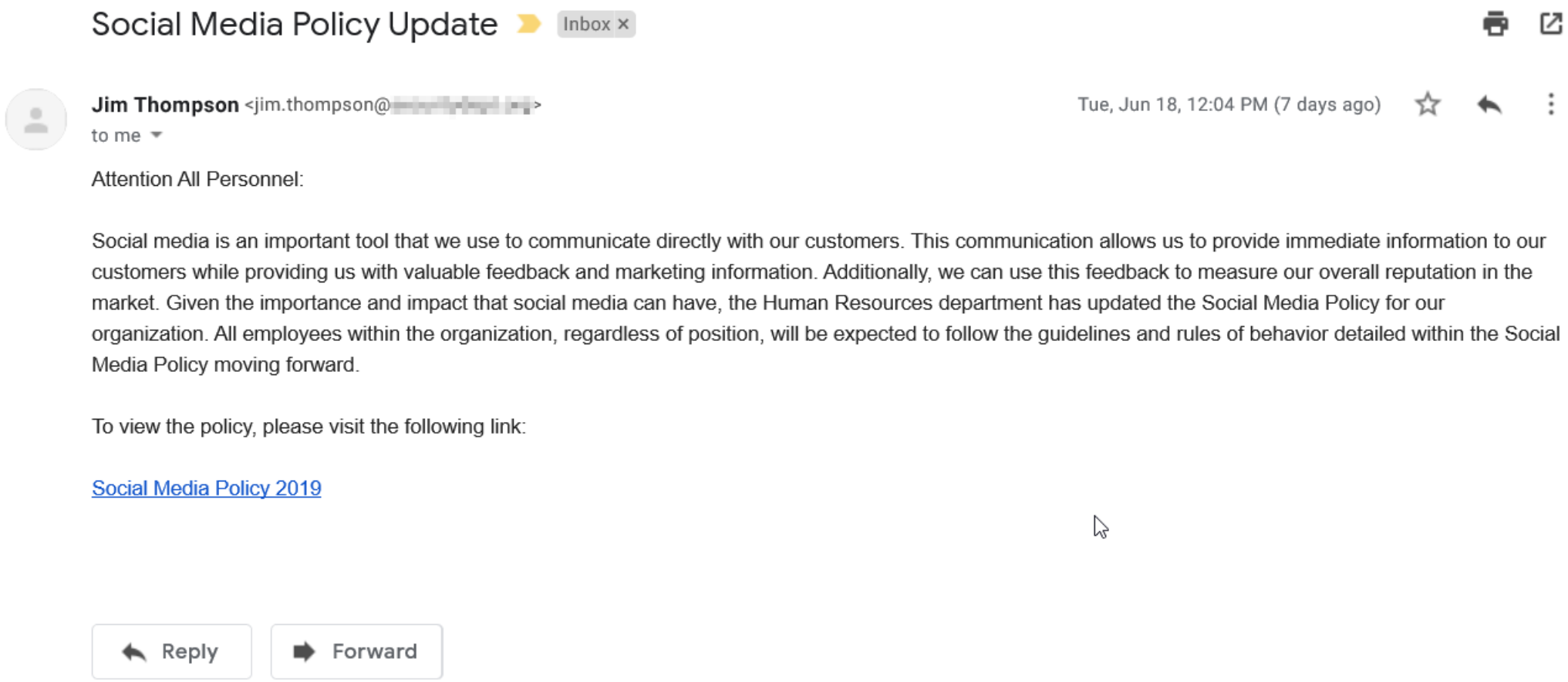
Source: https://www.mailguard.com.au/hubfs/180226-o365-sign.jpg

Protecting Credentials

- ❑ Encourage the use of password managers
- ❑ Enable multi factor authentication

Source: https://3.bp.blogspot.com/-1c4ljejrpSE/W9vDlxt0dcI/AAAAAAAAeZ4/3cobNyEarKYrPeEOTZ2MhavANBQQ_dQUACKgBGAs/s640/how-i-felt-when-reddit-kept-telling-me-to-change-my-password-104581.jpg

