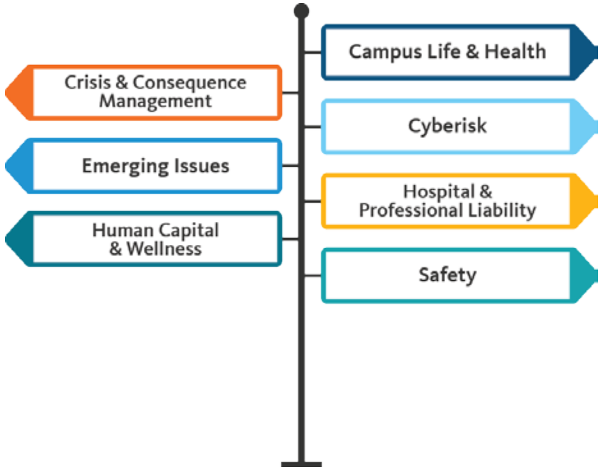
RISK SUMMIT

New Directions in Risk and Safety



Campus Life & Health

Crisis & Consequence Management

Cyberisk

Emerging Issues

Hospital & Professional Liability

Human Capital & Wellness

Safety

There is nothing on this system

Tales of doom

Presented by Robert Smith

Disclaimer

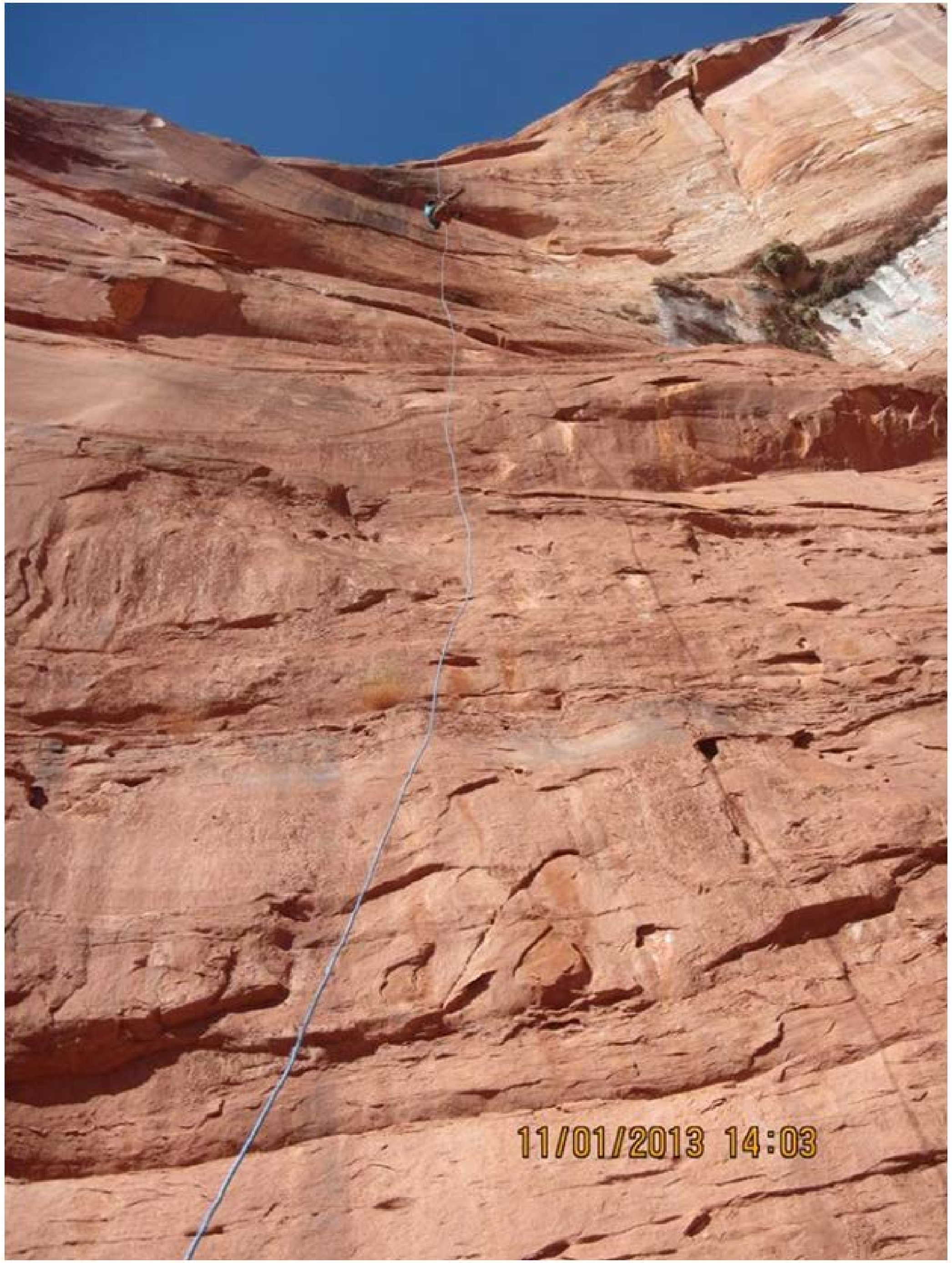
- Opinions expressed are solely my own and do not express the views or opinions of the University of California.
- This is an educational presentation.
- Case studies are simple abstractions.

Case study - North UC

- System 1 – compromised – “nothing”
  - 100% public information
- But wait, it had credentials and permissions to access to 3 other systems
  - 2 of the other systems had access to sensitive information!
- Intrusion = yes
- Information disclosure = no (lucky)
- Just the external forensics costs ~$70K and weeks of staff time!

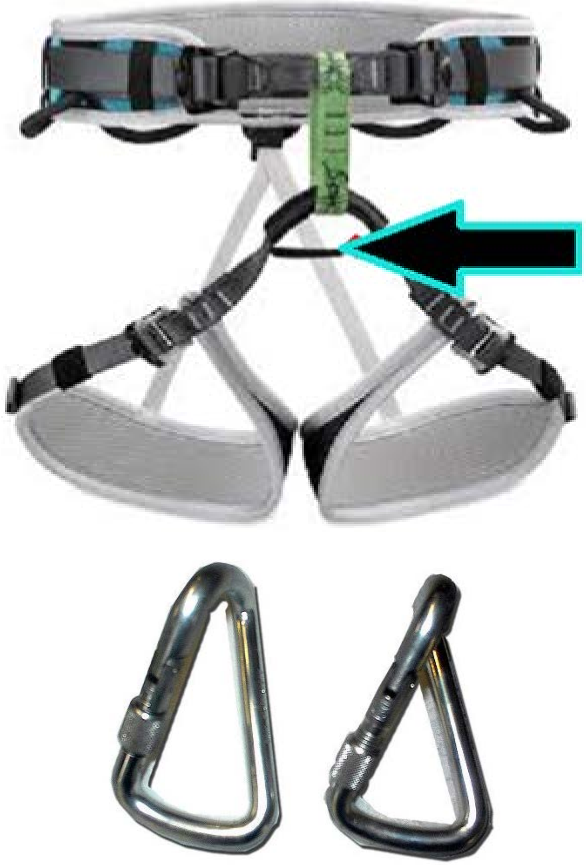
Risk Manager

Heike Noller of Denver, CO



Lake Powell in the Ticaboo Mesa area, 260’ rappel

Heike Noller of Denver, CO



Multi-sport athlete, she excelled in diving, cycling, skydiving, kickboxing and other sports
“I felt like it was nothing special anymore…and that’s, you know, the danger”.

