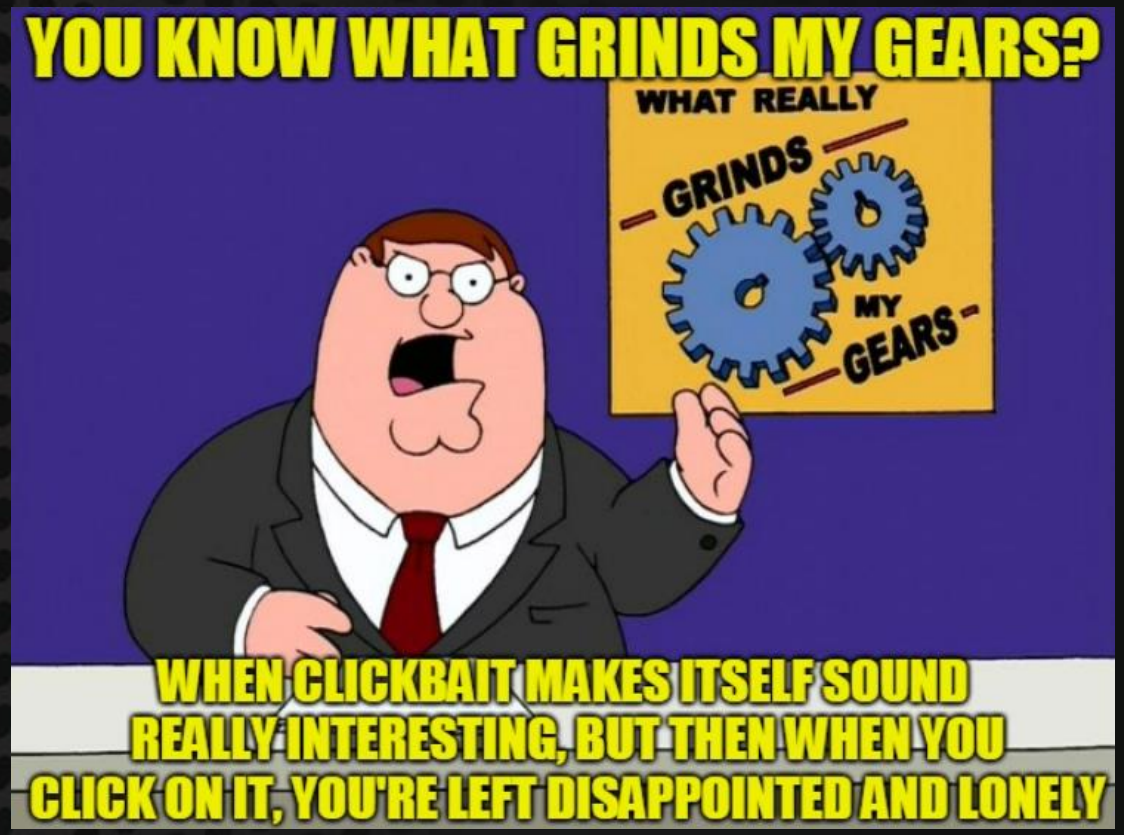
The Top $_num Reasons You Got Hacked in 2022

The answers should not shock you!



… adopting a prevention-first approach to cybersecurity is ultimately one of the best ways businesses can guard against malicious actors ….

@BHInfoSecurity

Hello! We Are Black Hills Information Security!

"Smart Install? more like Smart Intrusion" Jordan Drysdale

"PowerPoint Graphic Design is my Passion" Kent Ickler

Penetration Testers
Researchers
Educators

We think we are pretty decent people, just ask us.

@BHInfoSecurity

Executive Problem Statement

"Everyone keeps getting popped"
… are we next?
… have we already been compromised?
… would we know if we were?

Are our tools working?

- What are our tools?
- What can we detect?
- Which FTEs manage which tools?
- How can we test this?
- What are our gaps?
- What existing tools can fill them?
- What do we have to buy?
- Can we buy ourselves out of this problem?

What did we learn in 2022?

@BHInfoSecurity

2020's Top ExploitedCVEs

What is a CVE?

