

How to Frustrate a Penetration Tester

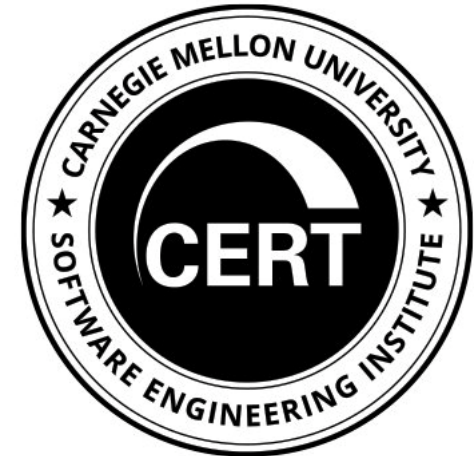
Justin Forbes

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

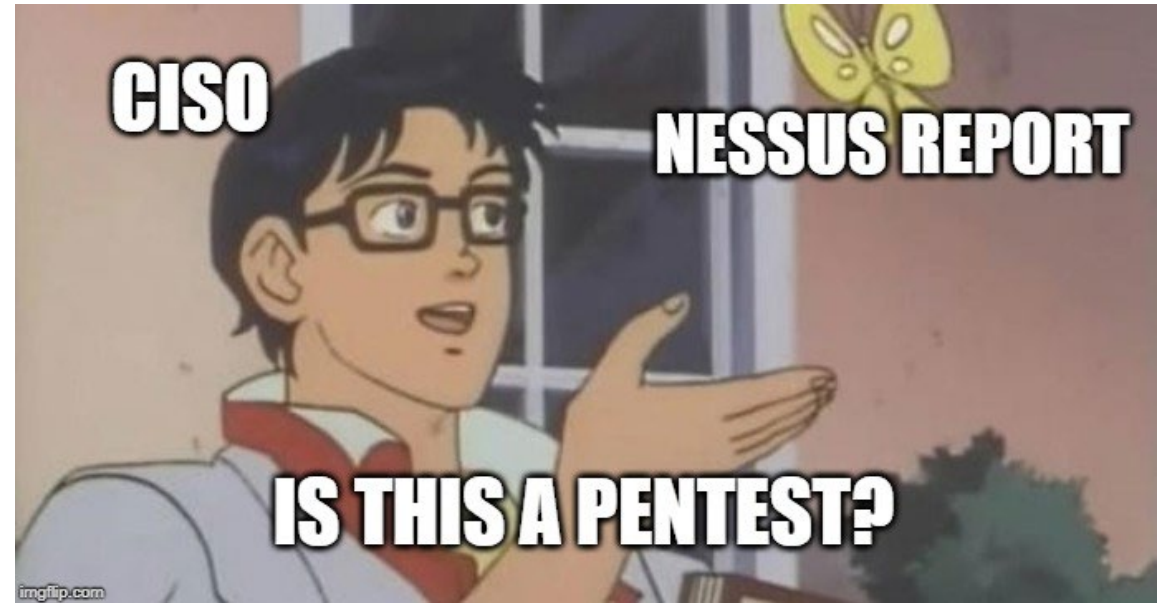
Who am I?