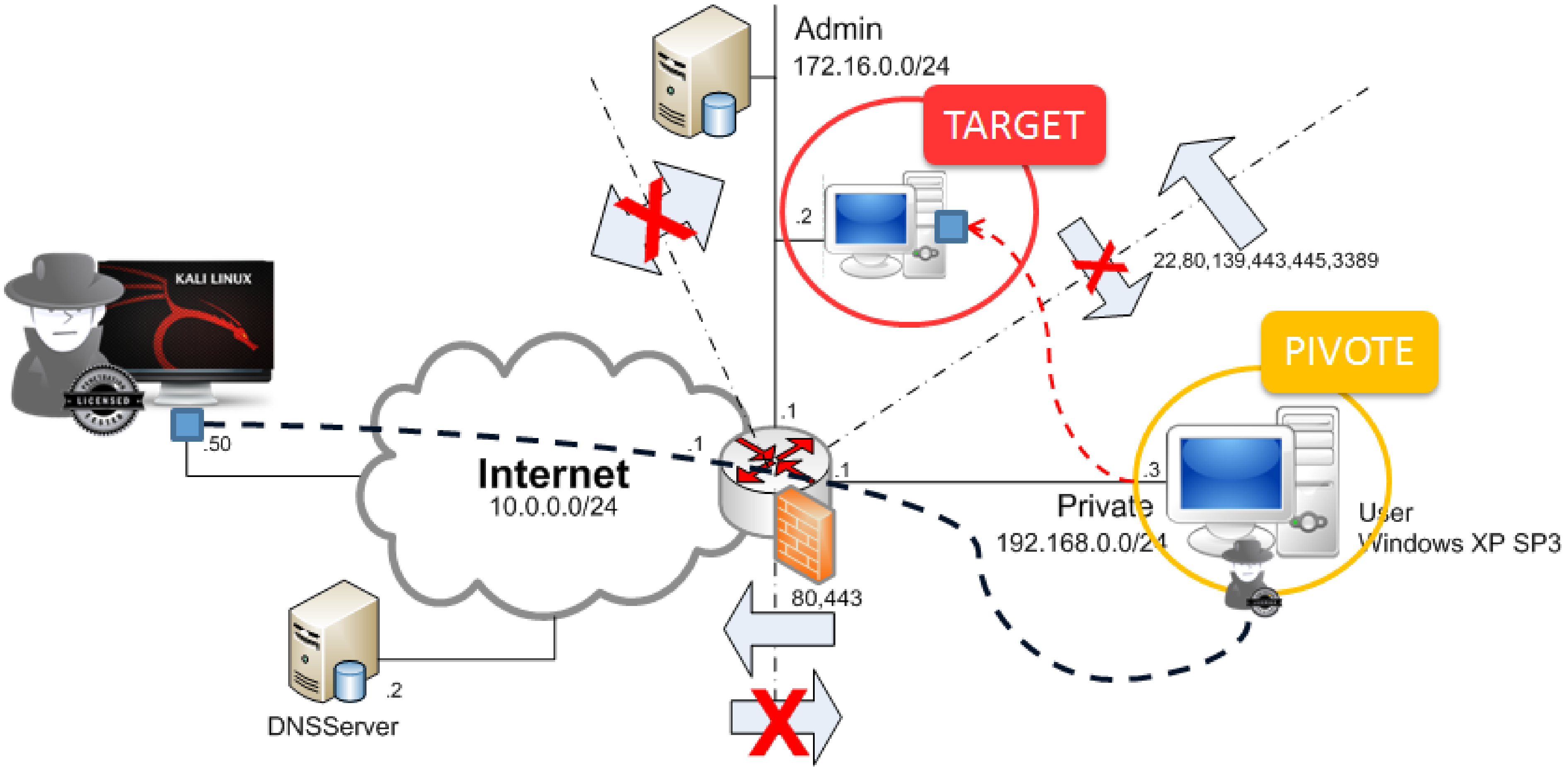
Case study – So Cal UC

- A system in admissions
- Local policy – nothing stored on PCs
- Reality – long term UC person
  - Testing applications
  - Custom reports
  - Wonderful assortment of Excel Kung Fu
  - SSNs
- $11K spent to meet “no disclosure” threshold