- A common vulnerability exploited *knowneningly*
- *Responsible Disclosure (CVEs are "public".. And "responsible")*

Or:
Common Vulnerabilities and Exposures
https://www.cve.org/

Sponsored by DHS & CISA

Table 1:Top Routinely Exploited CVEs in 2020

Vendor	CVE	Type
Citrix	CVE-2019-19781	arbitrary code execution
Pulse	CVE 2019-11510	arbitrary file reading
Fortinet	CVE 2018-13379	path traversal
F5- Big IP	CVE 2020-5902	remote code execution (RCE)
MobileIron	CVE 2020-15505	RCE
Microsoft	CVE-2017-11882	RCE
Atlassian	CVE-2019-11580	RCE
Drupal	CVE-2018-7600	RCE
Telerik	CVE 2019-18935	RCE
Microsoft	CVE-2019-0604	RCE
Microsoft	CVE-2020-0787	elevation of privilege
Microsoft	CVE-2020-1472	elevation of privilege

But why???

@BHInfoSecurity

2021's Top Exploited CVEs

Source: https://www.cisa.gov/uscert/ncas/alerts/aa21-209a

What changed?

- Not much, actually
- Long live Exchange!

(a gift that keeps giving)

But why???

Table 1: Top 15 Routinely Exploited Vulnerabilities in 2021

CVE	Vulnerability Name	Vendor and Product	Type
CVE-2021-44228	Log4Shell	Apache Log4j	Remote code execution (RCE)
CVE-2021-40539		Zoho ManageEngine AD SelfService Plus	RCE
CVE-2021-34523	ProxyShell	Microsoft Exchange Server	Elevation of privilege
CVE-2021-34473	ProxyShell	Microsoft Exchange Server	RCE
CVE-2021-31207	ProxyShell	Microsoft Exchange Server	Security feature bypass
CVE-2021-27065	ProxyLogon	Microsoft Exchange Server	RCE
CVE-2021-26858	ProxyLogon	Microsoft Exchange Server	RCE
CVE-2021-26857	ProxyLogon	Microsoft Exchange Server	RCE
CVE-2021-26855	ProxyLogon	Microsoft Exchange Server	RCE
CVE-2021-26084		Atlassian Confluence Server and Data Center	Arbitrary code execution
CVE-2021-21972		VMware vSphere Client	RCE
CVE-2020-1472	ZeroLogon	Microsoft Netlogon Remote Protocol (MS-NRPC)	Elevation of privilege
CVE-2020-0688		Microsoft Exchange Server	RCE
CVE-2019-11510		Pulse Secure Pulse Connect Secure	Arbitrary file reading
CVE-2018-13379		Fortinet FortiOS and FortiProxy	Path traversal

The Transition Slide

Something about scary Zero-Day Exploits destroying the network

Or… Hacker finding plaintext creds in SYSVOL

But why???

Hackers Though ...

What are we doing in 2022?

The same stuff we've been doing for years

- Using OSINT data to find targets
- Password spraying
- Socially engineering push notifications
- Phishing, albeit slightly different TTPs
- Weak protocol abuse
- Credential relay

- And some cool newish stuff
  - ADCS abuse
  - Coercion and forced auth

Investigation Methodology

John said we had to do this webcast or we'd be back in the coal bin.

CISA? We have our own empirical data.

- BHIS 2022 Q1-3 Engagement Analysis
  - In descending order of popularity:
    - Web application deep dives
    - External perspective, includes recon
    - Internal perspective
    - Assumed Compromise / Pivot
- Then, we started mining in our reports:
  - For each test type, alphabetically, what did we report?
  - What were the common themes?
  - We need an intern to help, there's so much to read.
- Lastly, we built this slide deck.
  - The remaining slides go in descending order

The Top 10 Reasons You Got Hacked in 2022

(Drumroll…)

@BHInfoSecurity

Number 10: Firewalls

...or.. lack of firewall policies, am I right?...

It's normal to find, crack, or escalate creds

But the **lack** of consistent firewall policy cost orgs big time:

- Facilitates easy lateral movement
- SMB Remote Procedure Calls – secrets please!?
  - Remote Registry start / stop consistently missed
- Your critical accounts running services stored in services.msc configuration?
  - Yeah, that's an escalatin'

27:05 - Scanning/Enumeration, Nmap SSH Brute "Find Open", Movement, Gaining Access

Gather 'round everyone, John's hacking again: https://www.youtube.com/watch?v=UuaVeJe1tsg

BLACK HILLS Information Security • 2008 •

Number 10: Fixing Your Firewall Problem

Let's call it 75%. It's more like 90%.