- ❑ 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



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



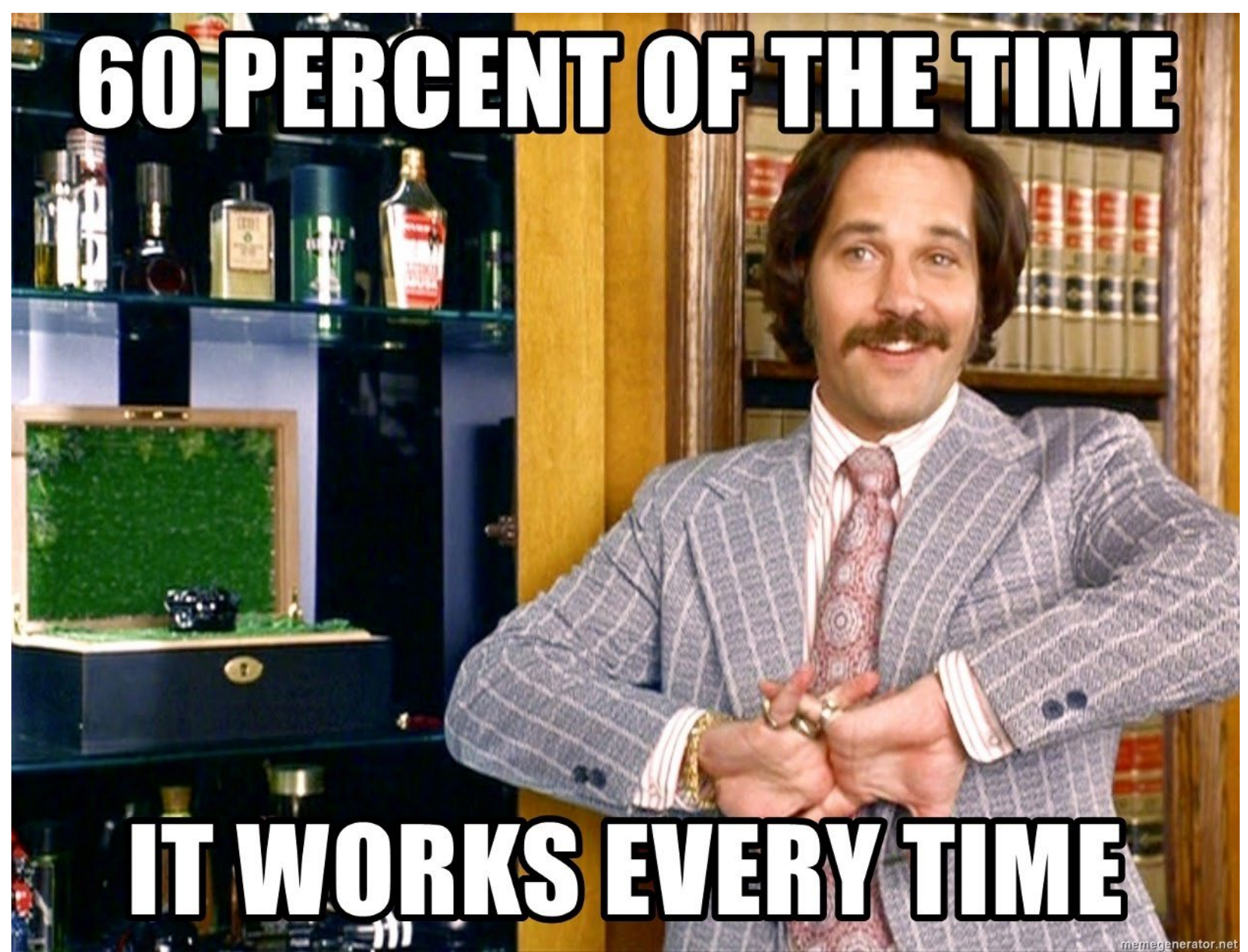
Source: <https://www.memecreator.org/static/images/memes/4647173.jpg>

How Does It Happen?

