tenable
network security

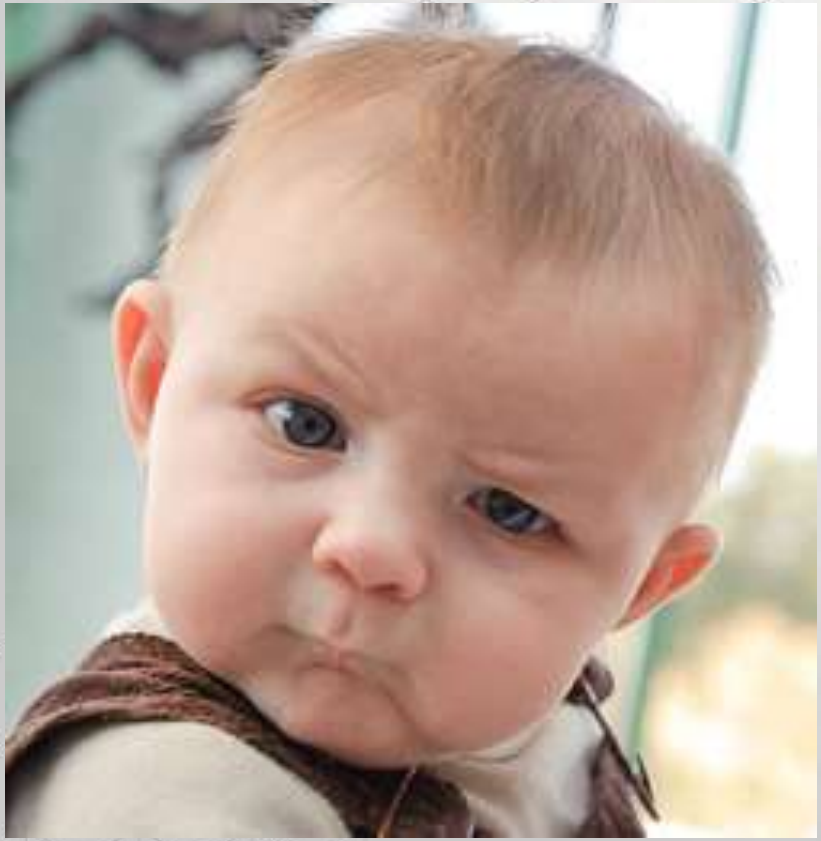
Reducing Your Patch Cycle to Less Than 5 Days

A “Vulnerabilities Exposed” Webcast

Paul Asadoorian & Jack Daniel

Skepticism

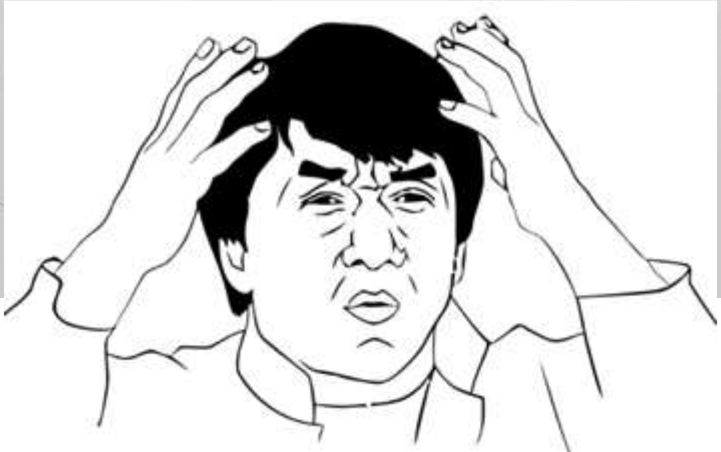
I can reduce my patch cycle to less than 5 days?



And spoons don't really sound like airplanes?

Who, What, When, Where, Why, How?

- **Who**: You, management, administrators
- **Why**: Yes, you can, but first, why should you?
- **How**: Then, how can you reduce your patch cycle?
- **What**: Finally, what can you use to make it easier?
- **When**: Now is good. Well, at least after you finish watching this webcast.



Why?

Known Vulnerabilities Cause Problems

- Most exploits are used against known vulnerabilities with a known patch
- Attacks using zero-day exploits aren’t main pain point for organizations
- Mandiant M-Trends, Trustwave GSR, and Verizon DBIR tell us to patch our stuff

Third Parties….

KuvatON.com
THIRD PARTY FACE PALM
For when there is so much fail.... you need that extra bit of outside help..

Third-party Software Hurts Us

March 14, 2013: 86% of vulnerabilities discovered in the most popular 50 programs in 2012 were in non-Microsoft (or “third-party”) programs. The result was published today in the Secunia Vulnerability Review 2013.