Delivering a Payload



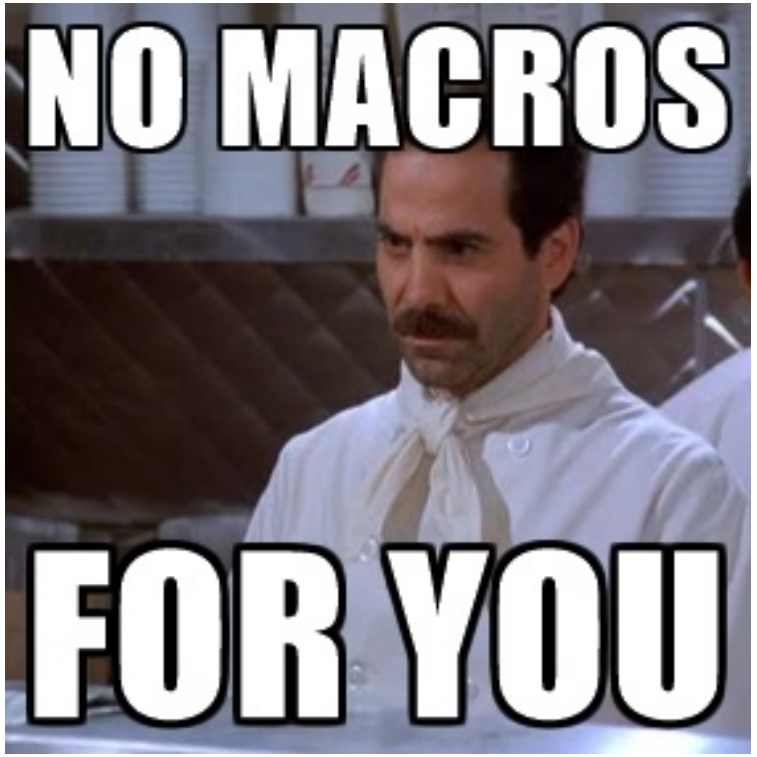
Payloads

- Common Payloads:
  - Office Macros
  - HTML Applications (HTA)
  - regsrv32
  - Living Off The Land Binaries and Scripts: https://lolbas-project.github.io/

Source: https://memegenerator.net/img/instances/62619915.jpg

Stopping Payloads

- Attack surface reduction: https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-exploit-guard/attack-surface-reduction-exploit-guard
- Change file type associations: https://support.microsoft.com/en-us/help/4028161/windows-10-change-default-programs

