



# Attack Detect Defend

## Part Two: Defenses, Detects, & Demo

ADD Presented By:

Antisyphon Training, Black Hills Information Security, Defensive  
Origins, Nebraska Cyber Security Conference

<https://necsc24.d4in.com/>

# Jordan & Kent



- Penetration Testers
- Curriculum Developers
- Internal and External Penetration Product Leads
- Knowledge Curators
- Degrees, Certifications and things



© Black Hills Information Security  
@BHInfoSecurity



# Executive Problem Statement II



- Our team needs an improved methodology for building detections and better defenses.



Can we buy our way to safety?

How many mega-breaches will there be this year?

Are we catching modern adversarial TTPs?

How do we keep up with escalating risks?

# Information Leakage via Data Breach Defenses



## DEFENSE

- Provide your employees an enterprise password management solution.
- Don't mix home and work.
- Recon & hunt: register your domain at <https://haveibeenpwned.com/>
- Policy: Define allowable services for your mail domains
- Strong Password Policy
- Use password filter lists: <https://learn.microsoft.com/en-us/entra/identity/authentication/concept-password-ban-bad-on-premises>



© Black Hills Information Security  
@BHInfoSecurity

© Black Hills Information Security  
@BHInfoSecurity

# Audit Policies That Pay The Bills!

ADCS: PKI is not audited by default - Event IDs 4886 + 4887

Kerberos ticket operations - Event IDs 4768 + 4769

DS Access: BloodHound, AD Enumeration - (Event ID 4662)

- And monitor for specific object GUIDs

PowerShell and CMD Event IDs 4688, 4103-4105, and Sysmon

Cloud? Yeah...you probably should ingest CloudTrail

EDR / AV / Firewall events: Event ID 4950

Terminal Services

DNS Events and WMI Invocation and Executions

DEFENSE



© Black Hills Information Security  
@BHInfoSecurity

© Black Hills Information Security  
@BHInfoSecurity



# Weak Password Policy

Use password filter lists: <https://learn.microsoft.com/en-us/entra/identity/authentication/concept-password-ban-bad-on-premises>

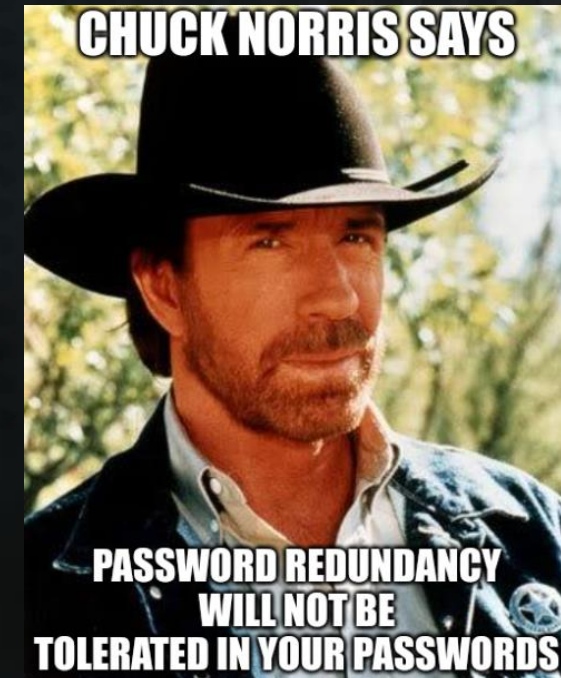
## Professional Advice

Help security avoid cultural friction.  
Support your security professionals.  
Implement a stronger password policy.  
Implement a Privileged Access Manager (PAM).  
Use password filter tools.

## Personal Advice

Since almost everything you've been taught is wrong, try this instead.

- Get a password manager, BitWarden is fine.
- Stop reusing passwords.
- Learn to use phrases.
- Stop reusing passwords.
- Freeze your credit file.
- Stop reusing passwords.



DEFENSE



© Black Hills Information Security  
@BHInfoSecurity

© Black Hills Information Security  
@BHInfoSecurity

# Unpatched Software and Web App Components

Policy: **Easy** → Enforce patching standards.

Procedure: **Medium** → Improve inventory controls.