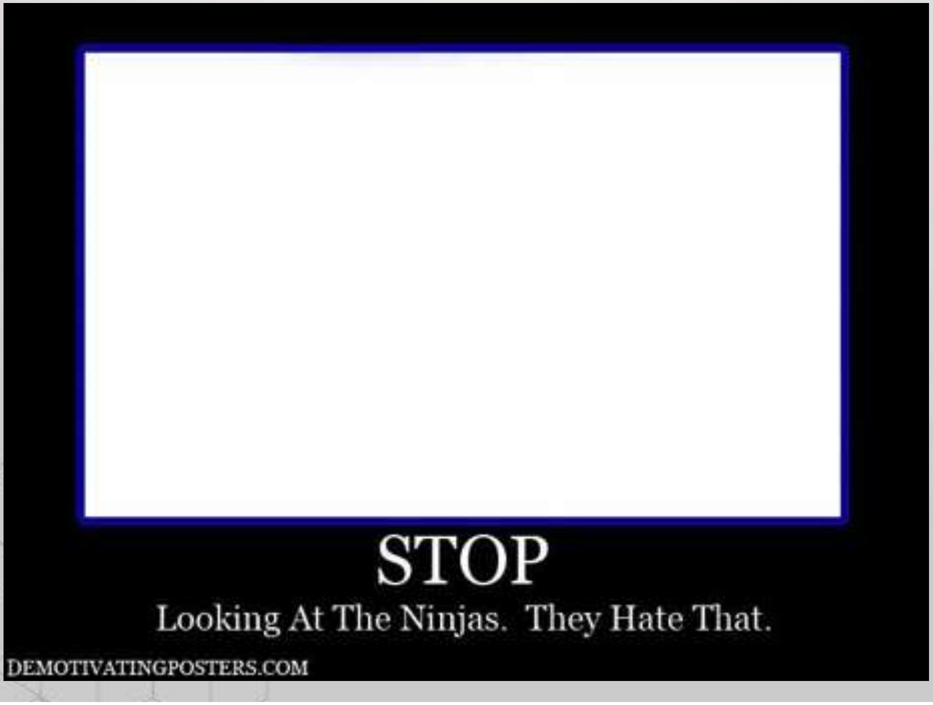
- https://secunia.com/blog/359/

First, a Story…

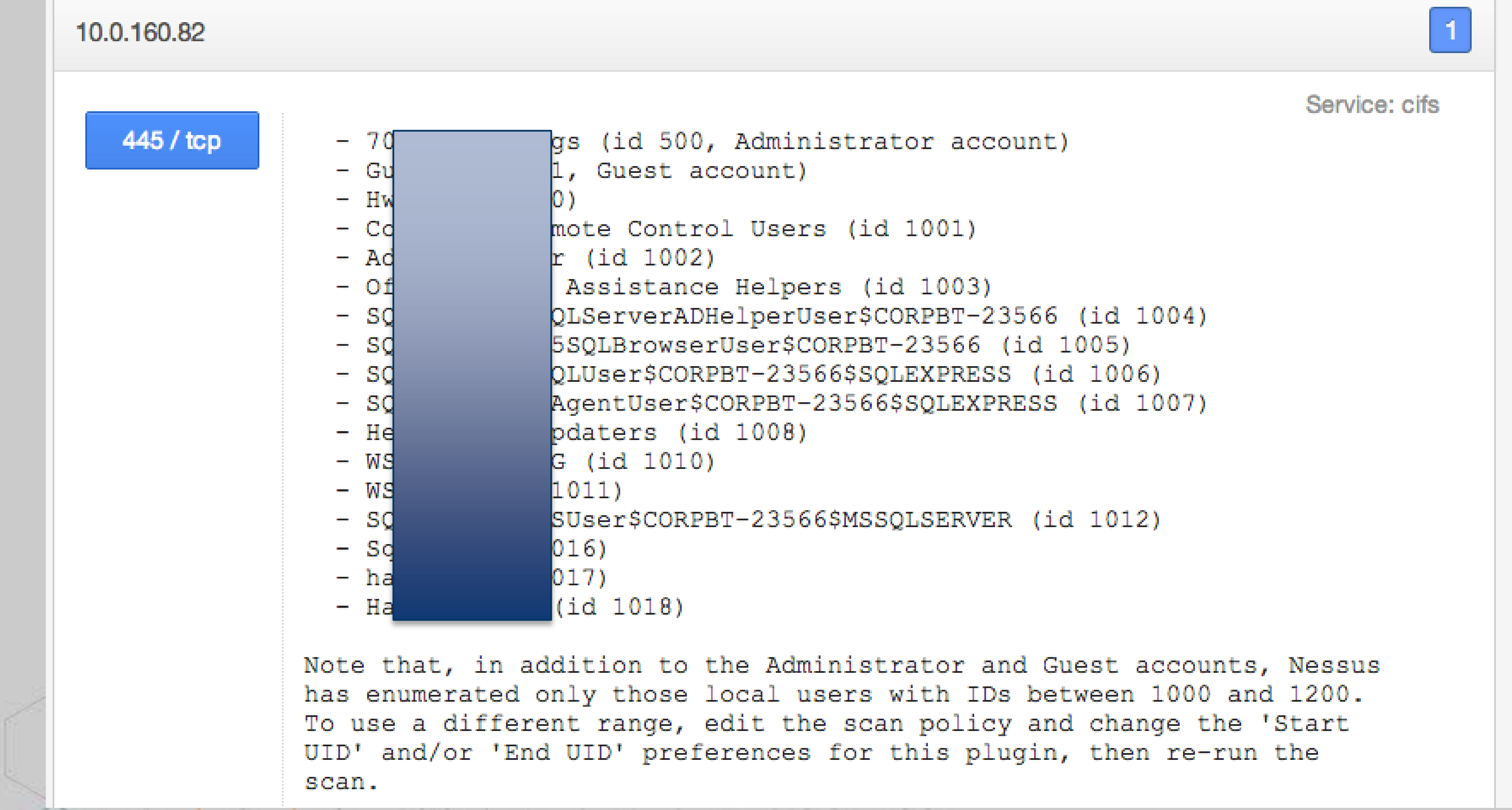
- The Needle in the Haystack Draws Blood
  - By Paul Asadoorian and Jack Daniel

