



# Attack Detect Defend

## Part One: Attacks & Demo

ADD Presented By:

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

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

**You are going to get hacked.  
It will not be over quickly.  
You will not enjoy it.  
Be prepared.**

John Strand



*How to Prepare Before the Compromise*  
<https://www.youtube.com/watch?v=V-3-RGsdqpM>







# tester a profile



**Kent, 40ish**



**Sr Penetration Tester**



**Ethics Instigator**



**Proponent of practical security testing**



**Curriculum developer and instructor**



**Tacit Knowledge Coordinator**



**Has degrees and things**



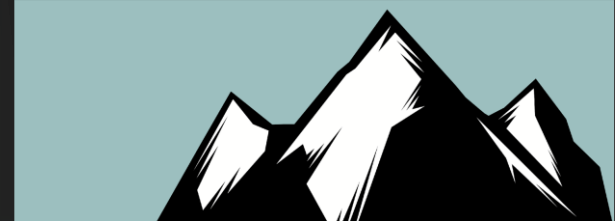
**Finishes slide decks at last minute**



© Black Hills Information Security  
@BHInfoSecurity



# tester a profile



519.7 Miles Away



Likes long walks through detailed methodologies



top blog post guy



Currently seeking:



CyberSec: Students not afraid to learn new things & write about it



CompSci: Python .net Go Rust



© Black Hills Information Security  
@BHInfoSecurity





# tester b profile



**Jordan**, feel 67, act 17, more like 47



Elder Penetration Tester



Quality Assurance team



Internal and External testing lead



Curriculum developer and instructor



Spreader of knowledge



Have taken certification tests



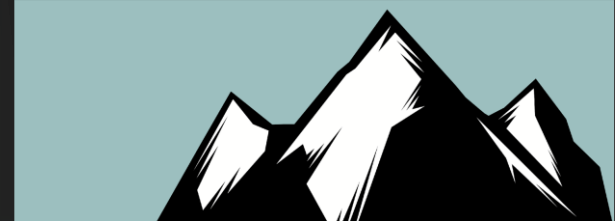
Have several hobbies



© Black Hills Information Security  
@BHInfoSecurity



# tester b profile



518.3 Miles Away



Prefer remote work and long, detailed reports



Let's solve some serious problems together :P



Currently seeking:



A safe online experience for all and a halt of the digital data dragnet



To stop being offered free credit monitoring



A zero-trust architected Internet backbone



© Black Hills Information Security  
@BHInfoSecurity



# Executive Problem Statement I

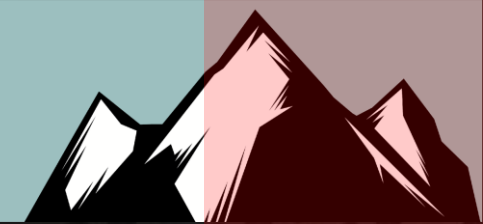


- Who are our adversaries?
- Do we have sufficient staff?
- Is there sufficient diversity of ideas in InfoSec?
- What should we do to protect:
  - Ourselves?
  - Our customers?
  - Our businesses?
  - Our identities?
- Are we getting good advice?
- Is our EDR going to take us down?



© Black Hills Information Security  
@BHInfoSecurity

# Demo – Live Range



ATTACK

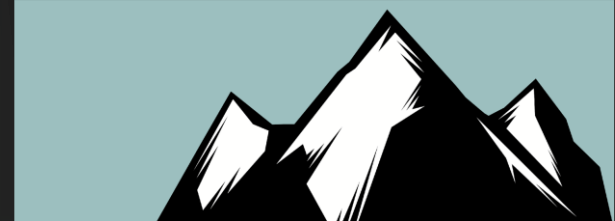
Azure Sentinel:  
Password Spray Attack Spike 1



© Black Hills Information Security  
@BHInfoSecurity



# Soooo.... we have a list to share.



- The list has already been shared.
- We curated about 750 report artifacts.
- We identified some trends.
- The results have analyst biases in them.
  - We report SSL and TLS findings, a lot.
  - However, those do not often result in compromise.
- Anyway, drum roll, the results are next....