- 75% of network environments do not have consistent firewall rules for workstation and server firewalls
- Get a single pane of glass, whatever your vendor, they likely have one.
  - Windows? GPOs.
  - Audit your policies!
- Host Based Firewalls are free…ish and very effective.
- Network Segmentation
- Zero-Trust

Number 9: Message Integrity

LDAP Signing / Channel Binding / SMB Signing

It is easy to ignore SMB message integrity until it matters

- No signing enforcement by default – just DCs

LDAP signing is also not enforced by default

- DCs not validating source integrity allows the worst kind of machine in the middle attacks

DEMOS INDEX

PART 1

- 01 - Basic Responder
- 02 - Simple Relay (Local Admin SMB to SMB)
- 03 - Dump AD Information HTTP to LDAP (IPv6 Poisoning)
- 04 – Fake Machine Account Creation via DHCP Poisoning (HTTP to LDAP)
- 05 - SMB to SOCKS AD Users, Groups and Machine Accounts Dump (SOCKS)
- 06 - Domain Administrator Privilege Escalation NetNTLM v1
- 07 - Machine Account Admin to (Exchange Trusted Subsystem Group)
- 08 - Printer LDAP Pass Back Attack
- 09 - MSSQL Relay via XP_DIRTREE
- 10 - SCCM Client Push Installation
- 11 - Files That Coerce (SMB Share)

Gabriel would like a word with you:
https://www.youtube.com/watch?v=b0lLxLJKaRs

@BHInfoSecurity

BLACK HILLS Information Security • 2008 •

Number 9: Implementing Message Integrity

LDAP Signing / Channel Binding / SMB Signing

- these are off by default
- require effort but little maintenance
- generally only discussed ad nauseum by pentesters
- rarely discussed in the in-flight magazines (like BloodHound)
- have huge implications on overall security posture |----------|

Insecure ^ Fort Knox

Executives don't care, IT operations folks have enough on their plates, we are again at around 75% of domains have not enforced these things.

- https://techcommunity.microsoft.com/t5/storage-at-microsoft/configure-smb-signing-with-confidence/ba-p/2418102
- https://learn.microsoft.com/en-us/troubleshoot/windows-server/identity/enable-ldap-signing-in-windows-server
- https://support.microsoft.com/en-us/topic/2020-ldap-channel-binding-and-ldap-signing-requirements-for-windows-kb4520412-ef185fb8-00f7-167d-744c-f299a66fc00a
- https://www.youtube.com/watch?v=Y7RYbW1Tpsk

Story: When not to use SMB Signing.

@BHInfoSecurity

Number 8: Defaults

Cloud, On-Prem, Network, IoT, Firewall, et cetera

- Access to everything:
  - Lolbins: PowerShell, cmd, ISE, MSBuild, CSC, InstallUtil, Regsvr32, Rundll32
  - Azure Active Directory
  - ms-ds-machineaccountquota, add guest users to AAD, NBNS, LLMNR
  - open telnet, at least the ports are obscure, right?
  - insufficient egress filters, 445 outbound? Sure!

There were lots of findings with "default" in the titles:

- Vendor-supplied default credentials
- Cloud default misconfiguration
- Default configuration in AD allowed:
  - Pivot via addition of machine object
  - Relayed credentials
  - Escalation via certificate template
- Promiscuous egress network default configuration

Number 8: Defaults

Cloud, On-Prem, Network, IoT, Firewall, et cetera

- Are we allowed to discuss
  - Policies
  - Procedures
  - Standards
  - Guidelines
  - Baselines
  - Playbooks
  - Tabletops
  - Education
  - Programs
  - Resources
  - CapEx

These controls only function if they have teeth

Number 7: Patching

Common Findings Leading to Exploitation:

- Unpatched and Unsupported Software
- Vulnerable and Outdated Components

Not as concerning as it used to be:

- EDR products and AV are better at catching exploit code being shoveled into memory
- Harder to remotely exploit than it used to be

However, this: "prove it or its not vulnerable"

Is oh so very wrong

- Bright red vulnerability scan results happen for a reason
  - Usually, The org is failing to manage patching
  - And their patching policies have no teeth
  - No PoCs are assigned to products
  - Service contracts are rarely renewed

Number 6: Weak Protocol Abuse

Once access was gained, internal networks are often quite squishy, soft, and pliable

- Weak protocol abuse (SMI, NBNS, LLMNR, DTP, IPv6, WPAD, mDNS, SQL)
- Network and infrastructure gear accessible via reused passwords
- Failure to maintain service contracts

LLMNR is still relevant. Sadly.