Attacker on Your Network

- It happens! (Malware, Physical Access, Compromise, Social Engineering, etc…)
- First Goal: Find users and high-profile target systems
  - Domain controllers
  - File servers
  - Domain administrators



Enumerate Local Accounts

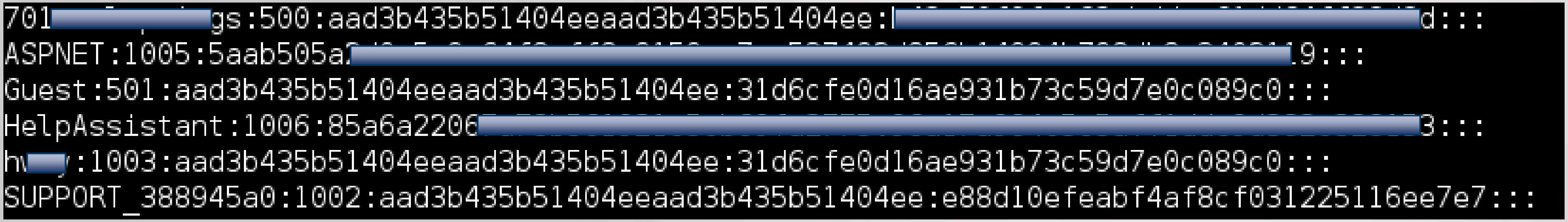


```
  - 70[redacted]gs (id 500, Administrator account)
  - Gu        1, Guest account)
  - Hw        0)
  - Co        mote Control Users (id 1001)
  - Ad        r (id 1002)
  - Of         Assistance Helpers (id 1003)
  - SQ        QLServerADHelperUser$CORPBT-23566 (id 1004)
  - SQ        5SQLBrowserUser$CORPBT-23566 (id 1005)
  - SQ        QLUser$CORPBT-23566$SQLEXPRESS (id 1006)
  - SQ        AgentUser$CORPBT-23566$SQLEXPRESS (id 1007)
  - He        pdaters (id 1008)
  - WS        G (id 1010)
  - WS        1011)
  - SQ        SUser$CORPBT-23566$MSSQLSERVER (id 1012)
  - Sq        016)
  - ha        017)
  - Ha        (id 1018)

Note that, in addition to the Administrator and Guest accounts, Nessus
has enumerated only those local users with IDs between 1000 and 1200.
To use a different range, edit the scan policy and change the 'Start
UID' and/or 'End UID' preferences for this plugin, then re-run the
scan.
```

Seek Out Easy Vulnerabilities

- One of the best choices: MS08-067
- Penetration testers celebrate its birthday
- Exploits are super reliable and give attacker system-level privileges

