Security Basics:
Burn It All and Start Over

John Strand

BLACK HILLS INFORMATION SECURITY

How do bad things happen?

- We seem to be in a loop
  - A very bad loop
- Getting angry at questions…
  - Best AV?
  - Best DLP?
  - Best Threat Intel Feed?
  - Best Firewall?
- Patterns and Chiasms

This.. Without the learn.

Password Example

- Most password complexity requirements are:
  - >8 Characters
  - Upper/Lower/Alpha/Numeric
  - No Dictionary words
  - Full of fail
- “We cannot fix this because of compliance!”

Truth!

NIST Greenbook

L is set for 6 months and 12 months. P is set for 1 in 1,000,000 (acceptable probability of guessing the password). R is set at 8.5 guesses per minute (guess rate possible with 300-baud service).

At 8.5 guesses per minute, the number of guesses per day would be 12,240.

Substituting 183 days for 6 months then using equation [3],

$$S = G \frac{P}{} \quad 183 \times 12240 - 000001 \quad 2.23992 \times 1012 \text{ passwords}$$

The 12-month value is twice that of the 6-month case.

TABLE 1

MAXIMUM LIFETIME (months)	Length of Password	
	26-Character alphabet	36-Character alphabet
6	9 (rounded up from 8-72)	8 (rounded up from 7.93)
12	9 (rounded up from 8.94)	8 (rounded down from 8.13)
21		

Cash Cow Tipping….

- Bypass everything..
  - AV, DLP, Firewalls, etc.
- Trivial to do..
- More smoke and mirrors
- Get previous sessions here:
  - Tinyurl.com/504extra2

Do You Run Any of These?

Avast_Bypass.pptx	433.39 KB
AVBypass.pptx.pdf	12.71 MB
AVBypasswithNOPsFun.docx	270.53 KB
AVG AV Bypass.pptx	624.05 KB
avg_bypass.pptx	0.92 MB
JRS-HackFest m edits 11-9-15.pptx	6.63 MB
kaspersky_powercat_bypass.pptx	187.69 KB
McAfee AV Bypass.pptx	435.96 KB
sad_panda.pptx	480 KB
SCCT2015.pptx	1.34 MB
Sophos AV Bypass.pptx	275.98 KB
Symantec-av-evasion-stuff.pptx	186.63 KB
Testing_Breaking_Security_Software.pptx	17.55 MB
Trend Micro AV Bypass-2.pptx	306.88 KB
Trend Micro AV Bypass.pptx	306.88 KB

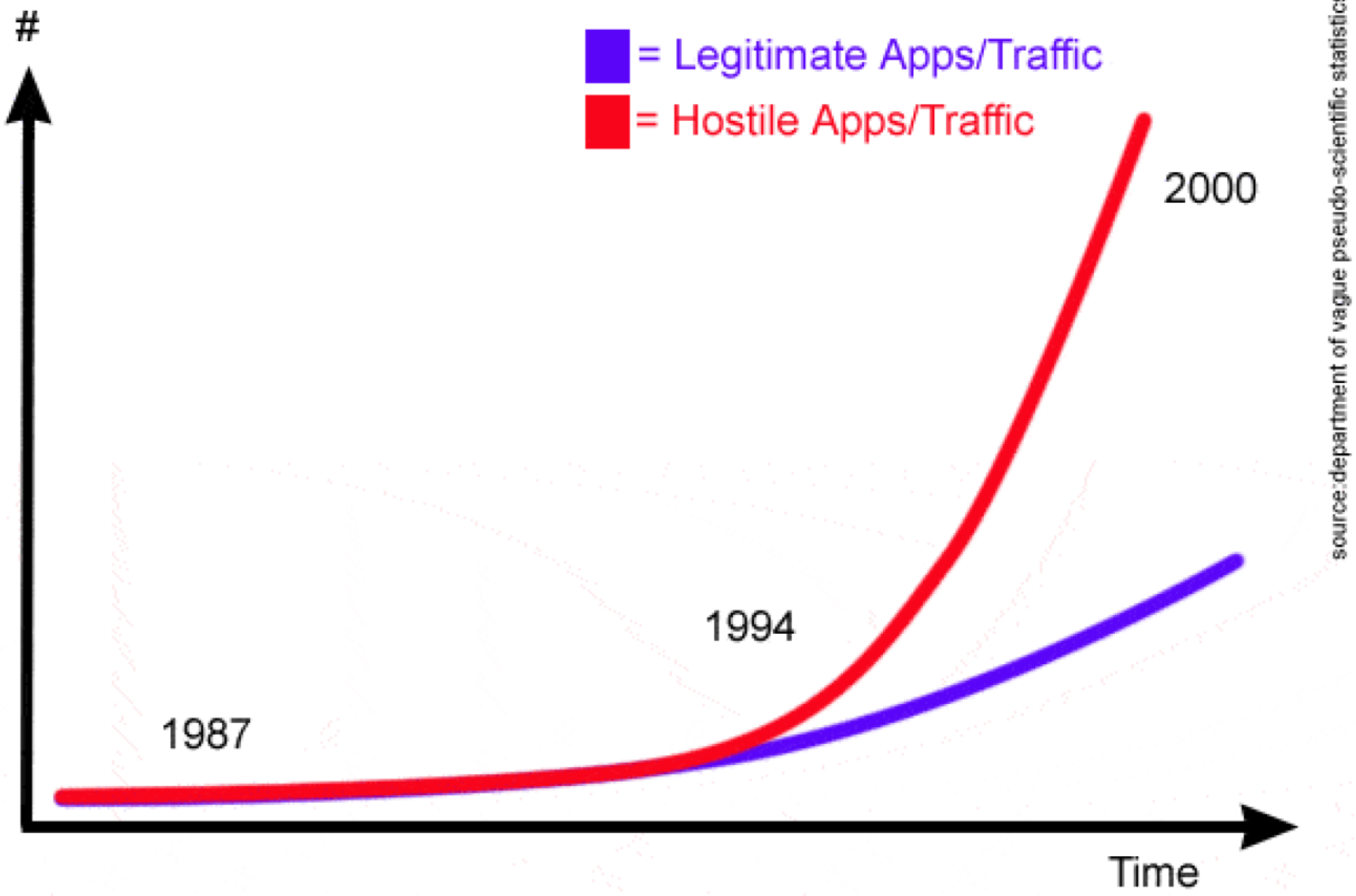
Moving Forward

- AV, DLP, Firewalls, Threat Intelligence Feeds, Cyber Kill-Chain
- Let's leave those old things behind
- If we started all over again… How would we do it?
- There is a lot of baggage over the years….
- Time to let that go too.
- This is all based on our testing and training
- Same loops, same patterns

Internet White Listing

- Internet Blacklisting WILL NOT WORK!!
  - Ever. Ever. Ever. Ever. Ever
- Restrict “Uncategorized”
- Please, put the pitchforks away
- You ***<u>can</u>*** do this
- It is not that hard… Really..