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

How to Frustrate a Penetration Tester

Phishing



Source: https://cdn-images-1.medium.com/max/1250/1*bEhPyKq9ckEHMrJIUm8xNg.jpeg

Two Main Goals of Phishing Emails

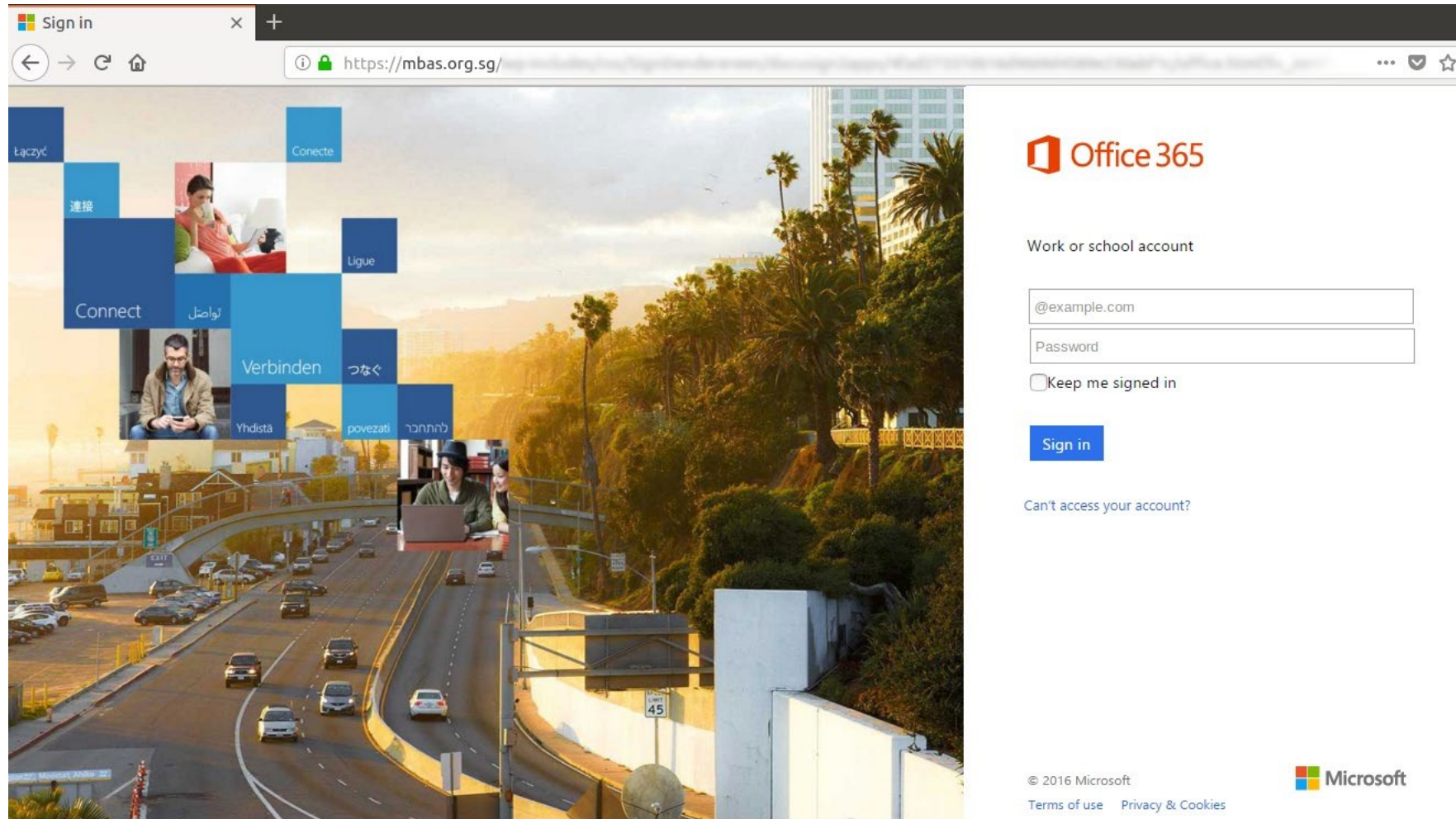
❑ Phishing for credentials

- 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/-1c4ljejrSE/W9vDlxt0dcl/AAAAAAAAeZ4/3cobNyEarKYrPeEOTZ2MhavANBQQ_dQUACKgBGAs/s640/how-i-felt-when-reddit-kept-telling-me-to-change-my-password-104581.jpg

Delivering a Payload

Social Media Policy Update Inbox x



Jim Thompson <jim.thompson@[REDACTED]>
to me ▾

Tue, Jun 18, 12:04 PM (7 days ago)



Attention All Personnel:

Social media is an important tool that we use to communicate directly with our customers. This communication allows us to provide immediate information to our customers while providing us with valuable feedback and marketing information. Additionally, we can use this feedback to measure our overall reputation in the market. Given the importance and impact that social media can have, the Human Resources department has updated the Social Media Policy for our organization. All employees within the organization, regardless of position, will be expected to follow the guidelines and rules of behavior detailed within the Social Media Policy moving forward.