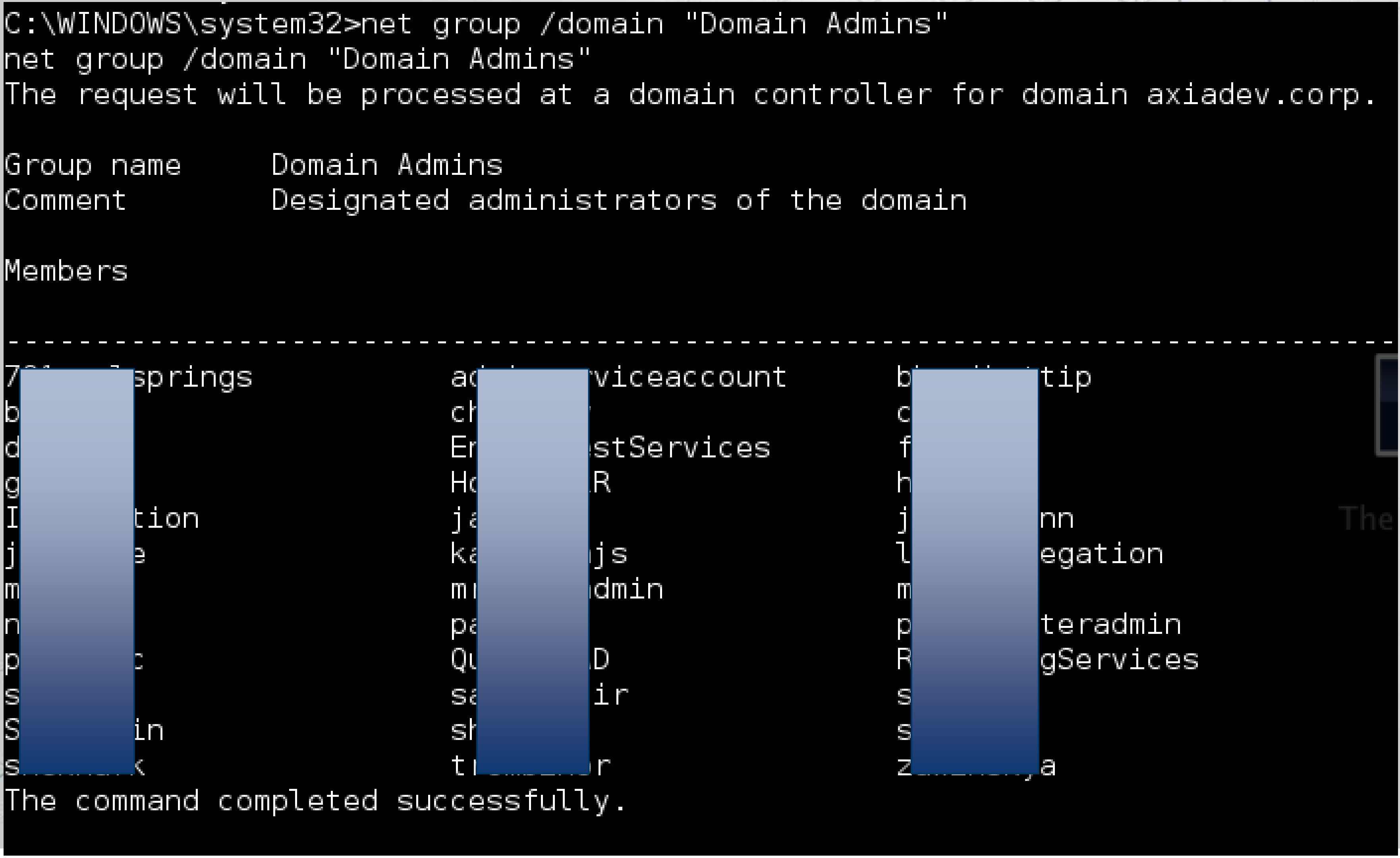
Dump Hashes & Crack Passwords



```
701[redacted]gs:500:aad3b435b51404eeaad3b435b51404ee:[redacted]d:::
ASPNET:1005:5aab505a[redacted]19:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1006:85a6a2206[redacted]3:::
h[redacted]:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:e88d10efeabf4af8cf031225116ee7e7:::
```