- Auto-relay everything, everywhere.

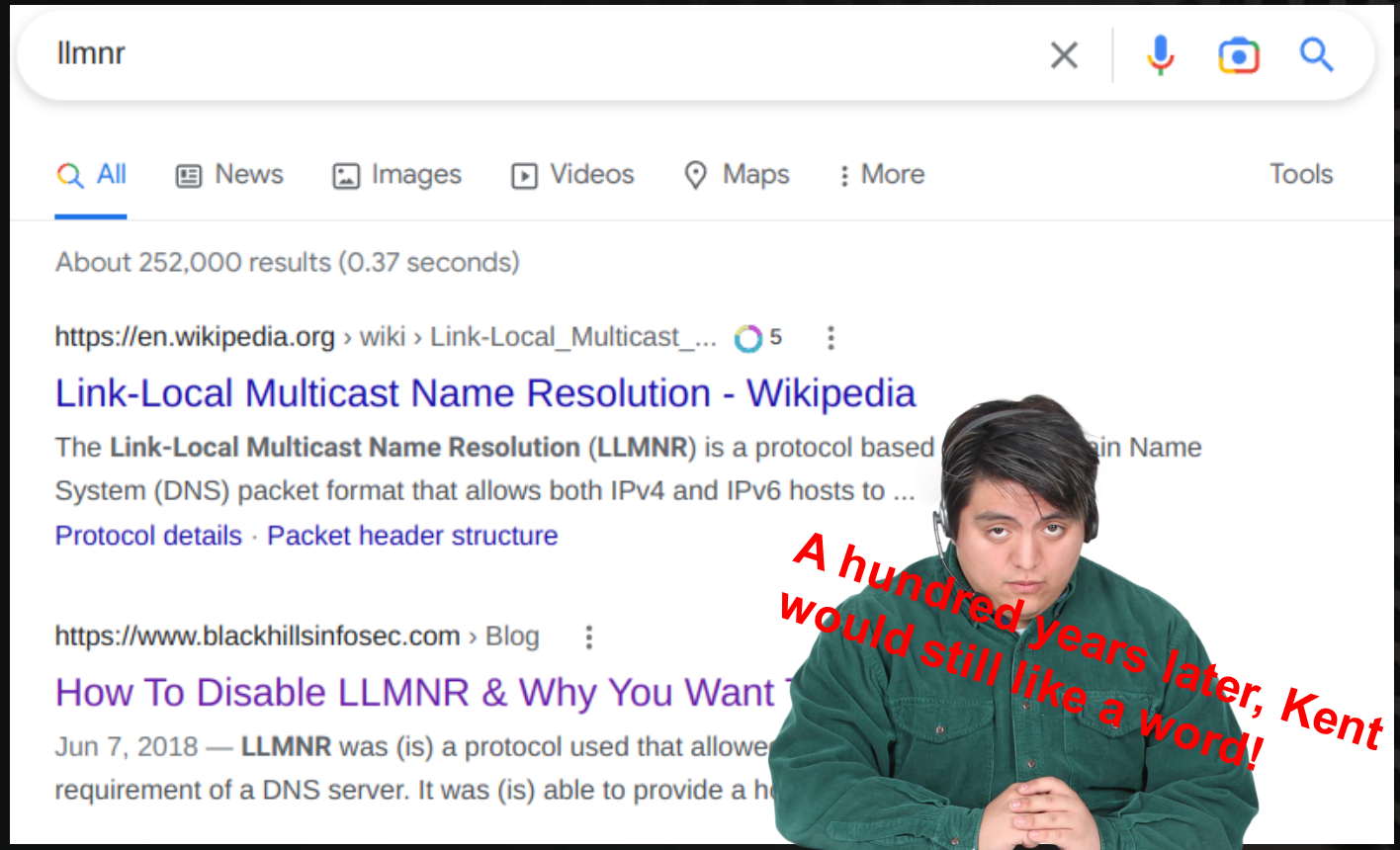
NBNS is still enabled by default

- All NICs on Windows OS

WPAD still nets us relayable creds

SQL browser still dumps cleartext

SMI still out there



Number 6: Weak Protocol Abuse

Solutions abound!