To view the policy, please visit the following link:

[Social Media Policy 2019](#)

 Reply

 Forward

Payloads

❑ Common Payloads:

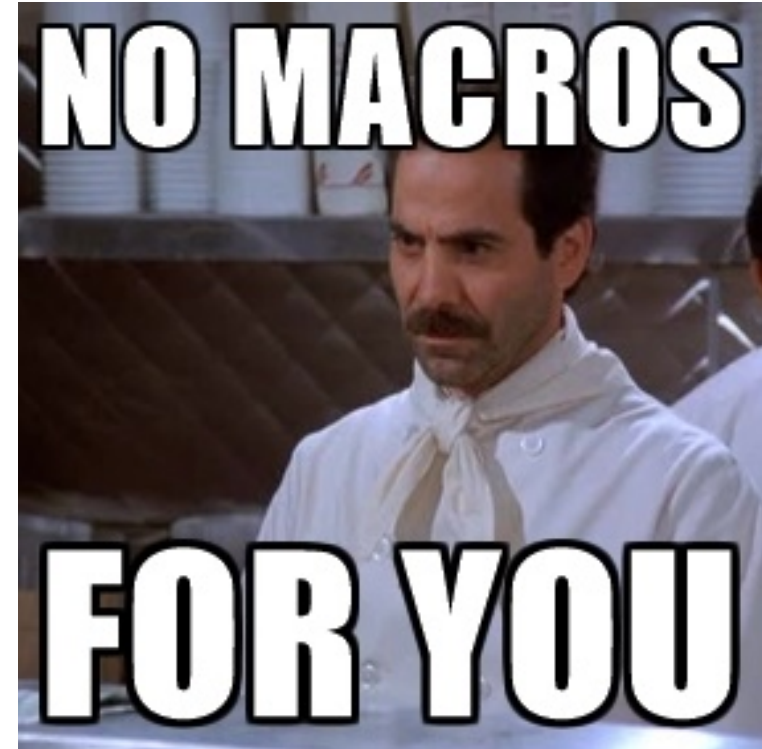
- Office Macros
- HTML Applications (HTA)
- regsrv32
- Living Off The Land Binaries and Scripts: <https://lolbas-project.github.io/>



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

How to Frustrate a Penetration Tester

Lack of Cyber Hygiene



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

CIS Controls



V7

Basic

- 1 Inventory and Control of Hardware Assets
- 2 Inventory and Control of Software Assets
- 3 Continuous Vulnerability Management
- 4 Controlled Use of Administrative Privileges
- 5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
- 6 Maintenance, Monitoring and Analysis of Audit Logs

Foundational

- 7 Email and Web Browser Protections
- 8 Malware Defenses
- 9 Limitation and Control of Network Ports, Protocols, and Services
- 10 Data Recovery Capabilities
- 11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
- 12 Boundary Defense
- 13 Data Protection
- 14 Controlled Access Based on the Need to Know
- 15 Wireless Access Control
- 16 Account Monitoring and Control

Organizational

- 17 Implement a Security Awareness and Training Program
- 18 Application Software Security
- 19 Incident Response and Management
- 20 Penetration Tests and Red Team Exercises