Program: **Hard** → Assign a point of contact to all systems and exposed services

- All acquisitions are processed according to inventory control documentation
  - Point of contact is assigned
  - Systems are patched, vendor passwords are rotated
  - Warranty is registered to point of contact or ticket-creation mailbox
  - Notifications of patch availability from vendors is high priority

DEFENSE

**unpatched**

*/ʌn'pætft/*

adjective

Missing updates or lacking vendor support.



© Black Hills Information Security  
@BHInfoSecurity

© Black Hills Information Security  
@BHInfoSecurity

# SMB/LDAP Signing



DEFENSE

SMB Signing is simple to configure and enforce with Group Policy.

We have been warned against saying, “It is easy to fix \_\_\_\_\_.”

Configuring LDAP signing is a bit more nuanced. Channel binding too.

Strategy?

- Configure it once (set it) and you shouldn't have to think about it again (forget it).
- Limit other opportunities for adversaries to get your credentials in transit.
  - Microsoft File Server Resource Manager (no LNK / URL / SCR / CPL files allowed)
  - Limit LLMNR, NBNS, and WPAD broadcasts
  - Set a WPAD record in your DNS
- Call your rep and demand answers.
- Keep learning.

**signing**

*/ˈsaɪnɪŋ/*

noun

Validation of authentication traffic sources at their destination. Can invalidate relay attacks.



© Black Hills Information Security  
@BHInfoSecurity

© Black Hills Information Security  
@BHInfoSecurity



# Lack of MFA on External Systems



DEFENSE

If we honestly expect the hacking game to even start to slow down, we are going to have to take some responsibility here.

Inventory controls.

- Know your surface.
- Reduce your surface to as little as possible.
- Enforce MFA on everything.

## Multi-factor

*/mʌltɪ 'fæktə/*  
adjective

Enforcing credentialed access.

- Something you know.
- Something you have.



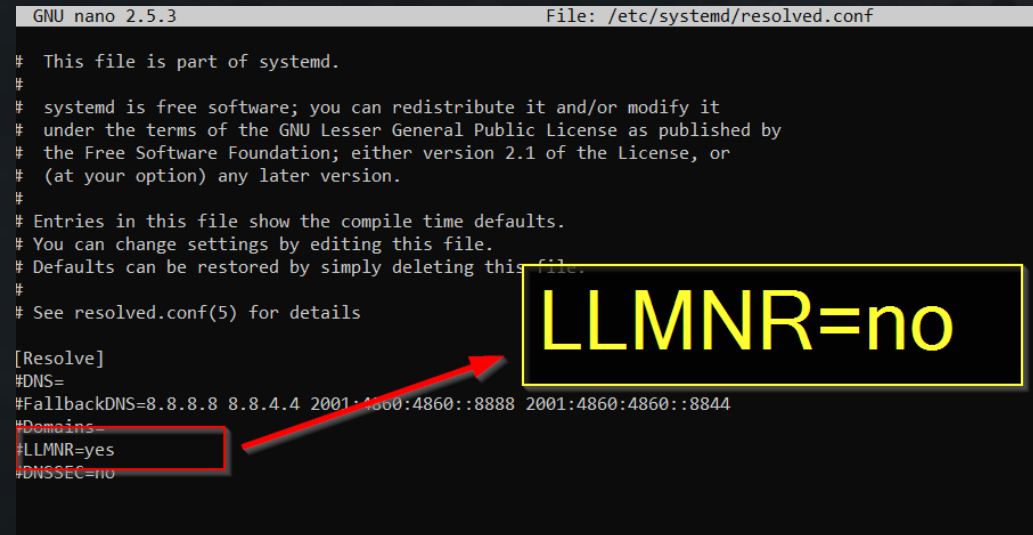
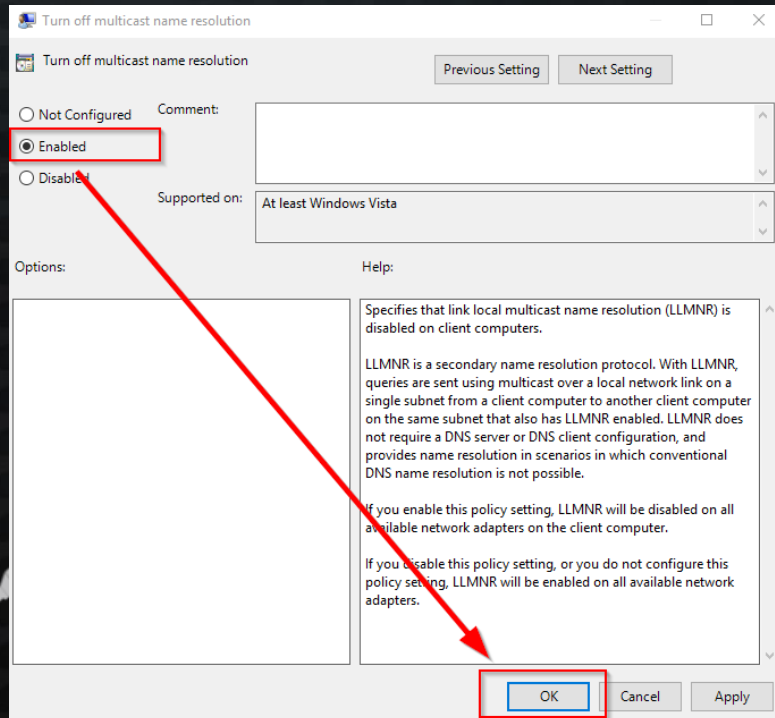
© Black Hills Information Security  
@BHInfoSecurity