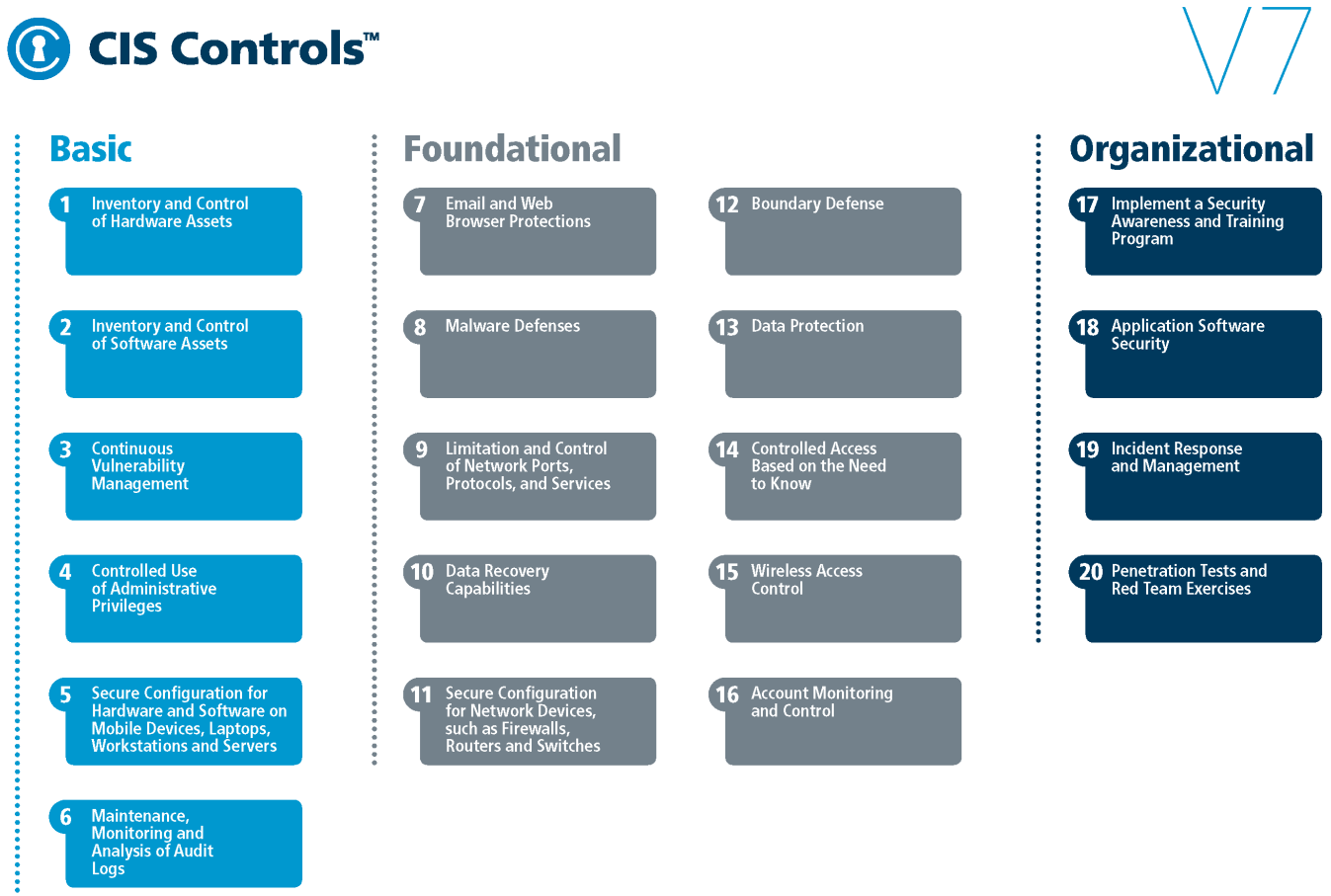


Source: https://www.stickleyonsecurity.com/article_images/1506030262.jpg

Lack of Cyber Hygiene

Source: https://10to8.com/wp-content/uploads/2018/11/cyber-security-meme.jpg

CIS Controls



Source: https://www.cisecurity.org/wp-content/uploads/2018/03/V7-Matrix-web-1024x720.png

Default Configurations

- Printers, cameras, web servers, VOIP systems, IPMI, switches, etc.
- Never seen an environment that didn't have at least one device with default credentials
- We prioritize systems that deploy/execute code