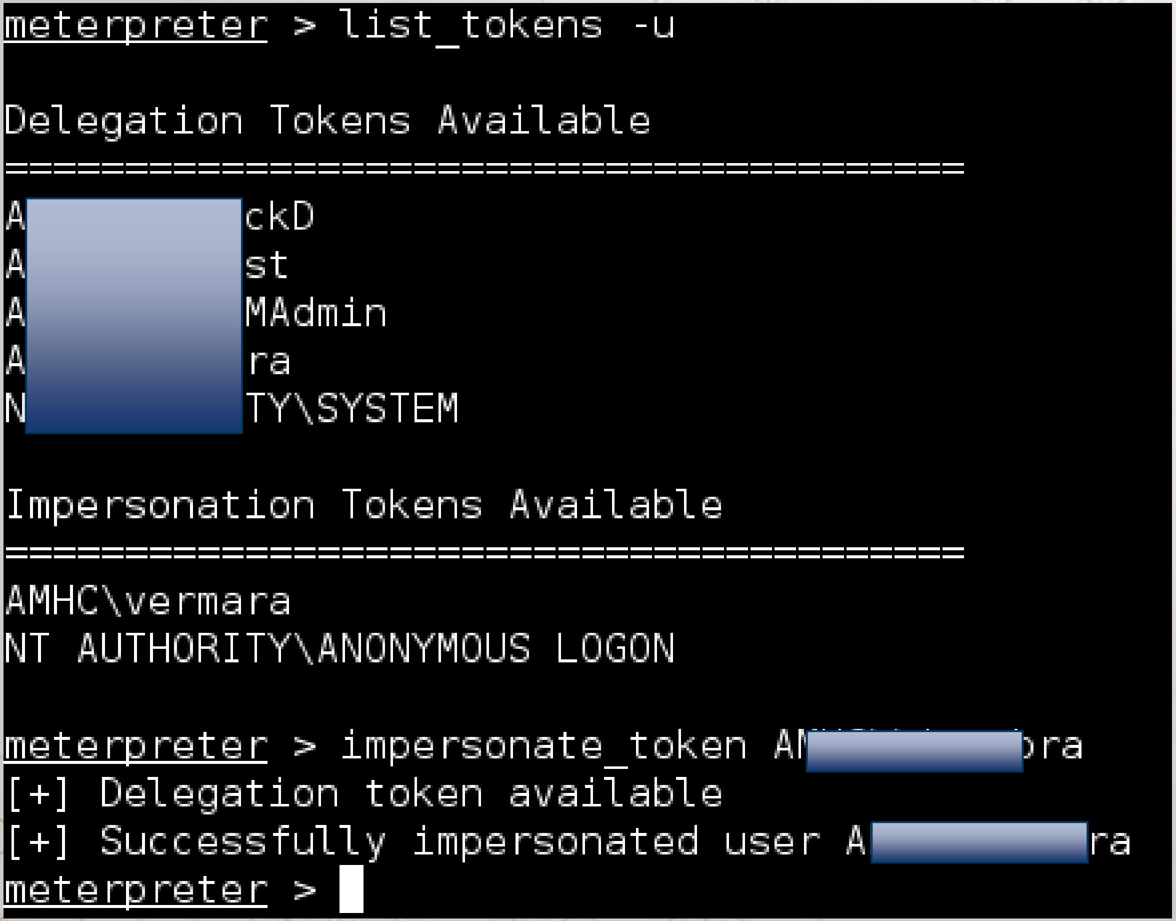
Re-use local administrator credentials/hashes to gain access to other systems

Enumerate Domain Admins



```
C:\WINDOWS\system32>net group /domain "Domain Admins"
net group /domain "Domain Admins"
The request will be processed at a domain controller for domain axiadev.corp.

Group name     Domain Admins
Comment        Designated administrators of the domain

Members

-------------------------------------------------------------------------------
7[redacted]springs        ad[redacted]viceaccount       b[redacted]tip
b                         ch                            c
d                         En      stServices            f
g                         Ho      R                     h
I     tion                ja                            j      nn
j     e                   ka      js                    l      egation
m                         m       dmin                  m
n                         pa                            p      teradmin
p     c                   Qu      D                     R      gServices
s                         sa      ir                    s
S     in                  sh                            s
s     k                   t       r                     z      a
The command completed successfully.
```