This presentation is bad!
And you should feel bad!

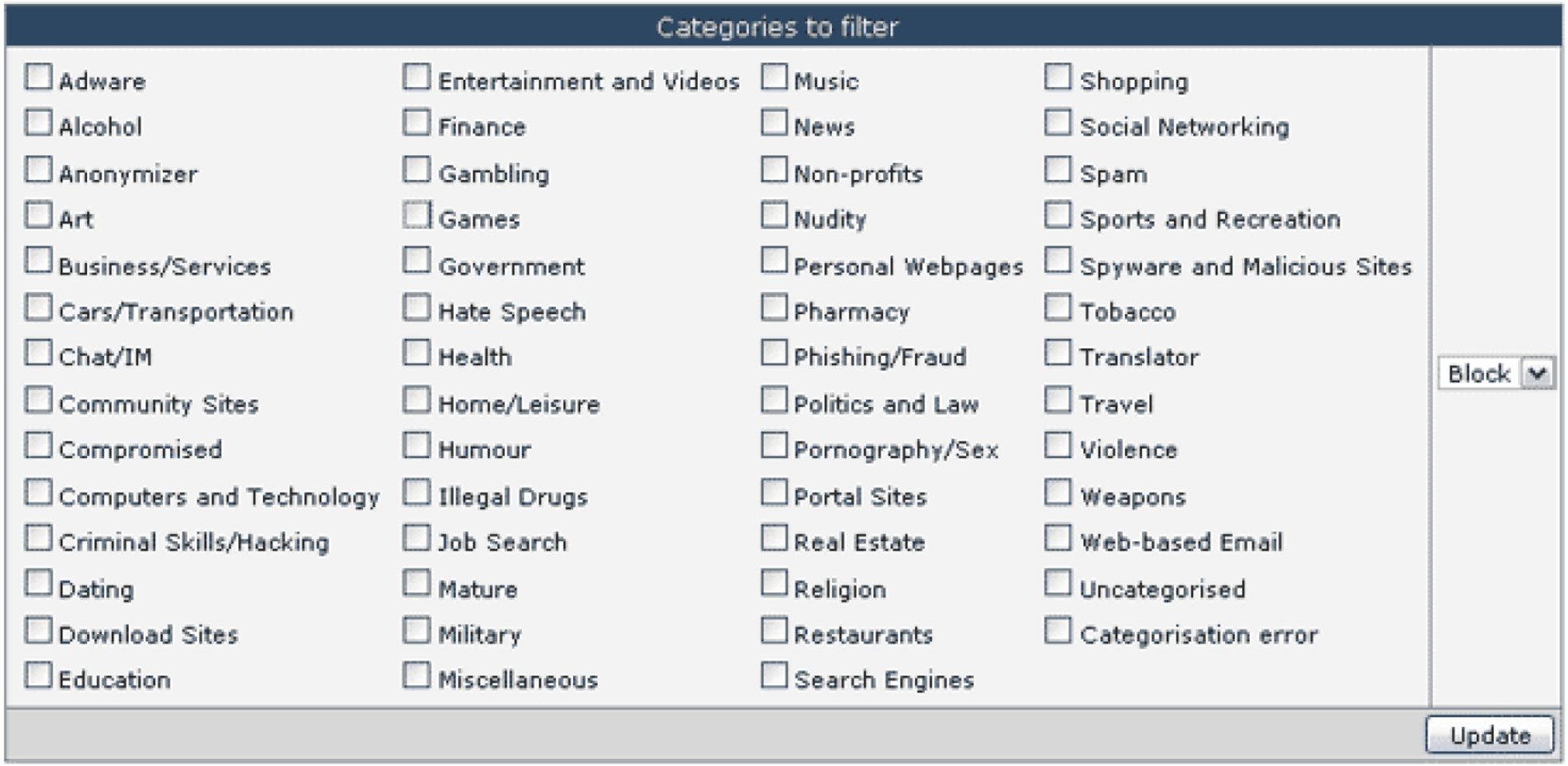


13 years ago… 13.

Let's Play A Game

- How many "legitimate" sites do your users go to?
  - 200? 500? 1000? 2000?
  - Really, lets find this out.
- Let's say we allow all of them (within reason)
- But! We remove ads… Please… Let them die.
- What would your exposure be?

Filtering


Categories to filter
Adware
Alcohol
Anonymizer
Art
Business/Services
Cars/Transportation
Chat/IM
Community Sites
Compromised
Computers and Technology
Criminal Skills/Hacking
Dating
Download Sites
Education
Entertainment and Videos
Finance
Gambling
Games
Government
Hate Speech
Health
Home/Leisure
Humour
Illegal Drugs
Job Search
Mature
Military
Miscellaneous
Music
News
Non-profits
Nudity
Personal Webpages
Pharmacy
Phishing/Fraud
Politics and Law
Pornography/Sex
Portal Sites
Real Estate
Religion
Restaurants
Search Engines
Shopping
Social Networking
Spam
Sports and Recreation
Spyware and Malicious Sites
Tobacco
Translator
Travel
Violence
Weapons
Web-based Email
Uncategorised
Categorisation error
Block
Update