Source: https://pbs.twimg.com/media/Dx8ZLLWWkAAZ7kh.jpg

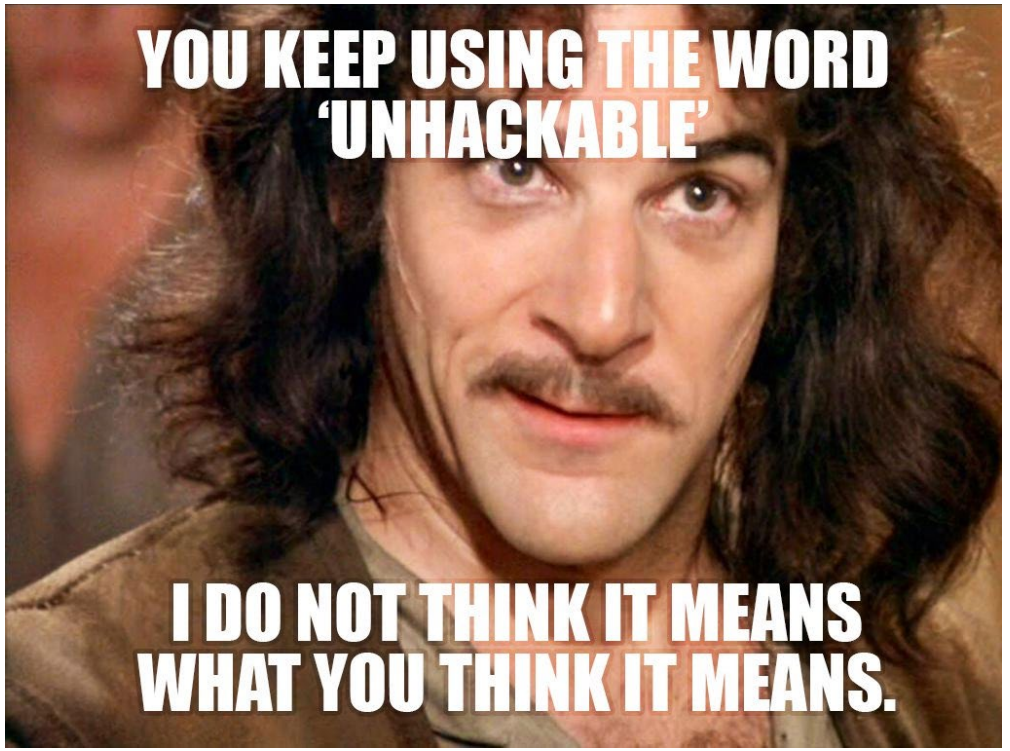
Patching

- Patching continues to be a struggle for many organizations
- Patching extends beyond just the Windows world
- “Too big to patch”
- Patch what you can and isolate the rest

Source: https://pbs.twimg.com/media/DscVRvoW0AI3UnQ.jpg

The Security Appliances Will Not Save You

- ❑ You can not buy your way to secure, but you can hire your way there