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

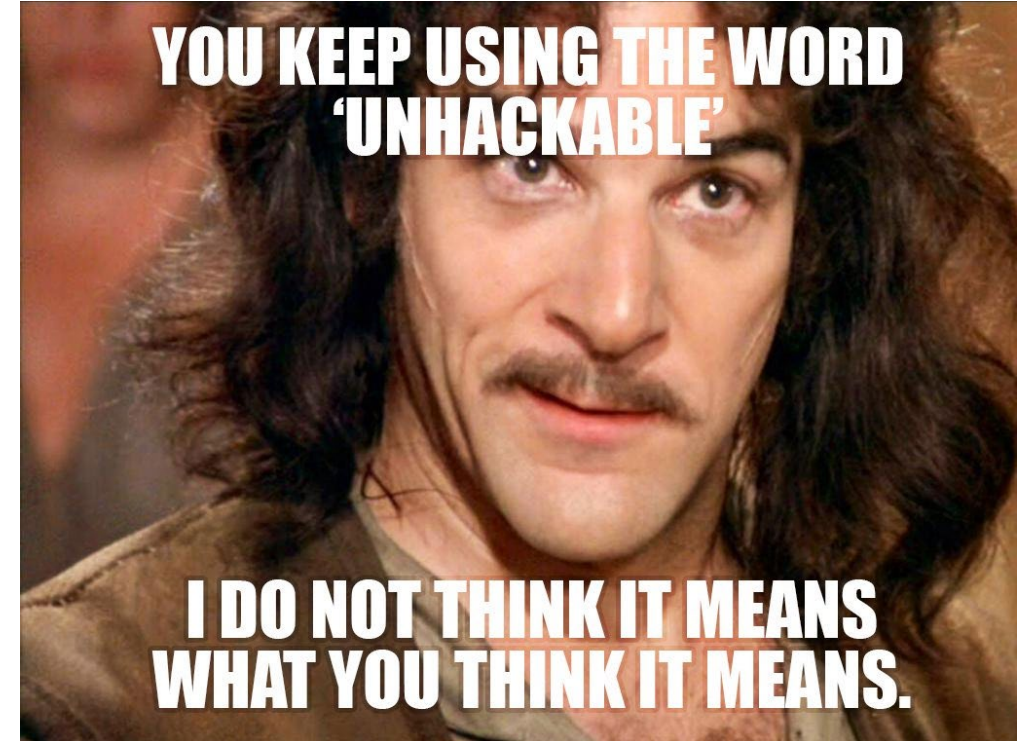
- ❑ Patching continues to be a struggle for many organizations
- ❑ Patching extends beyond just the Windows world
- ❑ “Too big to patch”
- ❑ Patch what you can and isolate the rest