Application White Listing

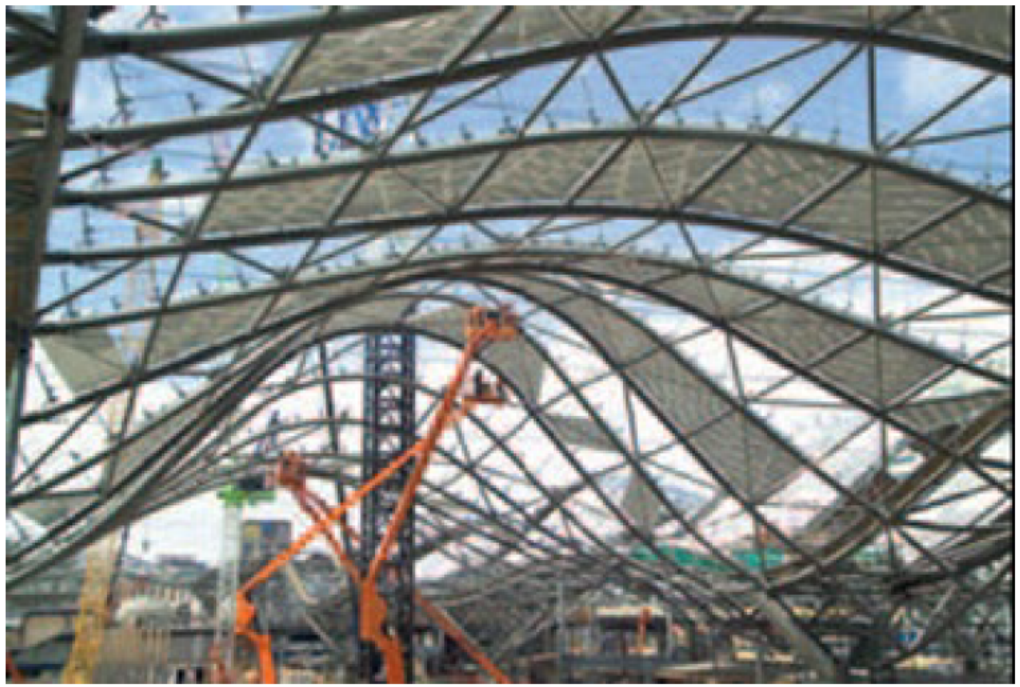
- Ok…. This one is not easy…
- We have a weird binary view of things
  - "If it can be broke, it is all broke"
- Sure, there is value to this view…
- But…

Default Rules

Action	User	Name	Condition	Exceptio
Allow	Everyone	(Default Rule) All files located in the Pro...	Path	
Allow	Everyone	(Default Rule) All files located in the Wi...	Path	
Allow	BUILTIN\Ad...	(Default Rule) All files	Path	

It's All About Architecture

- Failure points
- Mitigations
- weaknesses
- Mitigations
- Planning
- Mitigations
- Component Failure Thresholds
- Mitigations



Roadmaps

AuditScripts

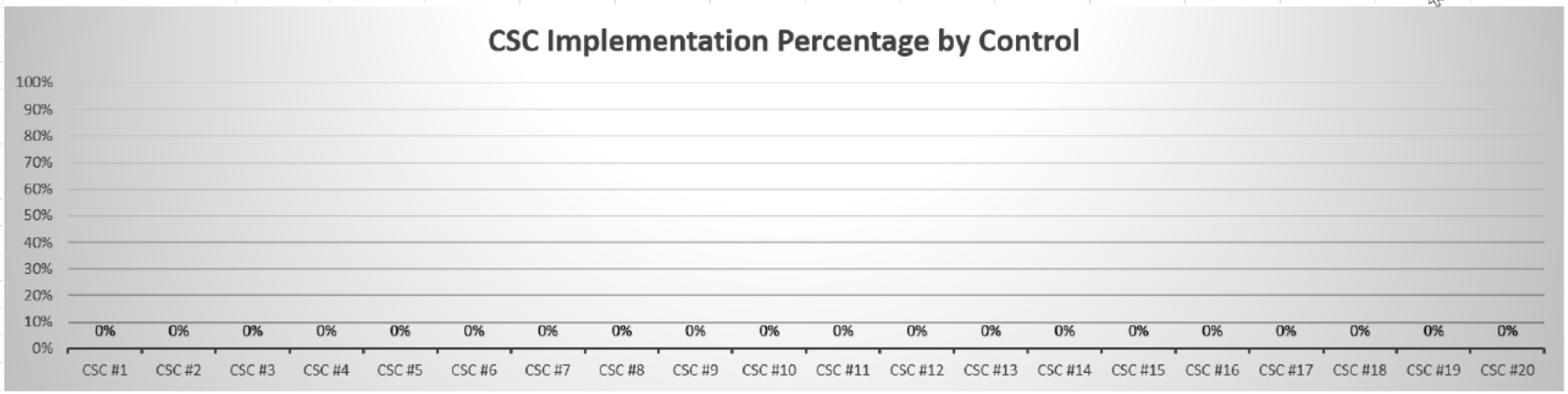
Critical Security Controls Initial Assessment Tool (v6.1c)

enclave SECURITY

Maturity level:	Description:	Score:
Level One	Policies Complete	0.00
Level Two	Controls 1-5 Implemented	0.00
Level Three	All Controls Implemented	0.00
Level Four	All Controls Automated	0.00
Level Five	All Controls Reported	0.00

Maturity Rating*: **0.00**

*Rating is on a 0-5 scale.