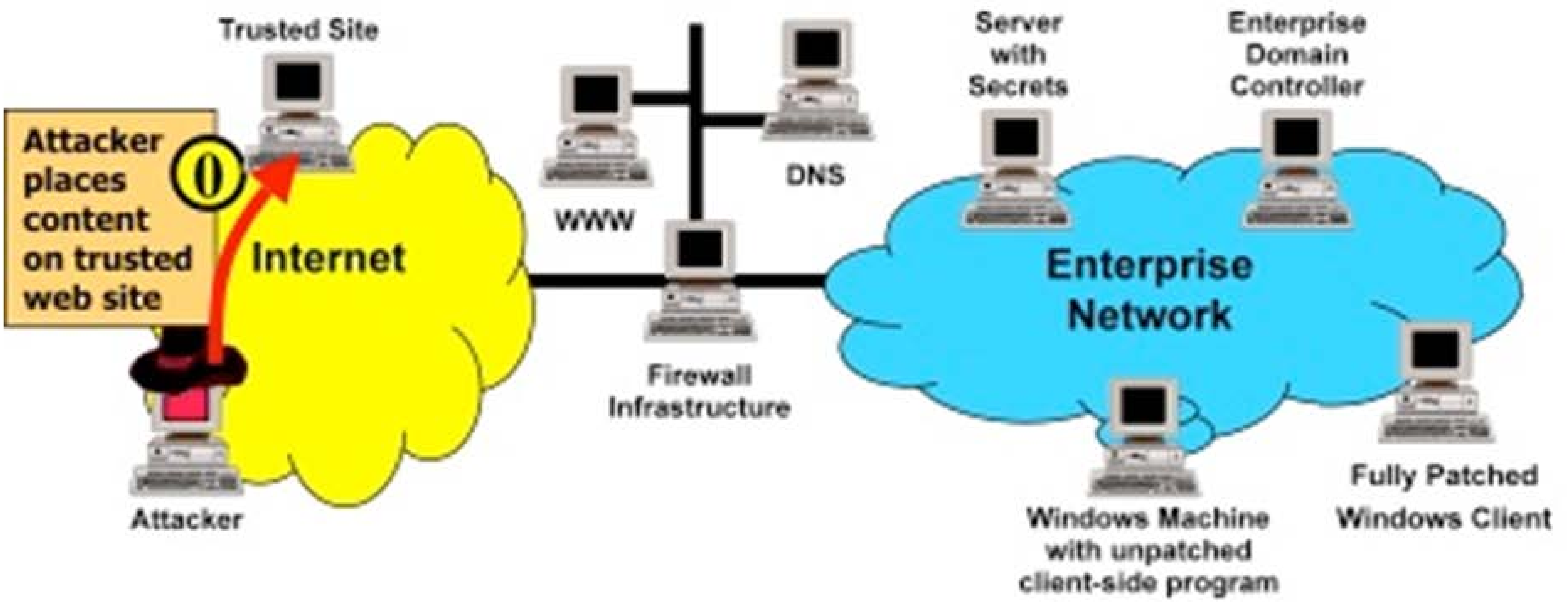
Anatomy of a pivot

ST2Labs
www.seguridadparatodos.es

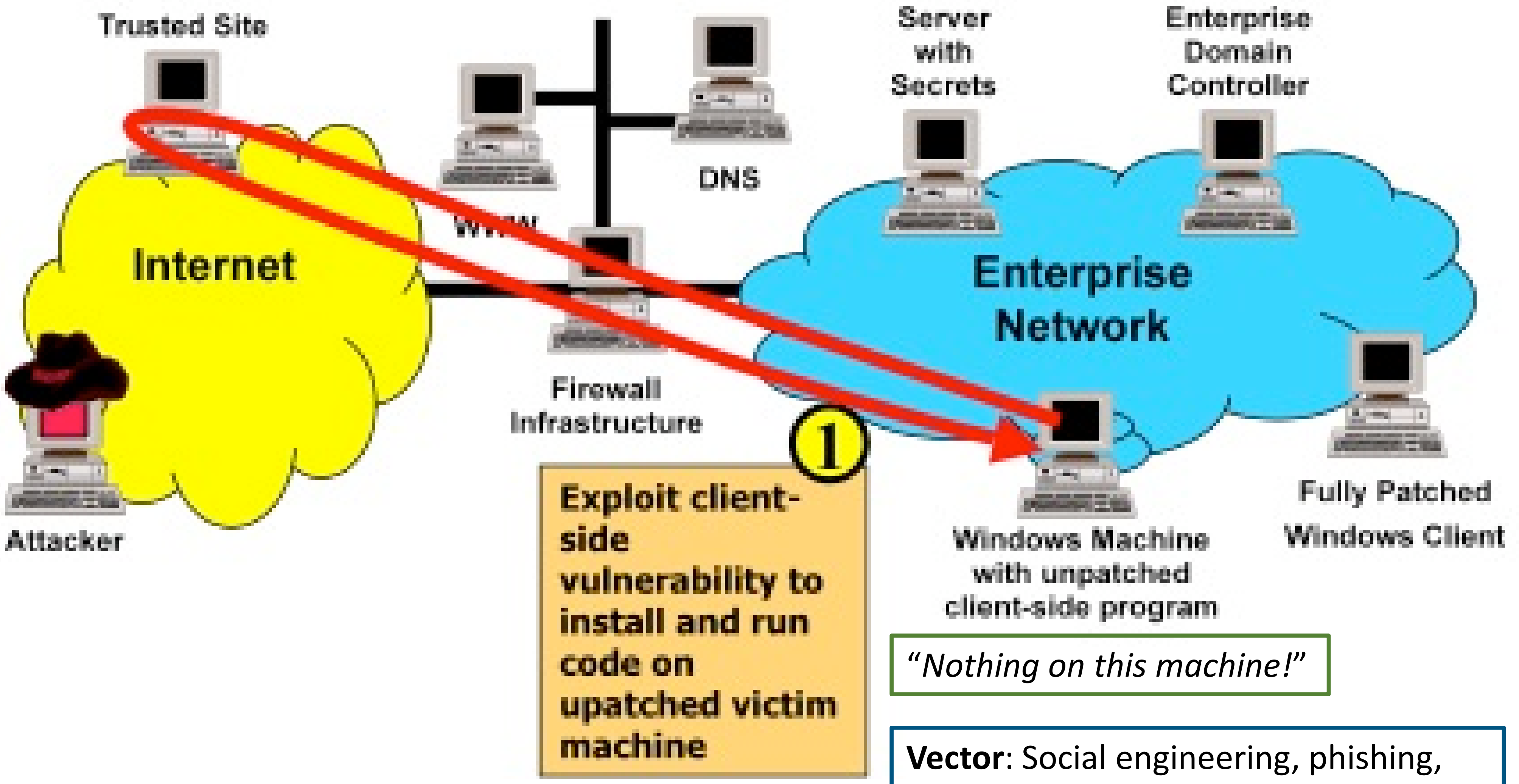
Anatomy of a pivot



Step 0: Attacker places content on trusted Site


Trusted Site
Attacker places content on trusted web site
0
Internet
Attacker
WWW
DNS
Firewall Infrastructure
Server with Secrets
Enterprise Domain Controller
Enterprise Network
Windows Machine with unpatched client-side program
Fully Patched Windows Client