- Disable LLMNR, lol. This one is just comedy gold for us
  - The infinite and never-ending gift
- Disable NBNS - a bit more challenging, but you can do it!
  - Script it, re-run it often.

- Patch your switches and routers

- Be careful with your SQL configurations (and web.config)

- SNMP public … really?

Disable LLMNR and NBNS on workstations alone

Network Segmentation, Inspection & L2 Protocol Filtering (VLAN isolated broadcast and multicast traffic)

Technet referencing a script on StackOverflow
https://social.technet.microsoft.com/wiki/contents/articles/53228.powershell-disable-netbios-on-your-network-adapters.aspx

BLACK HILLS Information Security • 2008 •

Number 5: Web Apps

Open Web Application Security Project
https://owasp.org/

Input Validation Issues
- Cross-Site Scripting
- SQL Injection
- Formjacking
- Failure to validate client inputs server-side

Session Management
- Cross-Origin Resource Sharing (cors)
- Failure to invalidate session data server side

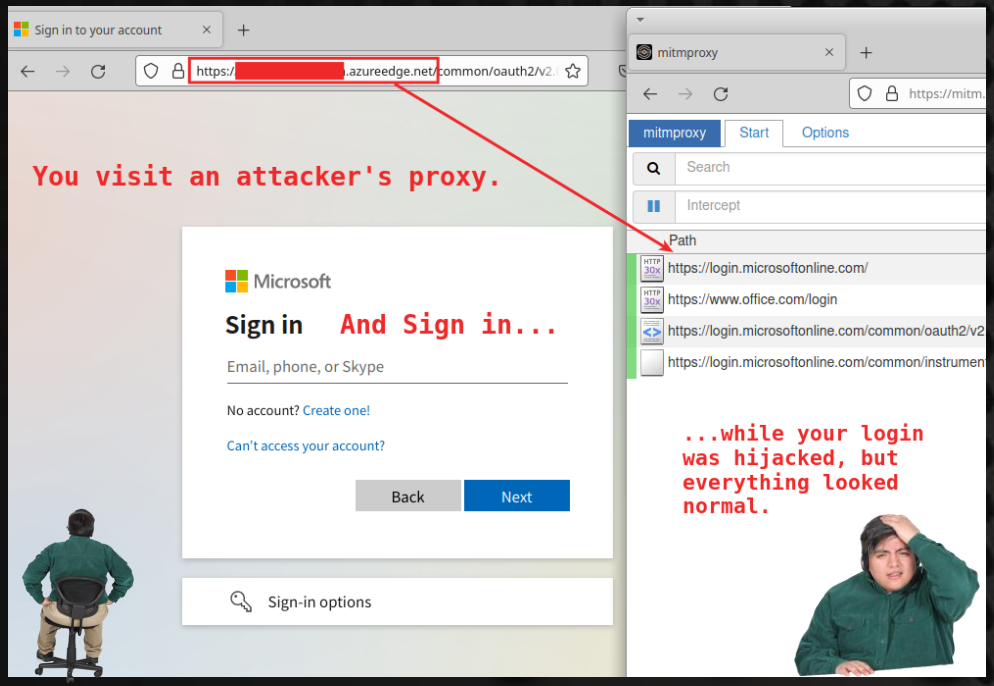
Legacy Code
- Bolting fixes on 20 year old ASP.net builds, yes **.NET is 20 years old**
- Developers leave, new ones put pieces together
- Disparate teams develop individual application components

Static Keys, Encryption, and Routines described in application .dlls
- Zero days are (and were) more common than we want to believe
  - Some end up buried under the weight of NDAs :/

Number 4: Employees

Social engineering continued to cause headaches across all industry verticals and horizontals