Impersonate a Domain Admin



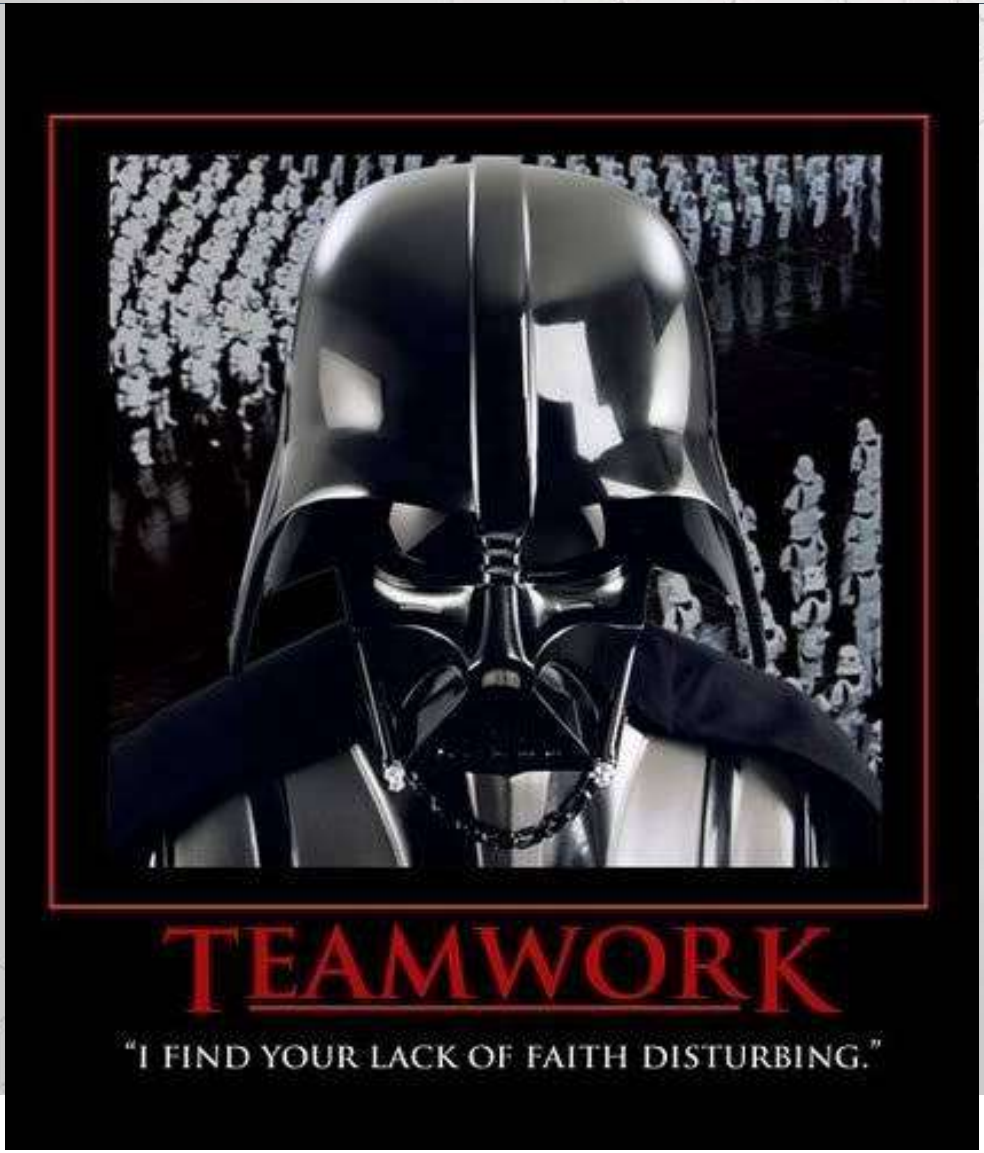
```
meterpreter > list_tokens -u

Delegation Tokens Available
========================================
A[redacted]ckD
A         st
A         MAdmin
A         ra
N         TY\SYSTEM

Impersonation Tokens Available
========================================
AMHC\vermara
NT AUTHORITY\ANONYMOUS LOGON

meterpreter > impersonate_token AM[redacted]ra
[+] Delegation token available
[+] Successfully impersonated user A[redacted]ra
meterpreter > 
```

Game Over

Moral of the Story

- You must keep up with patches on ALL of your systems
- You must identify easily-exploitable vulnerabilities and patch them FAST

Who?



Step 1 – Define

- Policy – What you will do and where you will do it
- Procedures – How you will do it and who you will do it with
- Get management to sign off on both of the above

It doesn't matter how many resources you have
if you don't know how to use them, they will never be enough

Step 2 – Communication & Process

- Communicate your policy and procedures to the right people!
- Management, security, administrators, and end users

How? (Not Magic)