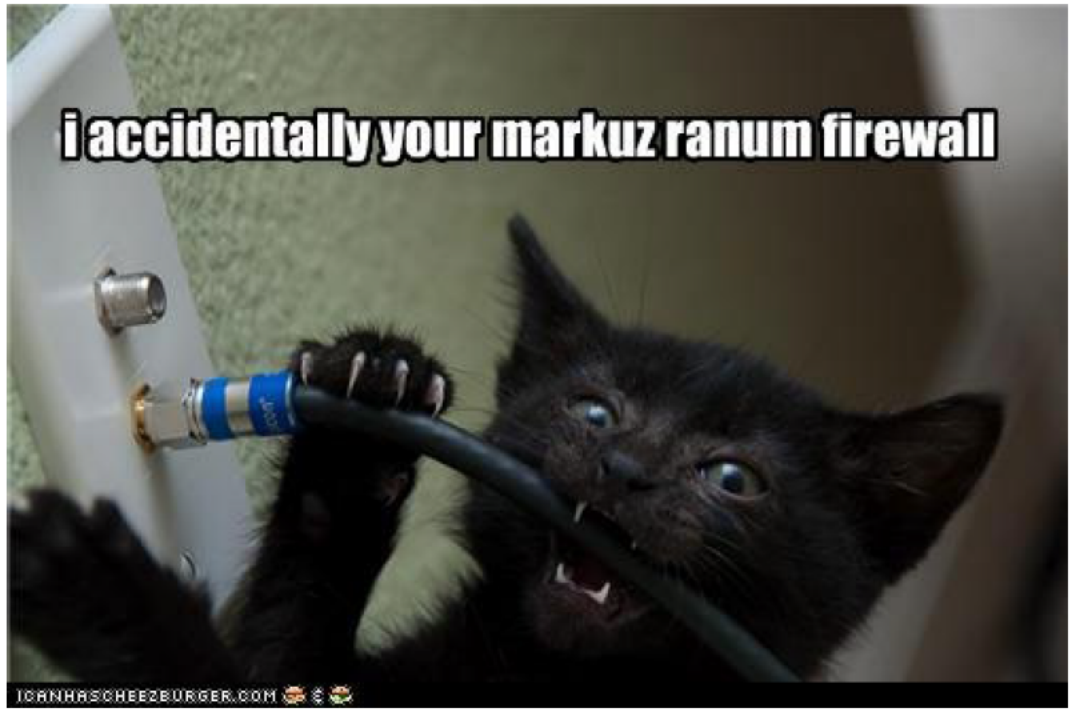
BLACK HILLS INFORMATION SECURITY

MITRE

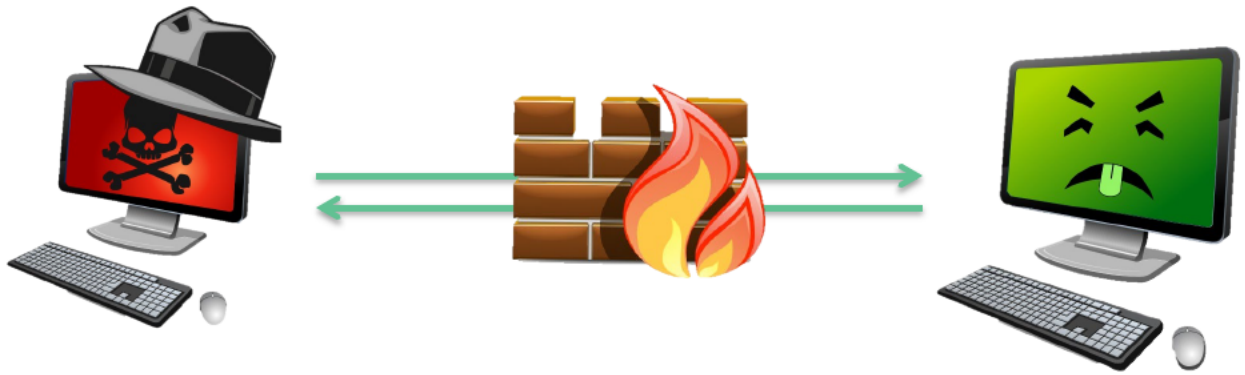
Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
Accessibility Features	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	Application Deployment Software	Command-Line Interface	Audio Capture	Automated Exfiltration	Commonly Used Port
AppCert DLLs	Accessibility Features	Binary Padding	Brute Force	Application Window Discovery	Distributed Component Object Model	Dynamic Data Exchange	Automated Collection	Data Compressed	Communication Through Removable Media
AppInit DLLs	AppCert DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Vulnerability	Execution through API	Browser Extensions	Data Encrypted	Connection Proxy
Application Shimming	AppInit DLLs	Code Signing	Credentials in Files	Network Service Scanning	Logon Scripts	Execution through Module Load	Clipboard Data	Data Transfer Size Limits	Custom Command and Control Protocol
Authentication Package	Application Shimming	Component Firmware	Exploitation of Vulnerability	Network Share Discovery	Pass the Hash	Graphical User Interface	Data Staged	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Bootkit	Bypass User Account Control	Component Object Model Hijacking	Forced Authentication	Peripheral Device Discovery	Pass the Ticket	InstallUtil	Data from Local System	Exfiltration Over Command and Control Channel	Data Encoding

Firewalls… Turn them on.

- Treat your internal network as hostile…
  - It is
- There is no good reason to have workstations talk with each other.
- None…