- SE calls are (almost never) fun.
  - But on occasion resulted in credentialed access or access to PII
- MFA Pushes
- Phishing still works, and is a bit more sinister
- Credential phishing can be quite stealthy (see screenshot)
  - Only takes one
- Seasonal Year Password Disorder (Winter2022!)
  - Made the DSM-5, finally
  - Might as well be a ratified protocol at this point
- Leaving passwords lying around the network
  - Snaffler @rhino's parser was widely used
  - {var}passwords.xlsx showed up many times
  - Hardcoded Creds in .net DLLs/EXEs on SYSVOL?
- Sharing out local drives with personal files
  - Way too common



Number 3: Optics (Lack Thereof)

Threat optics sliding scale:

- Blind <----------> Red-Tailed Hawk
- Let's be honest:
  - Most orgs that afford thorough pentests have optics
  - Many rely on third-party operators for optics
    - **WHO WATCHES THE WATCHERS**?
  - Has your org tested your watchers?

IBM investigations claim data breaches look like this:

- $9M average in the US
- ~200 days to detection
  - Another ~90 days to containment
- Empirically, orgs are failing to detect most pentest activities
  - PowerShell and CMD are heavily instrumented now … but Cobalt Strike?

But why???

https://www.ibm.com/reports/data-breach
https://www.varonis.com/blog/data-breach-statistics

Number 2: ADCS

ADCS has become a go to TTP for security analysts and adversaries

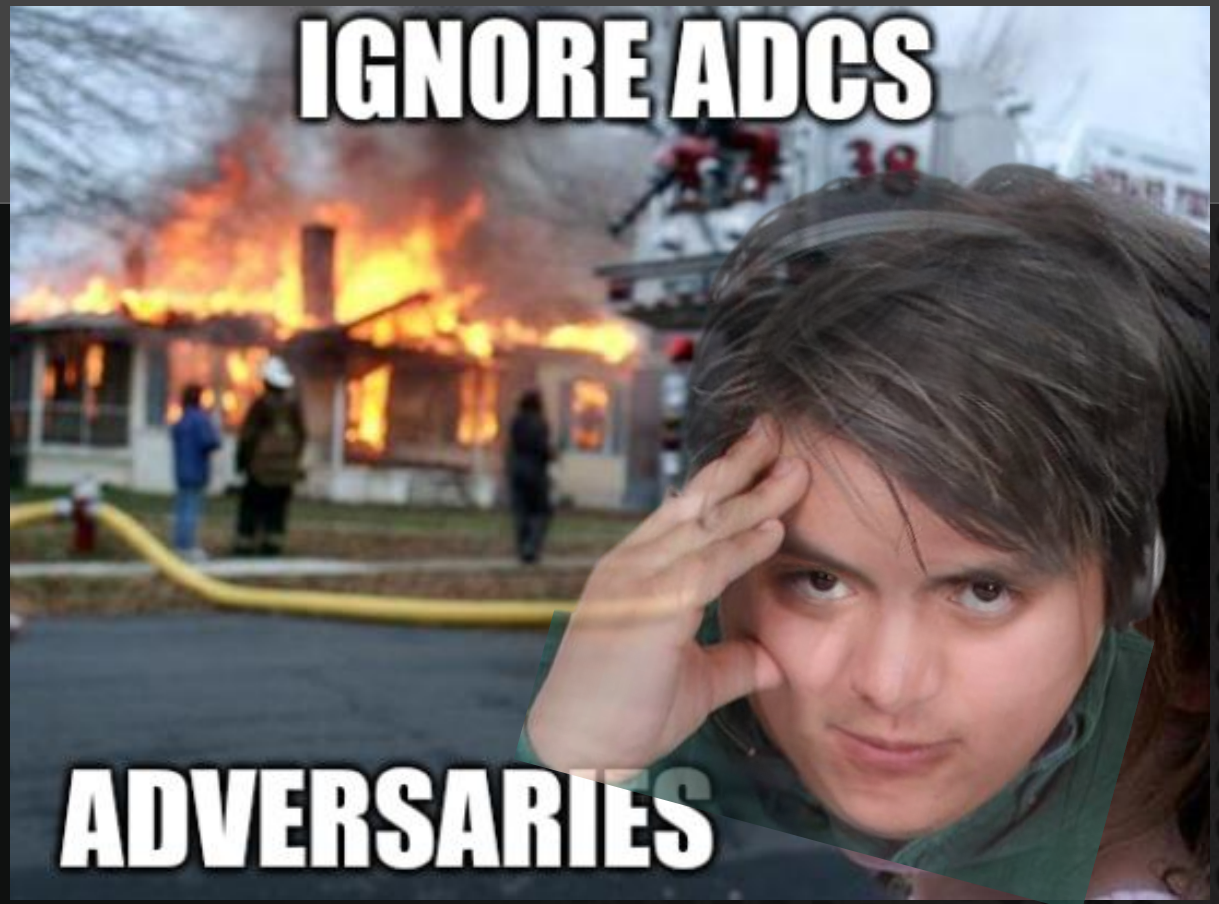
- Front of queue
- Early adversary check
- Easy check, Python? use Certipy. PowerShell? use Certify
  - find /vulnerable

