# Top 10 Things That Make a Hacker's Life Easy

CliftonLarsonAllen

CLAconnect.com

# Intro/Summary

1. I am going to share with you:
    1. Day to day experiences doing vulnerability assessments
    2. “Top 10 things” that make it easy (easier?) for hackers
    3. New/emerging vulnerabilities exploited by hackers
    4. Key defensive strategies to mitigate risks

# 10 things that make it easy for hackers

1. Giving users local admin privileges
2. Domain Admins don’t have separate user account
3. Domain Admins log into workstation
4. Weak passwords
5. Shared passwords

# 10 things that make it easy for hackers

6. Poor patching
7. Unnecessary ports and services
8. Weak/no encryption
9. Vendor Systems
10. Lack of security awareness

# Latest Trends/The New Hotness

- New methods on bypassing anti-virus
- Relaying network credentials (SMB or HTTP)
- Utilizing PowerShell to hack systems
- Using Mimikatz to steal clear text credentials
- Kerberos “Golden Ticket”

# Bypassing AV

Easy as 1-2-3….

# New Ways to Bypass AV

- Multiple tools available
- Free, open source
- Easy to use
- Can generate a new, totally unique payload that bypasses a majority of AV's in seconds
- We've been using it on EPTs over the last year with great success

# New Ways to Bypass AV

- Veil-Evasion
  - https://www.veil-framework.com/
- Crypter.py
  - Google search, proceed with caution

# How to protect yourself

- Strict egress filtering
  - Utilize whitelisting instead of blacklisting
- Whitelist applications
- Utilize proxy
  - SSL stripping

# Relaying creds

Yes, I am the host you're looking for…

# Relaying network creds

- Attacks Windows Single Sign-On
- Starts by spoofing NetBIOS traffic
- Tricks computer into attempting to authenticate to the attacker
- The computer automatically sends encrypted credentials to attacker
- Attacker relays the credentials to other target

# Relaying network creds

- SMB or HTTP
- Can be used to authenticate to alternate system or run malicious code on alternate system

# How to protect yourself

- Enforce SMB Signing
  - http://support.microsoft.com/kb/887429
  - http://technet.microsoft.com/en-us/library/cc731957.aspx

# PowerShell

That’s one powerful shell…

# PowerShell

- Windows scripting environment built on .NET
- Comes pre-installed
  - Attackers don’t have to worry about AV
- Able to perform many different tasks that command prompt couldn’t

# PowerShell

- Search for systems where you have local administrator access
- Search for where domain administrators are logged in
- Can download items from a URL
- Can inject malicious code straight into memory

# How to protect yourself

- Disable PowerShell if not used in your environment
- Microsoft EMET
  - http://support.microsoft.com/kb/2458544

# Mimikatz

I can see your password :)

# Mimikatz

- Windows stores your clear text password in memory when you log in
- Mimikatz can extract those clear text passwords from memory
- Need admin privileges on the host

# How to protect yourself

- Protect systems from malware
- Restrict admin access to systems

# Golden Ticket

Full access….forever

# Kerberos Golden Ticket

- Kerberos is an authentication protocol for Windows Active Directory environments
  - If you successfully authenticate, you are granted a “ticket”
- If your domain gets compromised, an attacker can steal the information needed to create “tickets”
- An attacker can create fake “golden tickets” that allow access to everything, even if everyone changes their password

# How to protect yourself

- Protect systems from malware
- Restrict admin access to systems
- Defense in depth/security layers

- If fully compromised, the krbtgt account password needs to be updated
  - Consult an expert

# DEMO