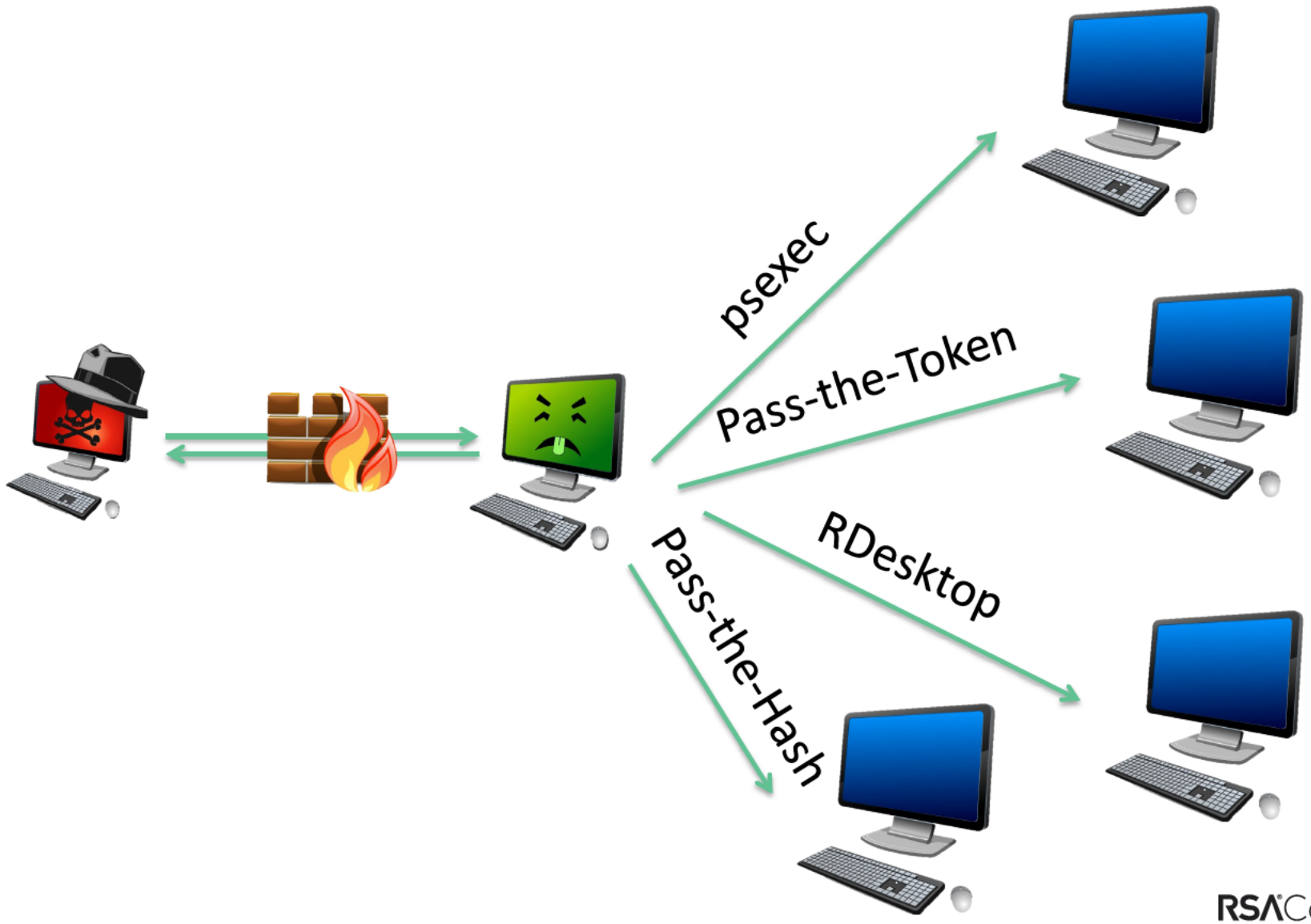


Just Your Standard Exploit

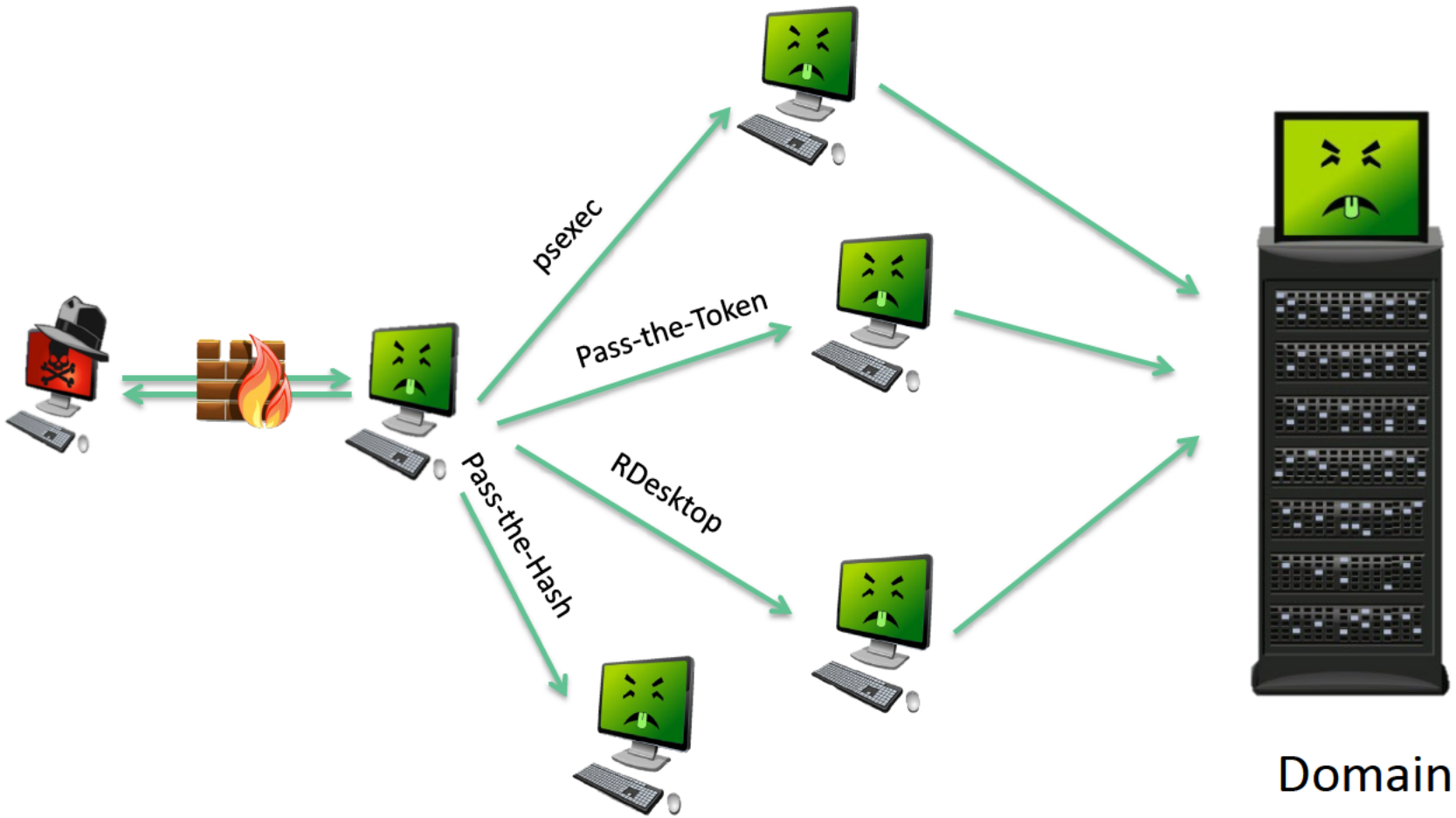


This is usually delivered as a client-slide exploit or a drive-by download.

Will These Protocols Trip IDS Alerts?