- ❑ Less is more when it comes to attack surface
- ❑ Marketers are not security engineers



Source: https://pbs.twimg.com/media/DM2WVizU8AEWoXG.jpg

Solutions

- ❑ Patch vs Breach
- ❑ Change management and system validation prior to deployment
- ❑ Follow the steps laid out in the CIS security controls
- ❑ Hire people not boxes

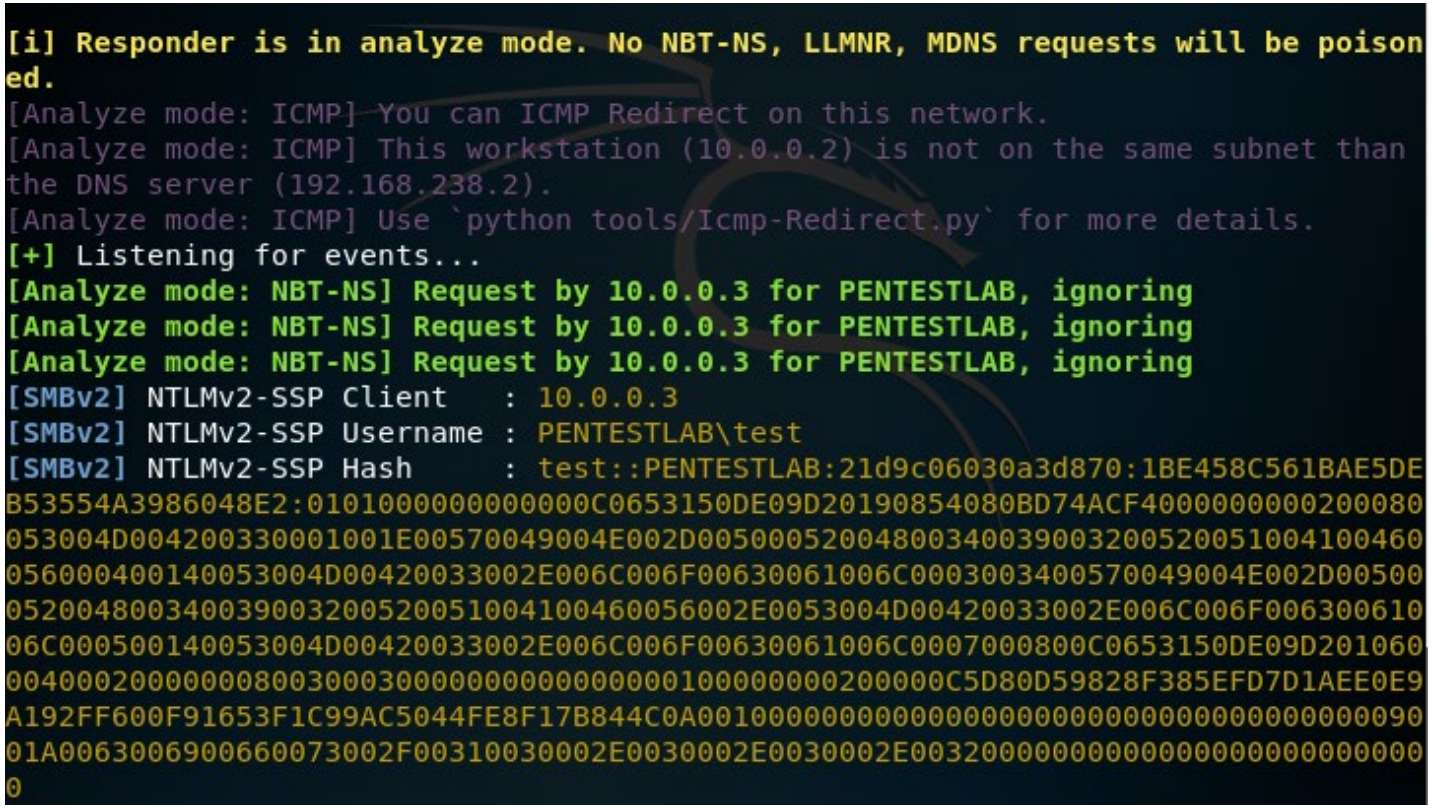
Source: https://cdn.netzpolitik.org/wp-upload/cyber-one-more-time-295x300.jpg