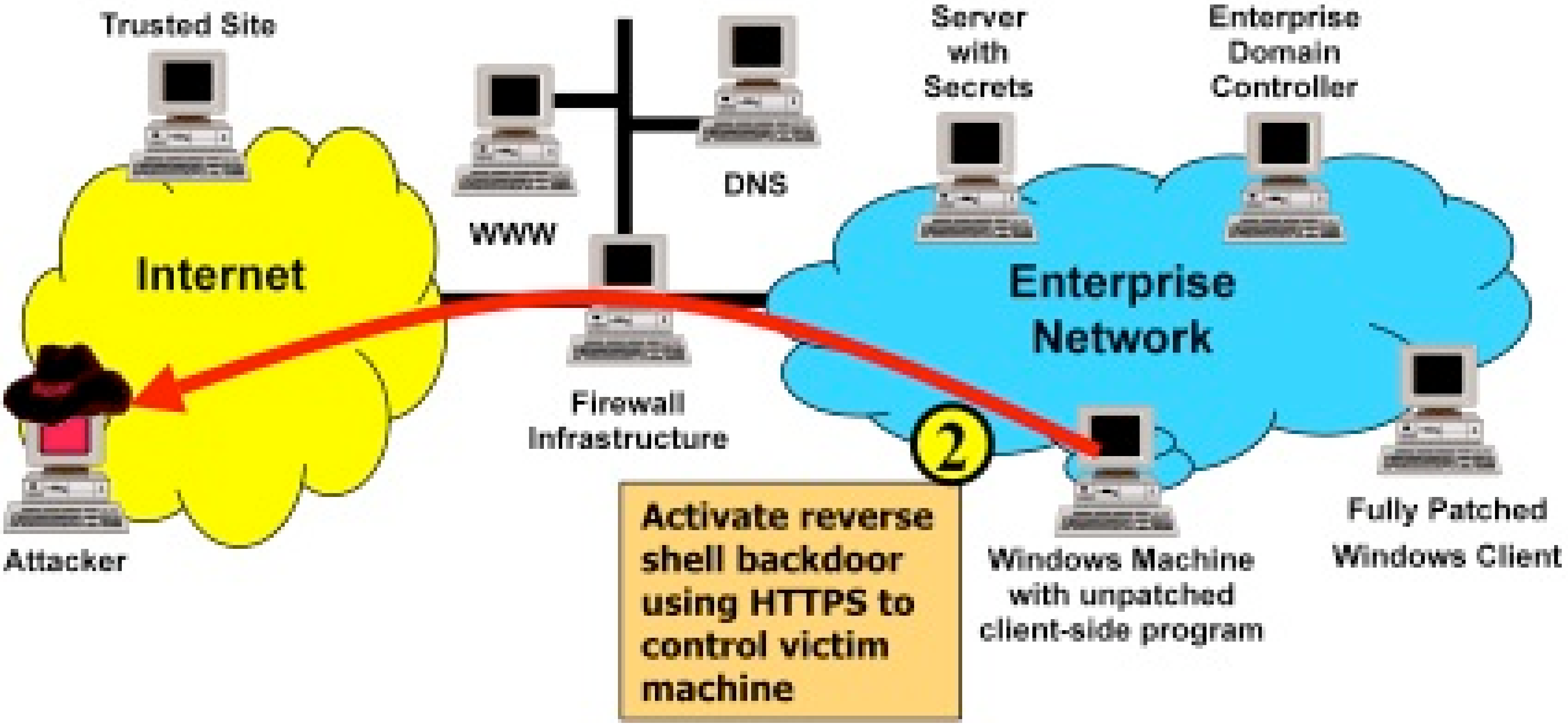
Step 1: Client-side exploitation


Trusted Site
WWW
DNS
Server with Secrets
Enterprise Domain Controller
Internet
Enterprise Network
Firewall Infrastructure
Attacker
1
Exploit client-side vulnerability to install and run code on upatched victim machine
Windows Machine with unpatched client-side program
Fully Patched Windows Client

"Nothing on this machine!"

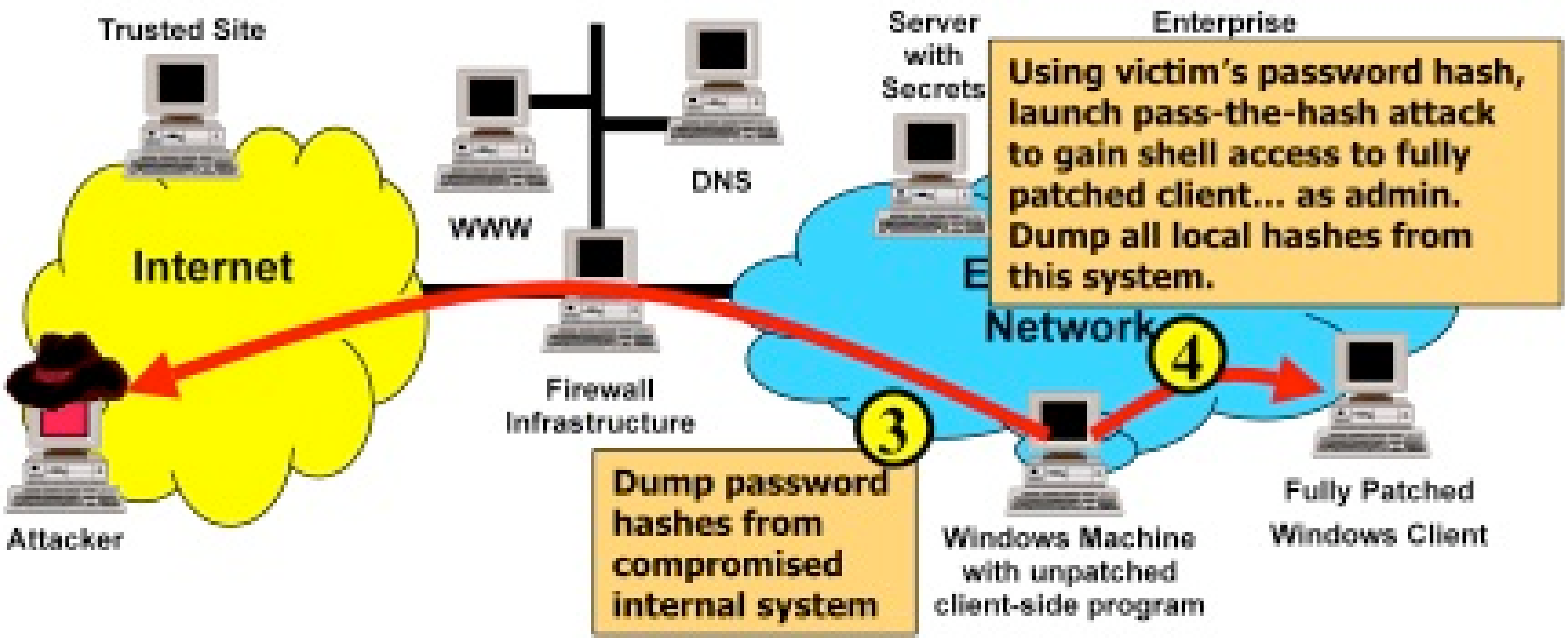
Vector: Social engineering, phishing, watering hole, spoofed e-mail

Step 2: Establish command and control – “C2”


Trusted Site
WWW
DNS
Server with Secrets
Enterprise Domain Controller
Internet
Enterprise Network
Firewall Infrastructure
Attacker
2
Windows Machine with unpatched client-side program
Fully Patched Windows Client