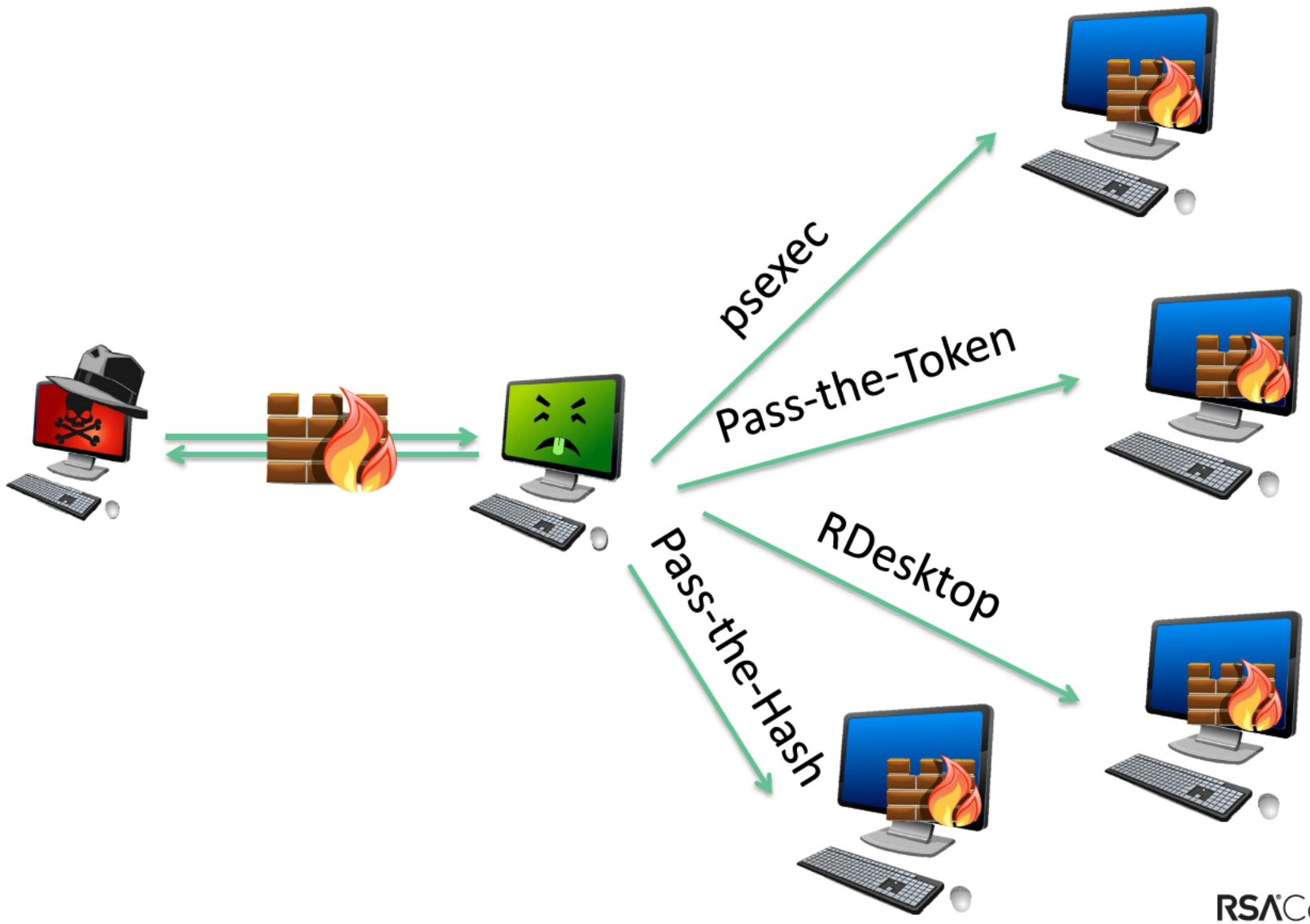
Most Likely They Will Not



Firewalls

- Treat the internal network as hostile
  - Because it is
- Set your internal system firewalls at the same level they would be at a coffee shop
  - All inbound traffic should be blocked and alerts should be generated
  - Exceptions for Admin networks
- Segment business units and/or organizational units
  - Why allow SMB RPC between subnets?
  - Contains the attacks even further than simple firewalls
- Many of the AV products have firewalls
- You can even use the built-in Windows firewall
  - If you are sadistic and desperate
- Private VLANS can work as well

Restriction of Lateral Movement

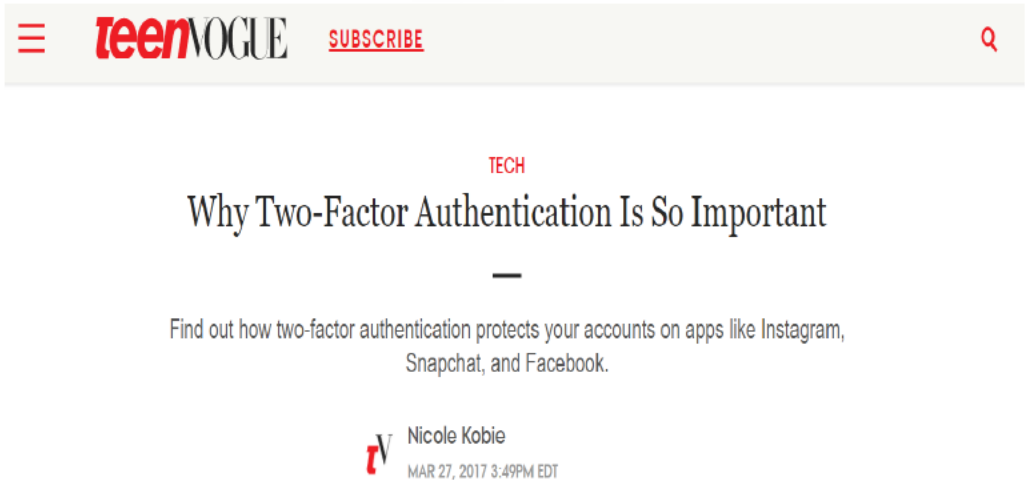


Passwords..

- The only thing that matters is length
- At least 16 characters long
- Allow dictionary words
- But! Keep Upper/Lower/Special/Numbers

Two Factor

- Why is it that most peoples personal email is more secure than their company email?
- Not bulletproof
- Will slow an attacker down
- A lot