The white paper:
https://specterops.io/wp-content/uploads/sites/3/2022/06/Certified_Pre-Owned.pdf

ADCS resulted in a lot of critical and high findings through Q3 at BHIS

- These findings *seem to be* escalating in consistency
  - Exploited early in tests, and let's say 9/10 for successful escalation
  - Escalating in knowledge … better documentation, tooling, etc

Number 2: ADCS



Clean these things up.

Know your tools:

- https://github.com/ly4k/Certipy
- https://github.com/GhostPack/Certify

Find vulnerable templates!

Clean up vulnerable templates.

Or you will likely go down in flames.

The Number 1 Reason You Got Hacked in 2022

(Drumroll…)

@BHInfoSecurity

Number 1: Credentials

These are Access Breaches

- Mike Felch once told me "creds are king" and he was right – credentialed access rules the day
- When we guess or crack passwords and write up "Weak Password Policy" what we mean is:

Someone else will compromise your passwords and gain access to your $_exposure with weak credentials.

16	weak password policy	M	insurance	1000 - 5000
30	weak password policy	M	finance	200 - 500
49	weak password policy	H	finance	500 - 1000
75	weak password policy	M	manufacturing	200 - 500
99	weak password policy	M	electronics	50 - 200
103	weak password policy	H	manufacturing	1000 - 5000
107	weak password policy	M	manufacturing	1000 - 5000
128	weak password policy	M	utilities	1000 - 5000
162	weak password policy	M	manufacturing	20000 - 25000
185	weak password policy	M	technology	500 - 1000
236	weak password policy	H	media	500 - 1000
268	weak password policy	M	finance	50 - 200
274	weak password policy	M	finance	50 - 200
313	weak password policy	L	education	1000 - 5000
327	weak password policy	L	online	1000 - 5000
59	weak passwords in use	L	finance	500 - 1000

Number 1: Credentials

Every BHIS a la carte contract type has a "credential related finding" in play for 2022:
Weak Password Policy
Credential Stuffing
Cleartext Credentials in *Shares, Source Code, on Desks*

But WHY?

- Web Apps
  - Our customers struggle with long passwords
- Domain
  - We don't have the political capital to get past 10 characters minimum length
- Source code
  - We got MVP without security testing!
- Wireless
  - We give the guest network key out at the front desk
- File Shares
  - We haven't had the capital resources to scrub our shares yet

The Top 10 Reasons You Got Hacked in 2022

Firewalls	10	Deploy and manage
Message Integrity	9	Enforce Signing
Default Configurations	8	Manage Configurations
Patching	7	Patch Management
Protocol Abuse	6	Harden Protocols
WebApps	5	OWASP Practices
Employees	4	Security Awareness
Weak Optics	3	EDR & SIEM
AD Certificate Services	2	Configure and Manage
Credentials	1	Longer Passwords

AND HOW TO PREVENT IT IN 2023

BLACK HILLS
Information Security
• 2008 •

Next Class: December 13-16, 2022

https://www.antisyphontraining.com/applied-purple-teaming-w-kent-ickler-and-jordan-drysdale/

https://www.blackhillsinfosec.com/

https://www.antisyphontraining.com/

https://www.activecountermeasures.com/

https://wildwesthackinfest.com/

https://defensiveorigins.com/

@BHInfoSecurity