Activate reverse shell backdoor using HTTPS to control victim machine

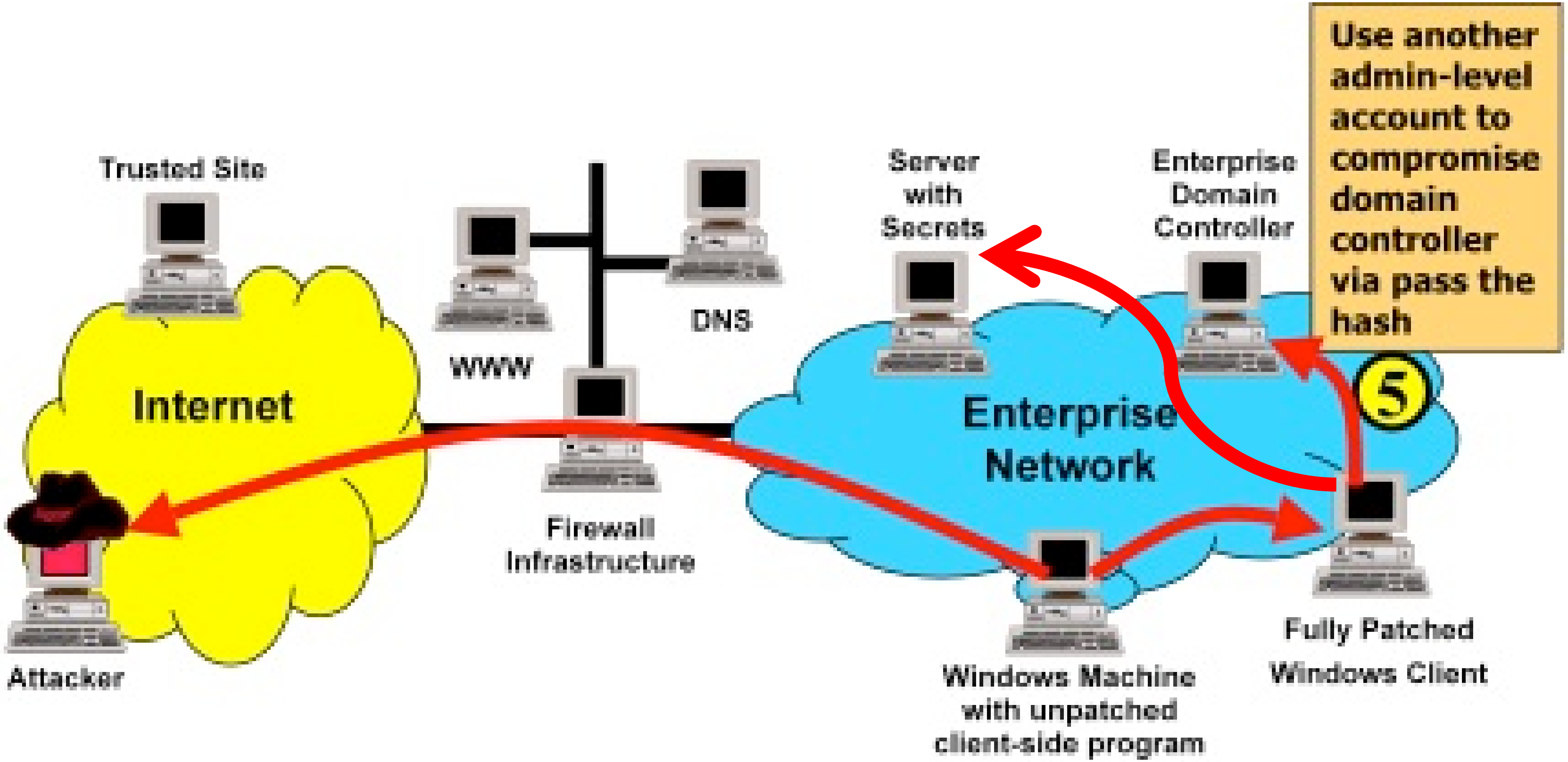
Steps 3 & 4: Dump hashes and use pass-the-hash attack to pivot



Using victim's password hash, launch pass-the-hash attack to gain shell access to fully patched client… as admin. Dump all local hashes from this system.

Dump password hashes from compromised internal system

Step 5: Pass the hash to compromise others

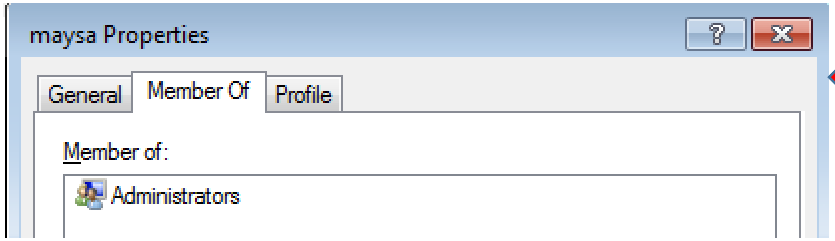

Trusted Site
WWW
DNS
Server with Secrets
Enterprise Domain Controller
Internet
Firewall Infrastructure
Enterprise Network
5
Attacker
Windows Machine with unpatched client-side program
Fully Patched Windows Client

Use another admin-level account to compromise domain controller via pass the hash

Steps 6 and 7: Exfiltration

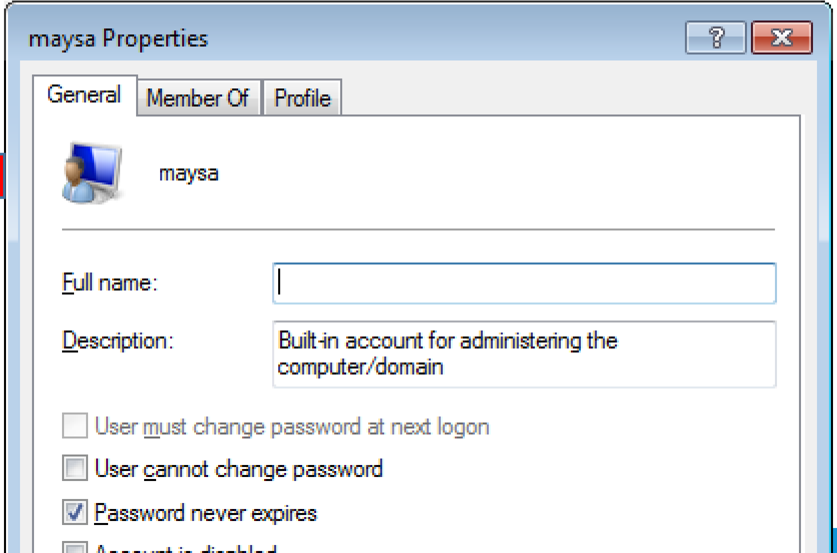
- “Nothing”
  - Account information
    - Credentials
    - Help Desk
  - Web history
  - Network history
  - Key loggers
    - Everything **every** user does

- “Sensitive information”
  - Financial Aid
  - PHI
  - Employee records
  - FERPA
  - Research
  - PCI – credit cards


maysa Properties

Member of:

Administrators


maysa Properties

maysa

Full name:

Description: Built-in account for administering the computer/domain

☐ User must change password at next logon

☐ User cannot change password

☑ Password never expires

☐ Account is disabled

Case Study – North UC

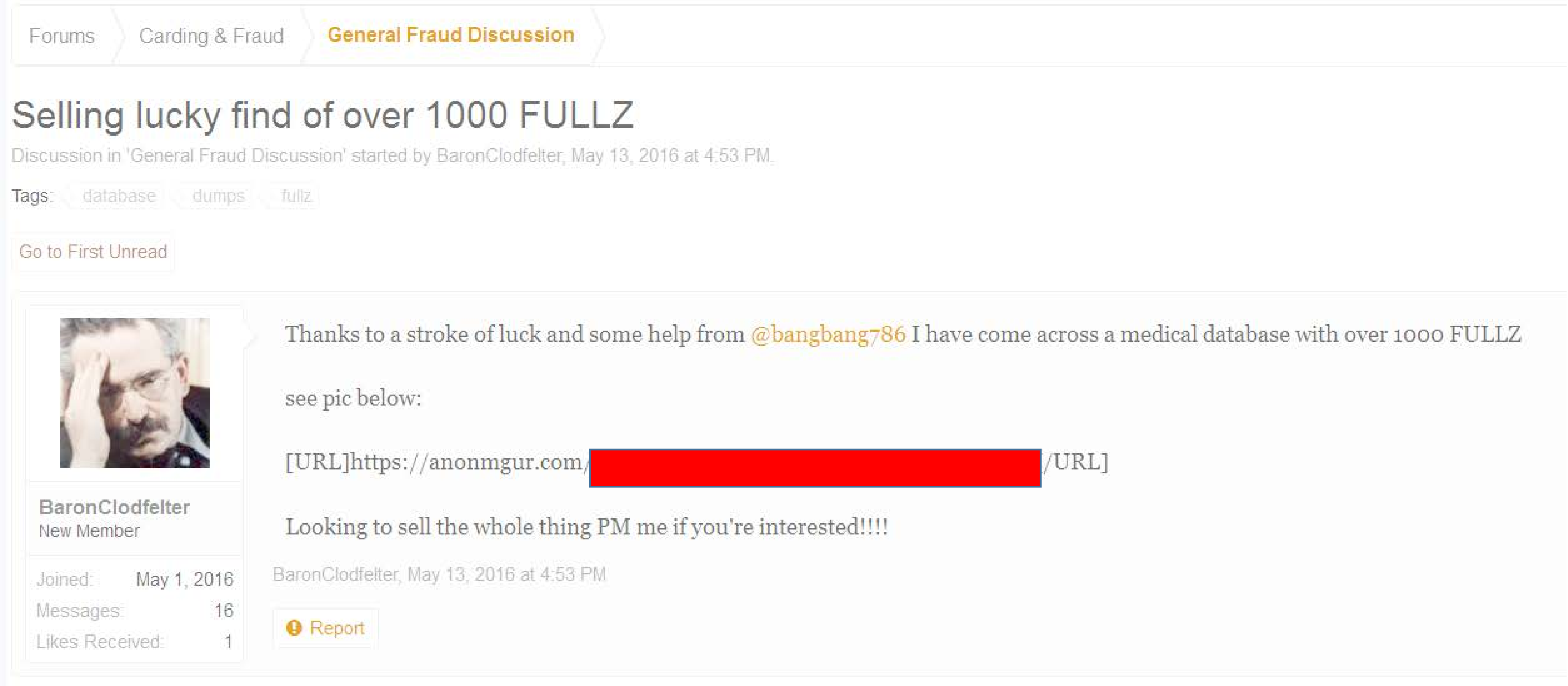
- 3 systems impacted
  - Attackers entered through one system
  - Unpatched Java on one system let the attackers in
    - Researcher had simply visited a popular website offering help on the use of Microsoft Excel formulas.
- But wait!
  - 30K files encrypted
    - "… which contained critical data collected for several ongoing multi-year studies."
  - Some data lost forever …
  - "Had we been subject to the HIPAA regulations or if the terms of our grants had included requirements that we meet federal information security standards, we could have faced millions of dollars in fines, termination of our grants, and the potential for an adverse determination in future grant applications."

How hard is this?

Video Demo

- Part 1: https://youtu.be/a08m53W3xUw
- Part 2: https://youtu.be/4sKFKNyMw8Y

How hard is this?



Forums › Carding & Fraud › General Fraud Discussion

Selling lucky find of over 1000 FULLZ

Discussion in 'General Fraud Discussion' started by BaronClodfelter, May 13, 2016 at 4:53 PM.

Tags: database dumps fullz

Go to First Unread

BaronClodfelter
New Member

Joined:	May 1, 2016
Messages:	16
Likes Received:	1

Thanks to a stroke of luck and some help from @bangbang786 I have come across a medical database with over 1000 FULLZ

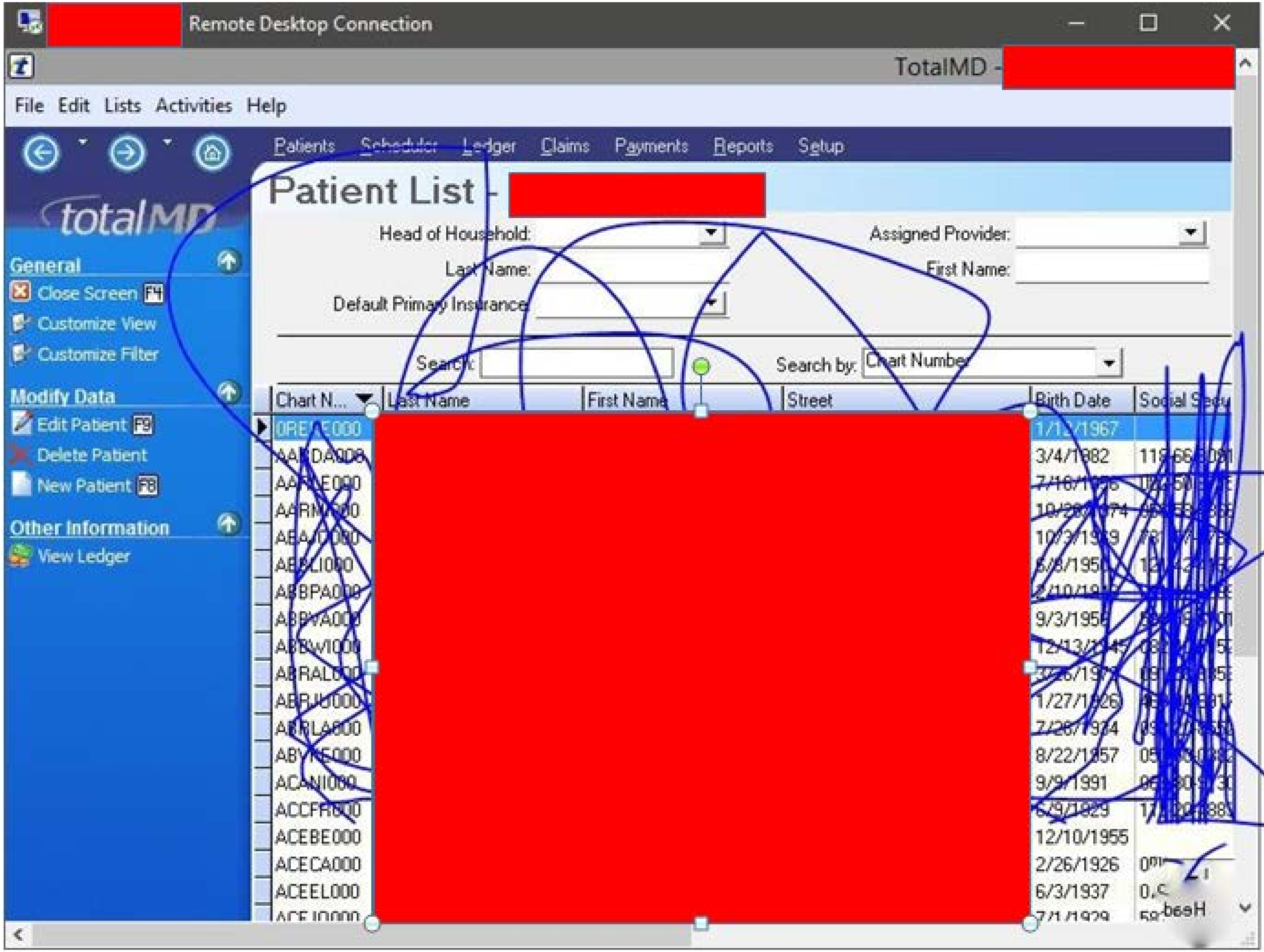
see pic below:

[URL]https://anonmgur.com/[redacted]/URL]

Looking to sell the whole thing PM me if you're interested!!!!

BaronClodfelter, May 13, 2016 at 4:53 PM

Report



[redacted] Remote Desktop Connection

TotalMD - [redacted]

Patient List - [redacted]

Head of Household:

Assigned Provider:

Last Name:

First Name:

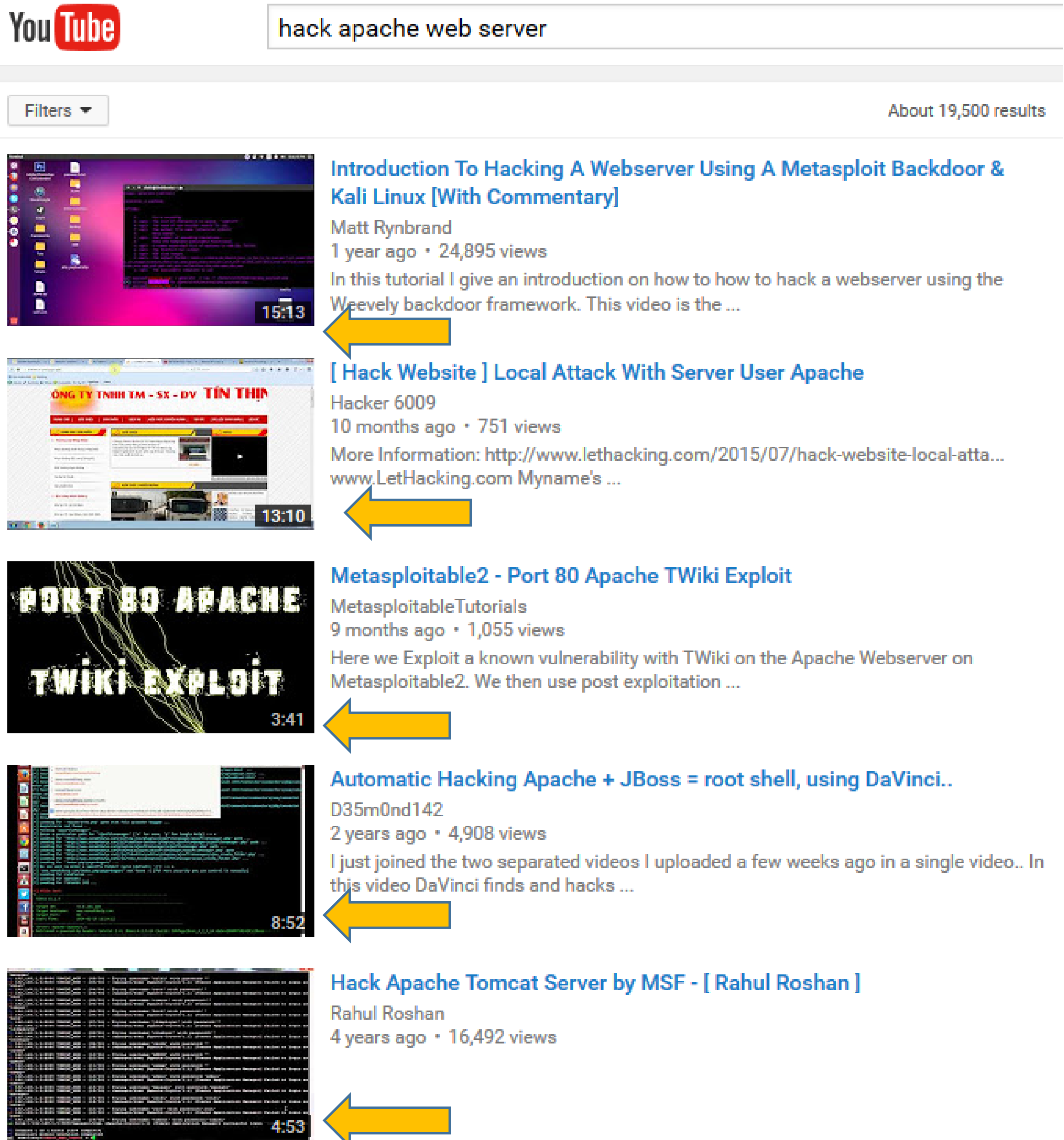
Default Primary Insurance:

Search:

Search by: Chart Number

Chart N...	Last Name	First Name	Street	Birth Date	Social Secu...
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	8/22/1957	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	9/9/1991	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
ACEBE000	[redacted]	[redacted]	[redacted]	12/10/1955	
ACECA000	[redacted]	[redacted]	[redacted]	2/26/1926	[redacted]
ACEEL000	[redacted]	[redacted]	[redacted]	6/3/1937	[redacted]
ACEJO000	[redacted]	[redacted]	[redacted]	7/1/1929	[redacted]