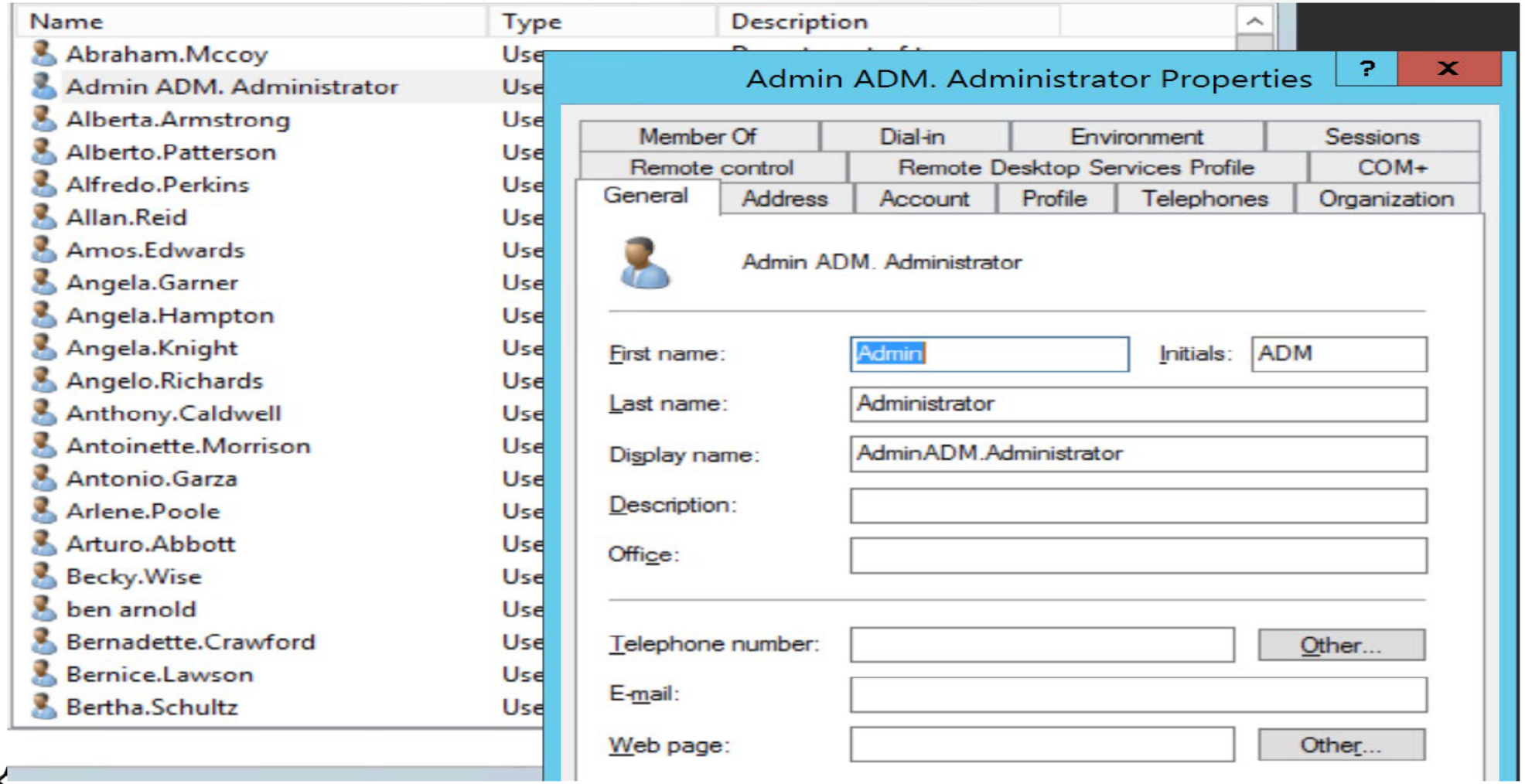


Teen Vogue… Teen. Vogue.

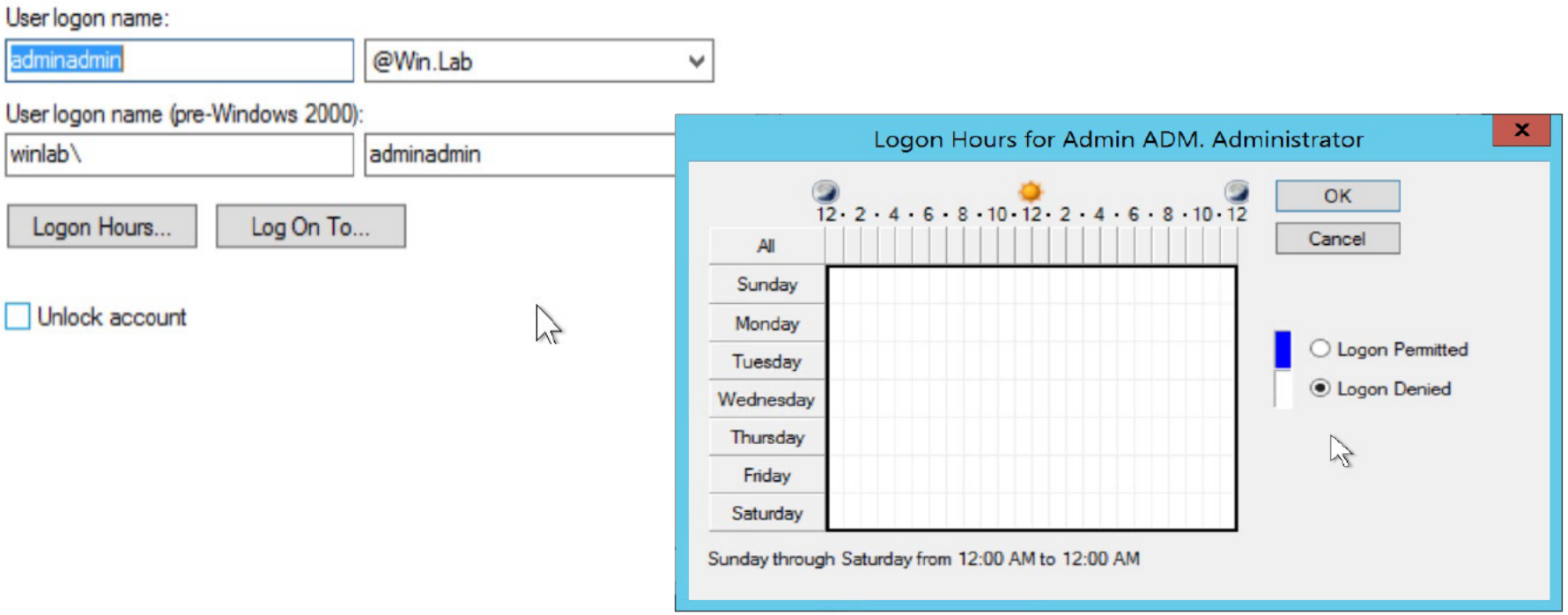
Smarter Logging
Active Directory HoneyAdmin