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>

How to Frustrate a Penetration Tester

Password Hashes



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

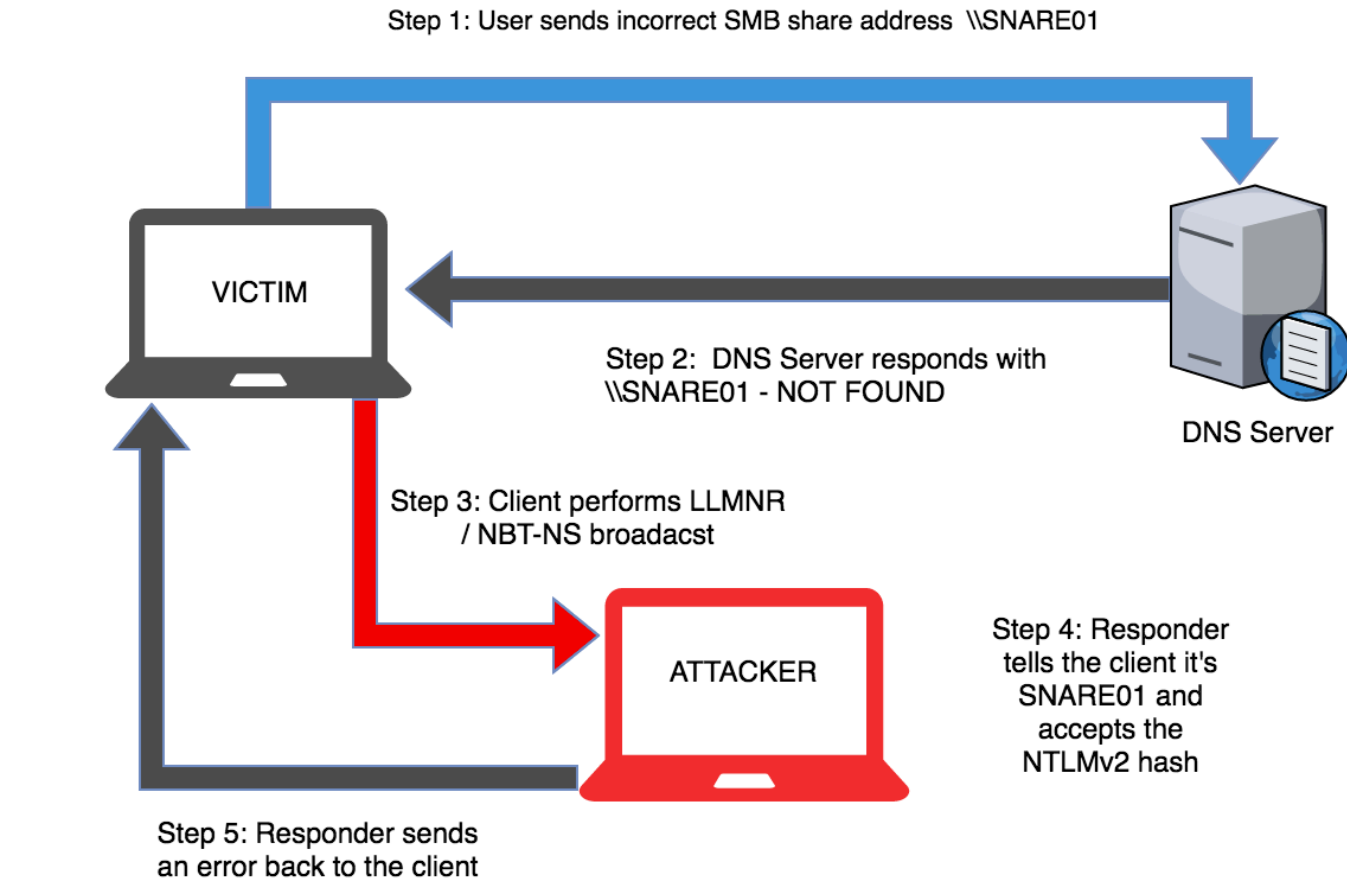
Tools I Use

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

```
[i] Responder is in analyze mode. No NBT-NS, LLMNR, MDNS requests will be poisoned.
[Analyze mode: ICMP] You can ICMP Redirect on this network.
[Analyze mode: ICMP] This workstation (10.0.0.2) is not on the same subnet than the DNS server (192.168.238.2).
[Analyze mode: ICMP] Use `python tools/Icmp-Redirect.py` for more details.
[+] Listening for events...
[Analyze mode: NBT-NS] Request by 10.0.0.3 for PENTESTLAB, ignoring
[Analyze mode: NBT-NS] Request by 10.0.0.3 for PENTESTLAB, ignoring
[Analyze mode: NBT-NS] Request by 10.0.0.3 for PENTESTLAB, ignoring
[SMBv2] NTLMv2-SSP Client      : 10.0.0.3
[SMBv2] NTLMv2-SSP Username   : PENTESTLAB\test
[SMBv2] NTLMv2-SSP Hash       : test::PENTESTLAB:21d9c06030a3d870:1BE458C561BAE5DE
B53554A3986048E2:0101000000000000C0653150DE09D20190854080BD74ACF4000000000200080
053004D004200330001001E00570049004E002D00500052004800340039003200520051004100460
056000400140053004D00420033002E006C006F00630061006C0003003400570049004E002D00500
052004800340039003200520051004100460056002E0053004D00420033002E006C006F006300610
06C000500140053004D00420033002E006C006F00630061006C0007000800C0653150DE09D201060
004000200000000800300030000000000000000000000000000000000000000000000000000000
A192FF600F91653F1C99AC5044FE8F17B844C0A001000000000000000000000000000000000000
01A0063006900660073002F00310030002E0030002E0030002E003200000000000000000000000
0
```

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

Basic Attack



Source: <https://www.voidwarranties.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>