YouTube



hack apache web server

Filters ▾

About 19,500 results

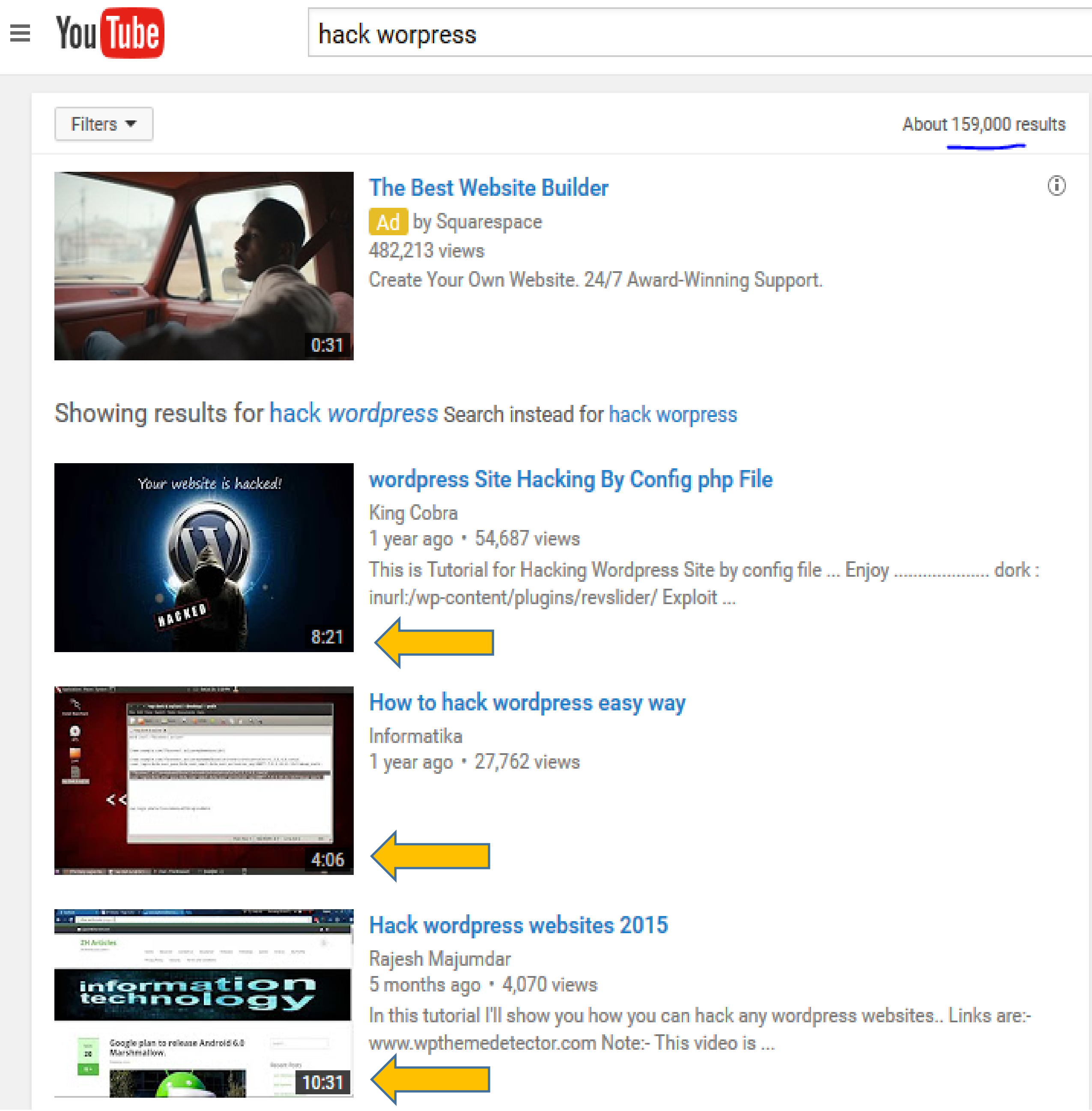
Introduction To Hacking A Webserver Using A Metasploit Backdoor & Kali Linux [With Commentary]
Matt Rynbrand
1 year ago • 24,895 views
In this tutorial I give an introduction on how to how to hack a webserver using the Weevely backdoor framework. This video is the ...
15:13

[Hack Website] Local Attack With Server User Apache
Hacker 6009
10 months ago • 751 views
More Information: http://www.lethacking.com/2015/07/hack-website-local-atta... www.LetHacking.com Myname's ...
13:10

Metasploitable2 - Port 80 Apache TWiki Exploit
MetasploitableTutorials
9 months ago • 1,055 views
Here we Exploit a known vulnerability with TWiki on the Apache Webserver on Metasploitable2. We then use post exploitation ...
3:41

Automatic Hacking Apache + JBoss = root shell, using DaVinci..
D35m0nd142
2 years ago • 4,908 views
I just joined the two separated videos I uploaded a few weeks ago in a single video.. In this video DaVinci finds and hacks ...
8:52

Hack Apache Tomcat Server by MSF - [Rahul Roshan]
Rahul Roshan
4 years ago • 16,492 views
4:53



hack worpress

Filters ▾

About 159,000 results

The Best Website Builder
Ad by Squarespace
482,213 views
Create Your Own Website. 24/7 Award-Winning Support.
0:31

Showing results for hack *wordpress* Search instead for hack worpress

wordpress Site Hacking By Config php File
King Cobra
1 year ago • 54,687 views
This is Tutorial for Hacking Wordpress Site by config file ... Enjoy .... dork : inurl:/wp-content/plugins/revslider/ Exploit ...
8:21

How to hack wordpress easy way
Informatika
1 year ago • 27,762 views
4:06

Hack wordpress websites 2015
Rajesh Majumdar
5 months ago • 4,070 views
In this tutorial I'll show you how you can hack any wordpress websites.. Links are:- www.wpthemedetector.com Note:- This video is ...
10:31

Case Study - So Cal UC - Nothing

- Compromised web server
- Got admin credentials
- Got onto a system with nothing on it
  - But wait
  - That system had visibility to 500+ more systems
  - And the attacker was now “admin”
- Ransomware!
- Just the forensics > $50K
  - + org impact
- Near miss

Wrap

Summary

- Climbing third hand
  - “Not too long ago, people thought that backing up rappels was strictly for sissies, or something you'd only resort to in special situations - bringing down an injured or incompetent climber, for example.”
  - Today - virtually every guide and climbing safety course teaches the use of an autoblock or third hand.
    - We assume something will go wrong
      - Many points of failure
    - Known good way reduce risk!

- Nothing on that system
  - Asymmetry of information security
    - The good guys have to protect all the points of entry ….
    - Christoffer - “A defender can never win, he can only delay the inevitable, the eventual victorious attacker. The defender have to protect against all attacks, arguably a somewhat difficult task.”
  - The bad guys just need one way in.
  - Asymmetric warfare is war between combatants whose relative power differs significantly or whose strategies or tactics differ significantly.
  - Even systems with nothing on them need to be appropriately secured.
    - Known good way to reduce risk!
    - Information security third hand

Sources

- https://www.sans.org/

SANS the most trusted source for computer security training, certification, and research www.sans.org

- Backpacker Magazine - 2016
- http://canyoncollective.com

CANYON COLLECTIVE

- Video demo of pivot attack
  - Brandon McCann
  - https://youtu.be/a08m53W3xUw
  - https://youtu.be/4sKFKNyMw8Y

Contact Page

Email: robert.smith@ucop.edu

Phone: (510) 587-6244