BLACK HILLS INFORMATION SECURITY

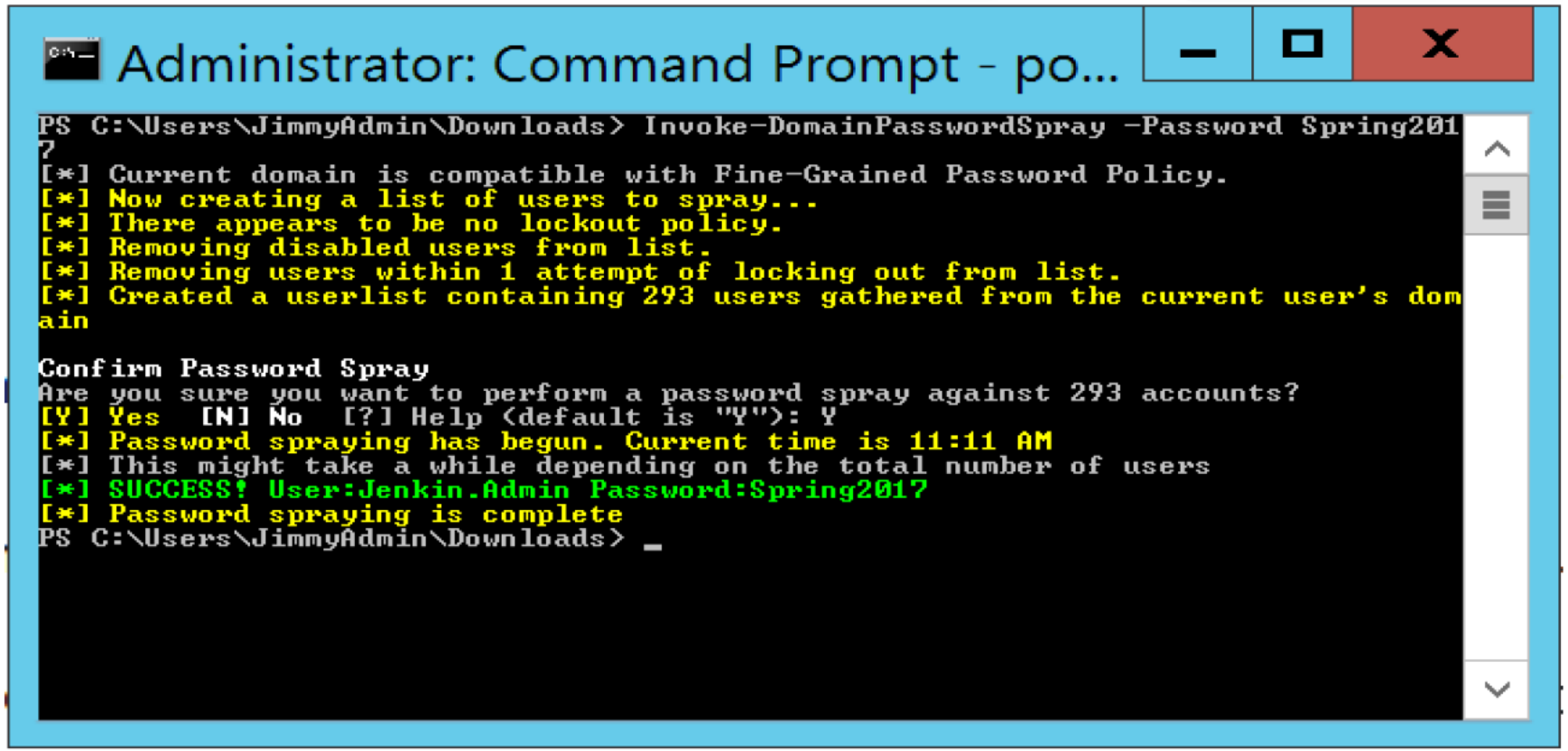
Go on.. Be obvious!



Disable Logon Hours



Password Spray



Alerts!

07-19-2017 10:11:53 User.Notice 10.233.233.10 Jul 19 11:11:53 WinLab-DC.Win.Lab MSWinEventLog 1 Security 6439 Wed Jul 19 11:11:52 2017 4625 Microsoft-Windows-Security-Auditing \adminadmin N/A Failure Audit WinLab-DC.Win.Lab Logon An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: adminadmin Account Domain: Failure Information: Failure Reason: Account logon time restriction violation. Status: 0xC000006E Sub Status: 0xC000006F Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: WINLAB-DC Source Network Address: fe80::34fe:5e09:f665:3b9 Source Port: 63183 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. The Subject fields indicate the

Please…. Log Sysmon

```
Process Create:
RuleName:
UtcTime: 2019-07-29 16:49:44.838
ProcessGuid: {ac6a4e42-23a8-5d3f-0000-0010f8353400}
ProcessId: 6816
Image: C:\Users\Sec504\Downloads\msf.exe
FileVersion: 2.2.14
Description: ApacheBench command line utility
Product: Apache HTTP Server
Company: Apache Software Foundation
OriginalFileName: ab.exe
CommandLine: "C:\Users\Sec504\Downloads\msf.exe"
CurrentDirectory: C:\Users\Sec504\Downloads\
User: THEBOSS\Sec504
LogonGuid: {ac6a4e42-61bd-5d37-0000-002033200700}
LogonId: 0x72033
TerminalSessionId: 2
IntegrityLevel: Medium
Hashes: MD5=532FA545F9B01DCA5E0991B7AB85E326,SHA256=4960AD6540BF6D8991ED93
ParentProcessGuid: {ac6a4e42-61c2-5d37-0000-001092270800}
ParentProcessId: 1772
ParentImage: C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
ParentCommandLine: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"
```

How do you eat an elephant?

- The issue is we try to jump straight into full implementation
- “Lets do a full Carbon Black install!”
- “Lets implement Tripwire everywhere!!!”
- Of New Years resolutions and past addictions

“Its OK dude… They don’t even TRY to eat me…”

Protect yourself!

- Adblock Plus
- OpenDNS
- Stay Patched!
- Passphrase
- Don’t run strange programs
- Microsoft AV is just fine
- Never talk with “Microsoft Tech Support”
- Kids… A note on kids

"Apply" Slide

- Stop doing what we have done
  - Traditional Defenses (SIEM, AV, Firewalls) are getting out of date very quickly
  - "Fix" passwords with length and 2FA
- Look to actual attacks and what detects and stops those attacks
  - Use MITRE
- Improve logging
  - Sysmon is your friend
- Set some traps

Thanks!

- John Strand
  - john@bhis.co
  - @strandjs
  - 303-710-1171

I am not wearing plaid today…