How to Frustrate a Penetration Tester

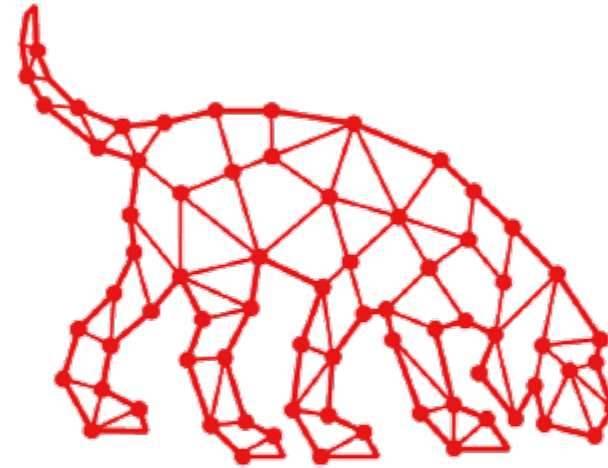
Active Directory Misconfigurations



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

Tools I Use

- ☐ Bloodhound
- ☐ PowerSploit
- ☐ CrackMapExec



BLOODHOUND

Source:

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

Users With Local Admin Rights

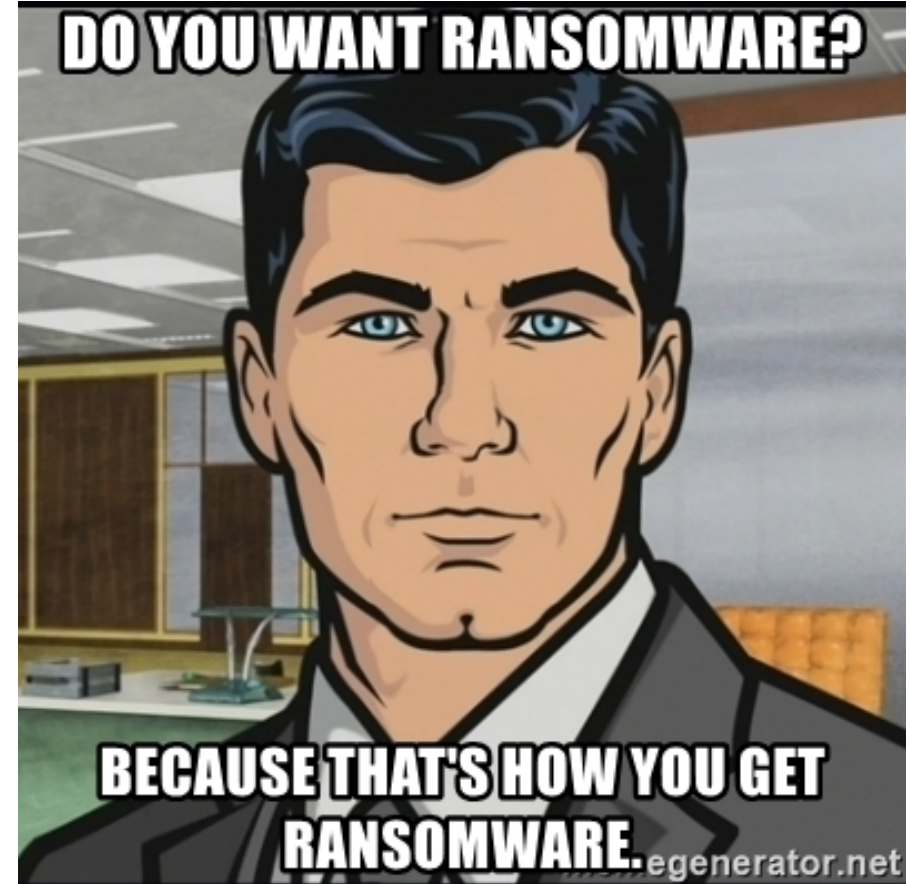
- ❑ Just browsing a malicious website or opening a phishing email means full system compromise, no privesc needed
- ❑ Figure out why the users need local admin and fix it



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>



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>

How to Frustrate a Penetration Tester

Thank You For Your Time



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