Step 3 – Find Them All

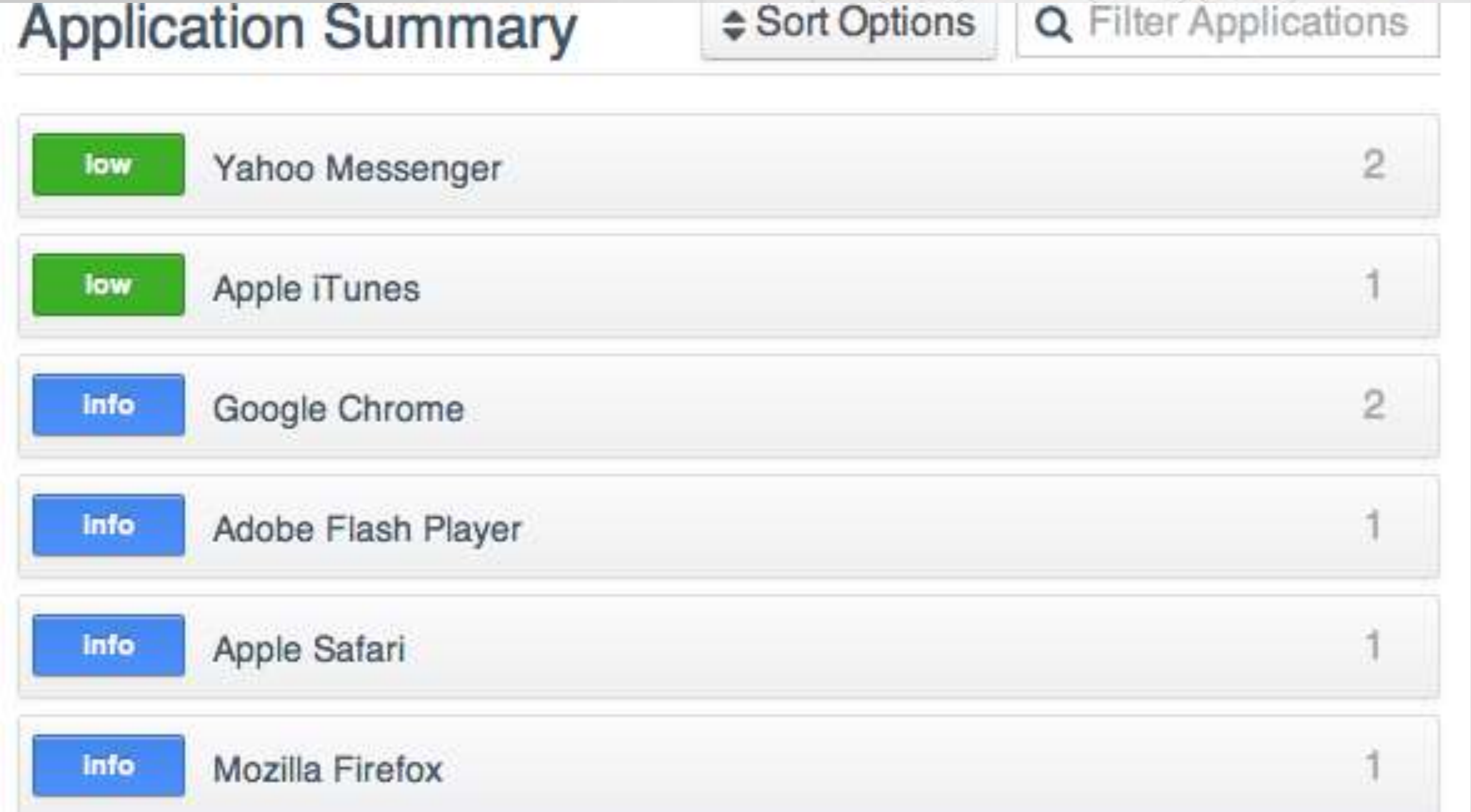
- Scan your network (frequently)
- Perform authenticated vulnerability scans
  - Servers & desktops
  - Network infrastructure
  - Virtualization platform
  - Storage systems
- Sniff your network for vulnerabilities
- Mine your logs for data

Ninja convention

Application Discovery

- Get rid of applications not supported or not in use
- Reduce your attack platform
- Less stuff to patch

Passively Detect Applications



Application Summary

low	Yahoo Messenger	2
low	Apple iTunes	1
Info	Google Chrome	2
Info	Adobe Flash Player	1
Info	Apple Safari	1
Info	Mozilla Firefox	1