Password Hashes

Source: https://memegenerator.net/img/instances/61411966/hashes-hashes-everywhere.jpg

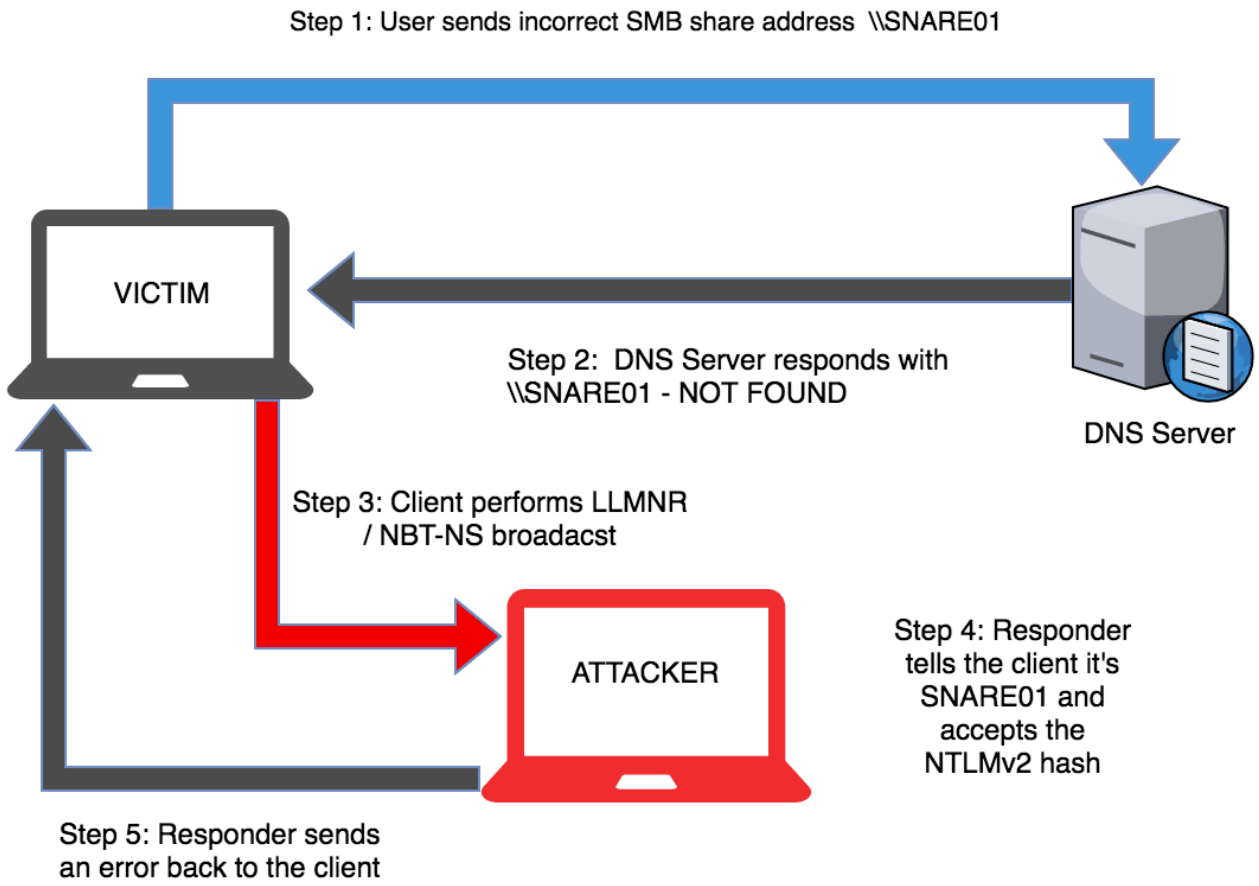
Tools I Use

- ❑ Responder
- ❑ CrackMapExec
- ❑ mitm6
- ❑ Hashcat
- ❑ smbexec.py
- ❑ ntlmrelayx.py
- ❑ Bettercap
- ❑ Multirelay



Source: https://pentestlab.files.wordpress.com/2018/05/nbns-spoofing-hashes-via-responder.png

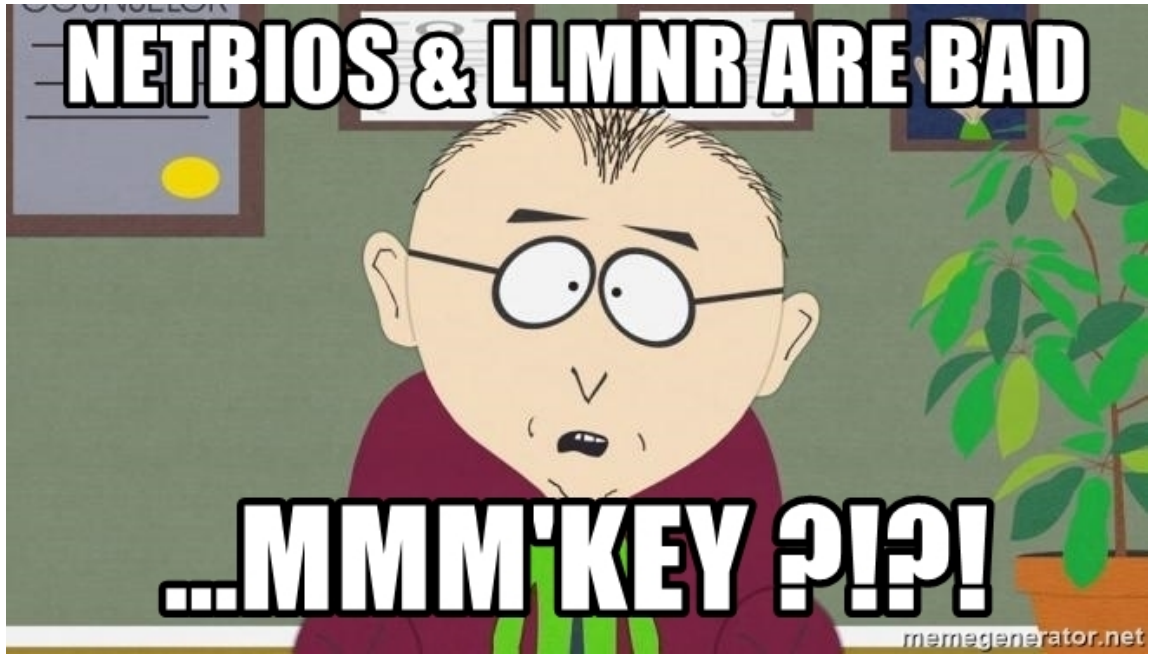
Basic Attack



Source: https://www.ivoidwarranties.tech/img/Responder/spoofing.png

Possible Solutions

- ❑ Disable LLMNR and NBT-NS: https://www.surecloud.com/sc-news/local-network-vulnerabilities-llmnr-nbt-ns-poisoning
- ❑ Enable SMB signing: https://support.microsoft.com/en-us/help/161372/how-to-enable-smb-signing-in-windows-nt
- ❑ Disable NTLM: https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-security-restrict-ntlm-ntlm-authentication-in-this-domain