© Black Hills Information Security  
@BHInfoSecurity

# Multicast and NBNS Poisoning

Some configuration is necessary.

- You can disable LLMNR with Group Policy.
- Disabling NBNS can be accomplished with PowerShell.
- Create a WPAD entry in DNS.



**poison**

*/ˈpɔɪz(ə)n/*

verb

To exert a baneful influence

DEFENSE

# Coercion and Forced Authentication

- East/West traffic inspection
- Firewalls:
  - Workstations? Yes!
  - Servers? Yes ... but !!!

| MITRE   ATT&CK®                    |                        |   |
|------------------------------------|------------------------|---|
| TECHNIQUES                         |                        | Mitigations   |
| Stores                             |                        |   |
| Exploitation for Credential Access |                        |   |
| Forced Authentication              |                        |   |
| Forge Web Credentials              | ▼                      |   |
| Input Capture                      | ▼                      |   |
| Modify Authentication Process      | ▼                      |   |
| ID                                 | Mitigation             | Description   |
| M1037                              | Filter Network Traffic | Block SMB traffic from exiting protocol traffic from exiting allowlisting. [12] [7] |
| M1027                              | Password Policies      | Use strong passwords to in  |

Sadly, coercion is more of a feature than a vulnerability.

Coercion is also often used as part of a chained attack...

- ...and downstream message integrity checks can reduce impact

DEFENSE

**coerce**

/koʊˈɜːs/

verb

To compel to an act or choice; to achieve by force.



© Black Hills Information Security  
@BHInfoSecurity


© Black Hills Information Security  
@BHInfoSecurity





## Audit certificate issuance.


- # ly4k/Certipy

Tool for Active Directory Certificate Services enumeration and abuse


 17

 86

 2k

 274

ContributorsUsed byStarsForks





/ˌsər'tɪfɪkət ɔ 'θɒrɪti/  
noun

© Black Hills Information Security  
@BHInfoSecurity

# Demo – Live Range



Azure Sentinel:  
Two Remote Desktop Exposures on Windows  
One SSH Listener on a Linux Server  
Attacker Attribution Lab



© Black Hills Information Security  
@BHInfoSecurity

# How Your Security Team

Reduced your external surface to ultra lockdown mode

Enrolled in breach monitoring

Updated your help desk procedures to enforce second factor validation

Tested your mail security, networks, domains, cloud, everything

Registered your appliances, hardware solutions, everything

Fixed default configurations. Improved password policies

## Prevented Compromise in 2024



© Black Hills Information Security  
@BHInfoSecurity

© Black Hills Information Security  
@BHInfoSecurity



# Questions?



- Next Generation
  - Advanced EDR
  - IDS/IPS/NGXFW
  - Machine learning
  - Artificial intelligence
  - Ransomewareness
  - Network Latent Threat
  - Advanced Persistent Threat
  - Generative AI
  - Blockchain
  - Delving into LLMs
- Black Hills Information Security
    - <http://www.blackhillsinfosec.com>
    - @BHInfoSecurity



© Black Hills Information Security  
@BHInfoSecurity