© Black Hills Information Security  
@BHInfoSecurity

# Attack 1: Recon-Based Cred Things

This was our most common **LOW** priority finding. 170 instances.

- It usually looks like this.

23,578 hits

> he [REDACTED]@nebraska.gov	me [REDACTED]
> va [REDACTED]nebraska.gov	bi [REDACTED]
> je [REDACTED]@nebraska.gov	Ne [REDACTED]
> je [REDACTED]s@nebraska.gov	ri [REDACTED]
> je [REDACTED]@nebraska.gov	JN [REDACTED]
> me [REDACTED]nebraska.gov	11 [REDACTED]
> em [REDACTED]nebraska.gov	Ha [REDACTED]

938 hits

host	username	password
> https://nebraska.gov/	Gr [REDACTED].com	[REDACTED]
> https://nebraska.gov/	Te [REDACTED].com	[REDACTED]
> https://nebraska.gov	CH [REDACTED]esp.com.br	[REDACTED]
> https://nebraska.gov/	TL [REDACTED]	[REDACTED]
> https://nebraska.gov/	AS [REDACTED]company.com	[REDACTED]
> https://nebraska.gov/	Ra [REDACTED]um.com	[REDACTED]
> https://nebraska.gov/	Ds [REDACTED]rus.com	[REDACTED]
> https://networks.nebraska.gov/	Pa [REDACTED]	[REDACTED]
> https://nebraska.gov/login	JL [REDACTED]	[REDACTED]
> https://childsupport.nebraska.gov/	AR [REDACTED]	[REDACTED]
> https://networks.nebraska.gov/	MI [REDACTED]	[REDACTED]

ATTACK



# Attack 2: Guessable Creds



114 instances as **medium**

11 instances as **high**

7 or 8 character minimum

Misconfigured password age

Poor lockout config

ATTACK

```
PS C:\Users\doadmin> net accounts /dom
Force user logoff how long after time expires?:      Never
Minimum password age (days):                        1
Maximum password age (days):                        42
Minimum password length:                             7
Length of password history maintained:               24
Lockout threshold:                                   Never
Lockout duration (minutes):                          10
Lockout observation window (minutes):                10
Computer role:                                       PRIMARY
The command completed successfully.
```

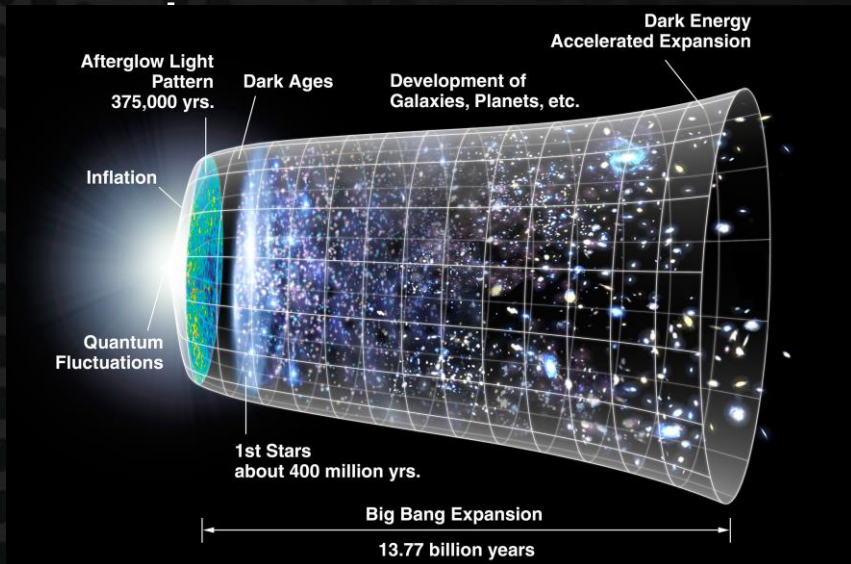


© Black Hills Information Security  
@BHInfoSecurity



# Attack 3: Direct Exploitation

Imagine, the big



In the beginning, there was acquisition...  
Then there was HR.  
...and our unpatched MoveIt server  
brought on the heat death of the universe.