Source: https://memegenerator.net/img/instances/71294035.jpg

Additional Considerations

- IPv6 man in the middle: https://blog.fox-it.com/2018/01/11/mitm6-compromising-ipv4-networks-via-ipv6/
- WPAD: https://pentest.blog/what-is-llmnr-wpad-and-how-to-abuse-them-during-pentest/
- ARP Poisoning: https://danielmiessler.com/study/bettercap/

Source: https://media.makeameme.org/created/stop-trying-to-r45cg2.jpg

Active Directory Misconfigurations

Source: https://makeameme.org/meme/look-at-me-5aa4e6

Tools I Use

- ❑ Bloodhound
- ❑ PowerSploit
- ❑ CrackMapExec

Source:
https://avatars1.githubusercontent.com/u/25502277?s=400&v=4

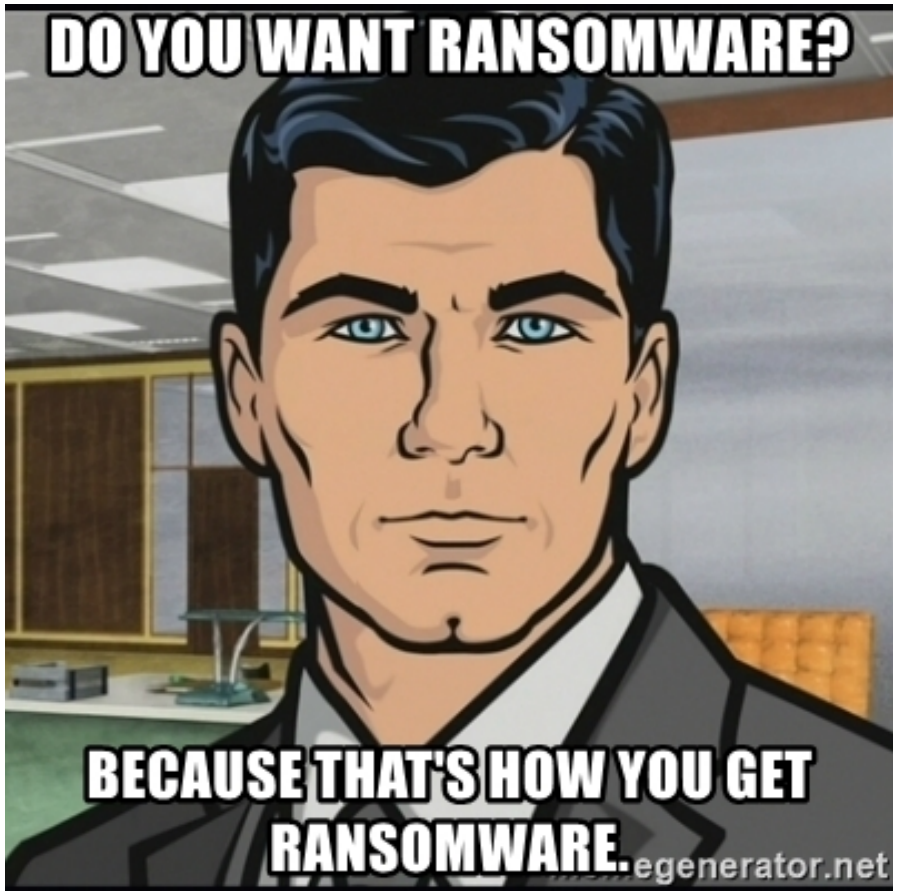
Users With Local Admin Rights

- Just browsing a malicious website or opening a phishing email means full system compromise, no privesc needed
- Figure out why the users need local admin and fix it

Source: https://media.makeameme.org/created/yall-got-any-5a4e4c.jpg

Same Local Admin Account Across the Org

- A single compromised local admin password or hash leads to full network compromise
- Very common when systems are deployed from a standard image



Source: https://memegenerator.net/img/instances/69496915/do-you-want-ransomware-because-thats-how-you-get-ransomware.jpg