The Patch Management Struggle

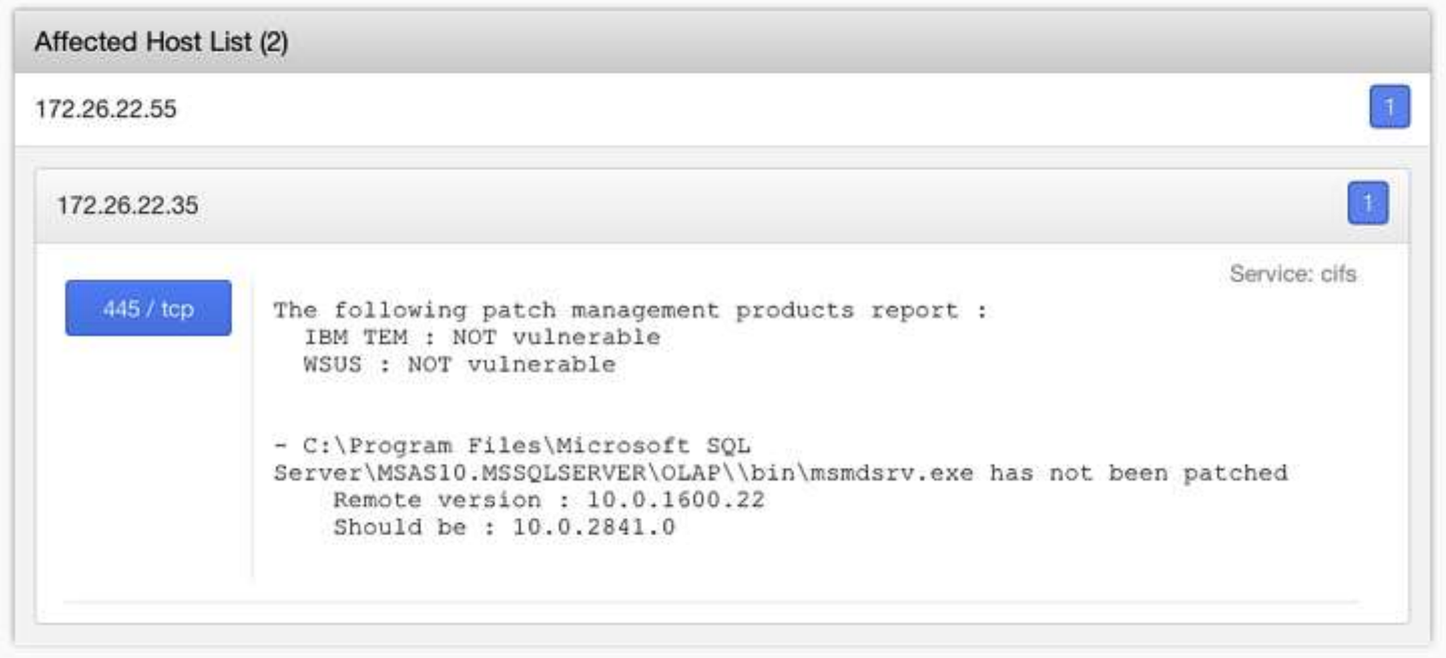
Our systems are missing patches!

Security Guy

Sysadmin

Patch Management

- Integrate vulnerability scanning with Patch Management
- Reduces troubleshooting time



```
The following patch management products report :
  IBM TEM : NOT vulnerable
  WSUS : NOT vulnerable


- C:\Program Files\Microsoft SQL
Server\MSAS10.MSSQLSERVER\OLAP\\bin\msmdsrv.exe has not been patched
    Remote version : 10.0.1600.22
    Should be : 10.0.2841.0
```

Detect Early

- Vulnerability detection happens in many ways
  - Active scanning
  - Credentialed scanning
  - Passive scanning
  - Log analysis

- Find smaller issues now, before they become larger ones

Step 4 – Prioritize & Fix

- Patch fewer things faster with more impact
- Group your vulnerabilities by:
  - Exploitability
  - Severity *
  - Critical Systems *
  - Software
  - Age

*** Warning! Danger!**

Testing Your Patches

- Look at what has been patched first, are they working? Testing done for you!
- Microsoft also does A LOT of testing for you
  - Microsoft also pulls patches back

Your ability to rollback a patch needs to be equal or greater than your ability to apply a patch

Step 5 – Lather, Rinse, & Repeat

- While :; do
  - Discover – Find all vulnerabilities
  - Test – Make sure patches work
  - Apply – Implement patches
  - Discover – Ensure remediation worked

What?

- Nessus® – Active and credentialed scanning
- Passive Vulnerability Scanner™ (PVS™) – Find the leaks
- SecurityCenter Continuous View™ – Logs as a source for vulnerability information

Nessus

Nessus®
vulnerability scanner

- Credentialed patch auditing
- Patch management Integration
- Detect mobile vulnerabilities
- Discover remotely-exploitable vulnerabilities

Nessus® PS
perimeter service

tenable
network security

PVS

- Passively detect
  - Hosts
  - Mobile devices
  - Services
  - Applications
  - Vulnerabilities
  - Connections and trust relationships

SecurityCenter

- Complete, real-time enterprise vulnerability management
- Combine data from Nessus, PVS, LCE, and other sources
- Hundreds of pre-built dashboards and reports
- Workflow management with process automation and ticketing

Tenable Resources

Blog:
http://blog.tenable.com

Podcast:
http://www.tenable.com/podcast

Videos:
http://www.youtube.com/tenablesecurity

Discussion portal:
https://discussions.nessus.org

Buy Nessus, Perimeter Service, Training, & Bundles:
https://store.tenable.com

Become a Tenable Partner:
https://www.tenable.com/partners

Try SecurityCenter and Nessus now

For more information or to evaluate SecurityCenter Continuous View:

http://www.tenable.com/products/securitycenter-continuous-view

Evaluate Nessus free for 15 days:

http://www.tenable.com/products/nessus/evaluate

tenable
network security

Questions?

????

tenable network security

Thank You

Contact us:

Paul Asadoorian – paul@nessus.org
Jack Daniel – jdaniel@tenable.com

“Vulnerabilities Exposed” webcast #2:

September 24 at 2 pm EDT

Addressing the Challenges of Virtualization