## Inventory Controls

CIS Control 1: [Inventory and Control of Enterprise Assets](#)

CIS Control 2: [Inventory and Control of Software Assets](#)

CIS Control 3: [Data Protection](#)

**The #1 reason  
organizations abandon  
the CIS framework!**

ATTACK



© Black Hills Information Security  
@BHInfoSecurity

# Attack 4: Other Peeps Creds



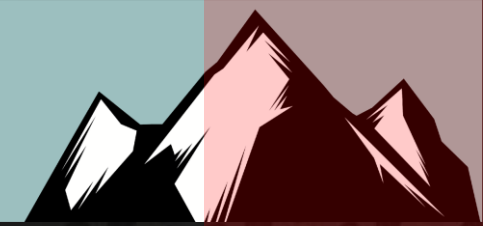
- Default settings.
- So many default settings.
- Message integrity off by default
- I mean, why should we validate the integrity of a privileged authentication request against our domain controller to dump LAPS passwords, create a computer object, request delegation for PC131, and escalate an arbitrary user account to EA??
- Event ID 4741

```
python3 ntlmrelayx.py -6 -t ldaps://dc01 -wh  
hacked-wpad --add-computer pc131 --delegate-  
access -ts -of /opt/work/relays --dump-gmsa  
--dump-laps --escalate-user john.strand
```

ATTACK



# Attack 5: You Forgot MFA



We reported a Lack of MFA 60 times as either **High** or **Critical**.

60 / 150 = 40% of networks are not defended against a weak password policy.

This is among the most shocking datapoints in the study.

**P@s\$w0rds at the U.S. Department of the Interior: Easily Cracked Passwords, Lack of Multifactor Authentication, and Other Failures Put Critical DOI Systems at Risk**

**This is a revised version of the report prepared for public release.**

ATTACK

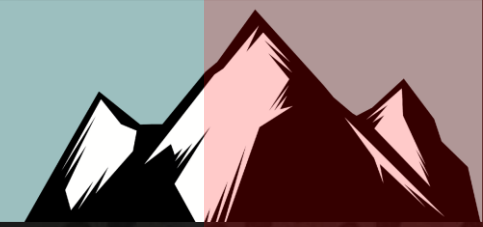


© Black Hills Information Security  
@BHInfoSecurity

[https://www.doioig.gov/sites/default/files/2021-migration/Final%20Inspection%20Report\\_DOI%20Password\\_Public.pdf](https://www.doioig.gov/sites/default/files/2021-migration/Final%20Inspection%20Report_DOI%20Password_Public.pdf)



# Attack 6: Network Infrastructure



We had 69 instances reported as **High**

- WPAD is kinda new again.
  - Browser hijacking.
    - Via default configuration.
  - HTTP auth relay to LDAP/LDAPs.
    - msDS-keyCredentialLink
- LLMNR is still around.
  - Not as frequent as it used to be.
- NBNS is still on by default on adapters.
  - Not as frequent as it used to be.



ATTACK

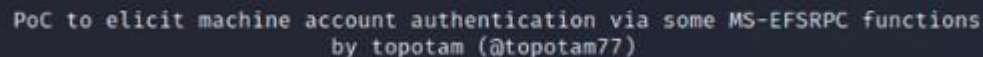


© Black Hills Information Security  
@BHInfoSecurity

- Not sure how to "meme" this.
- Use a valid username/password to coerce authentication, relay the response elsewhere, achieve complete and utter world domination in the process.