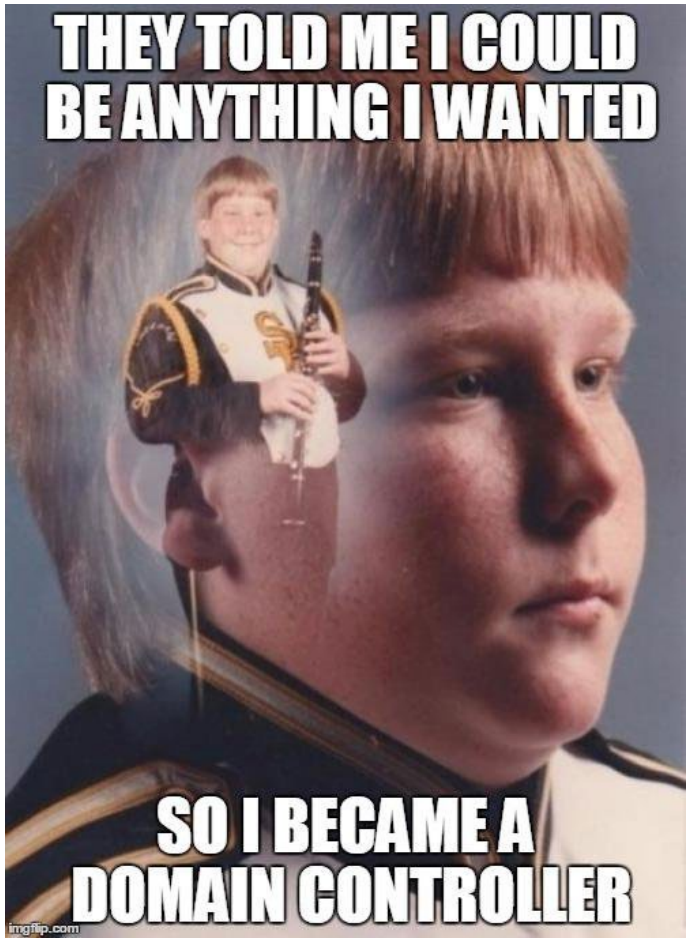
Stopping Lateral Movement

- Microsoft LAPS: https://gallery.technet.microsoft.com/Step-by-Step-Deploy-Local-7c9ef772/file/150657/1/Step%20by%20Step%20Guide%20to%20Deploy%20Microsoft%20LAPS.pdf
- Disable remote local admin access: https://blogs.technet.microsoft.com/secguide/2014/09/02/blocking-remote-use-of-local-accounts/
- Enable Windows firewall: https://medium.com/think-stack/preventing-lateral-movement-using-network-access-groups-7e8d539a9029

Source: https://redcanary.com/wp-content/uploads/image4-13.png

Other Active Directory Issues to Watch For

- ❑ Trusts
- ❑ DCSync/DCShadow
- ❑ Password policy
- ❑ Lack of admin/user separation



Source: https://user-images.githubusercontent.com/2307945/35466403-d9a4f3f2-0303-11e8-9d94-a2e4b2df7a2c.jpg

Takeaways

- ❑ We are all trying, we can’t just flip a switch and be secure
- ❑ Making money and staying in business is more important than security
- ❑ Security in small steps instead of big leaps

Source: https://memegenerator.net/img/instances/72354755.jpg

Who Wants a Job?

- Looking for penetration testers/developers

- Contact me:
  - Twitter: @justinforbes
  - https://www.linkedin.com/in/justinforbes/
  - jforbes@cert.org
  - Pittsec Slack: jforbes
  - In the vendor area after this talk

Source: https://i.kym-cdn.com/photos/images/original/001/066/150/255.jpg

I Like to Talk About Security

- ❑ I like talking about every aspect of security
- ❑ Contact me:
  - Twitter: @justinforbes
  - https://www.linkedin.com/in/justinforbes/
  - jforbes@cert.org
  - Pittsec Slack: jforbes
  - In the CTF area in five minutes
- ❑ Lets get a drink later

Source: https://memeshappen.com/media/created/2018/04/HEY-LETS-TALK.jpg

Thank You For Your Time

Source: https://media1.giphy.com/media/FnGJfc18tDDHy/giphy.gif