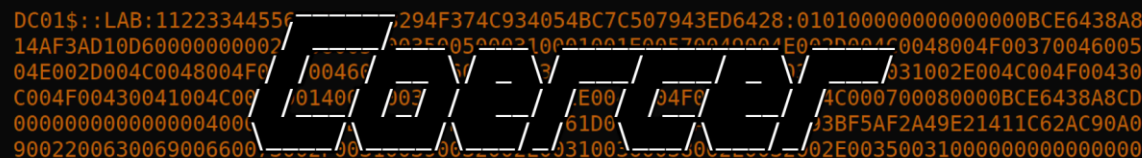
This repository contains a list of




Inspired by @tifkin\_ & @elac



**In one easy step.**



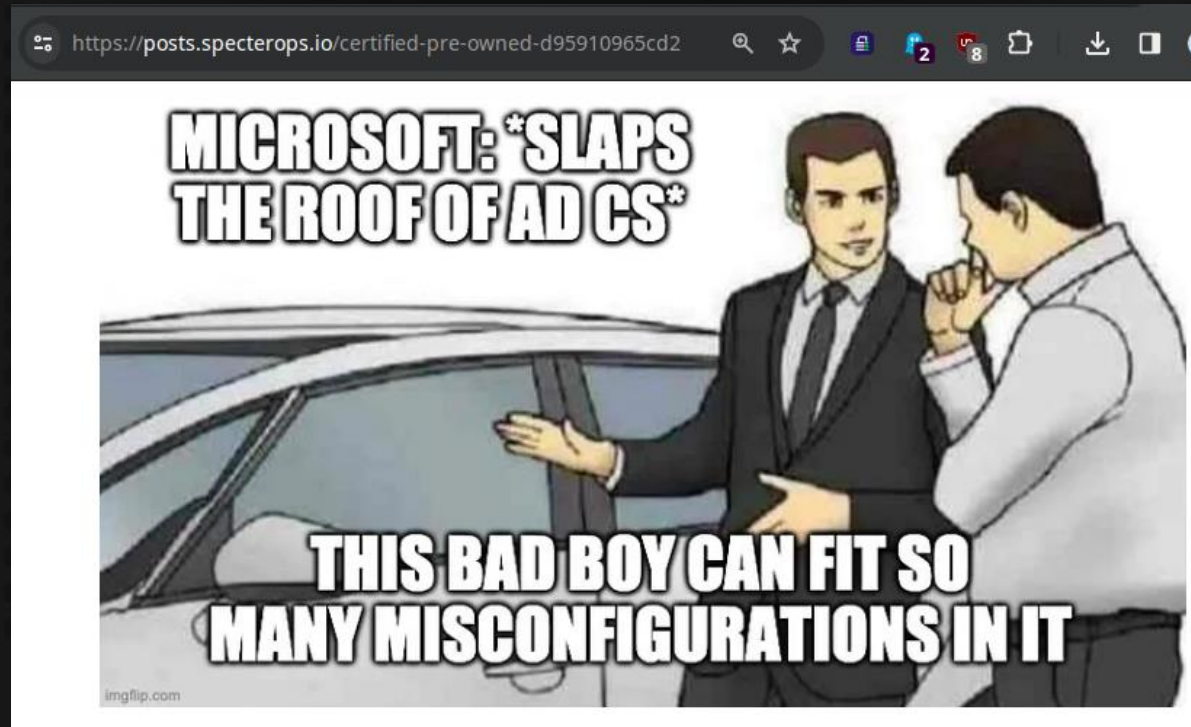
© Black Hills Information Security  
 @BHInfoSecurity



# Attack 8: PKI DAaaS via ADCS

Reported 64 times as **high** or **critical**

- Go read the whitepaper: <https://posts.specterops.io/certified-pre-owned-d95910965cd2>
- If you have ADCS, it is probably vulnerable to several conditions.



ATTACK



© Black Hills Information Security  
@BHInfoSecurity



# Attack 9: Combine Things

All password and credential related vulnerabilities:

- Password Reuse
  - Widespread Administrator
  - Password Expiration Exceptions
  - Missing Authentication
  - Systems Using Vendor-Supplied Credentials
  - Cleartext Storage of Passwords
  - Cleartext Secrets in Source Code
  - Secrets Stored in Automation Routines
- 
- 586 total matches – 125 instances of weak password policy
  - = 461 references in findings to cred\* password\* secret\*



ATTACK



© Black Hills Information Security  
@BHInfoSecurity

# Demo – Live Range



DETECT

Azure Sentinel:  
Password Spray Attack Spike 2



© Black Hills Information Security  
@BHInfoSecurity