How Breaches Really Happen

10-D Security

www.10dsecurity.com

©2016 10-D, Inc. All Rights Reserved.

About 10-D Security

- Dedicated Information Security Firm
- Clients Nationwide, primarily in financial industry
- Services
  - Penetration Testing
  - Social Engineering
  - Vulnerability Scanning
  - IT Audits
  - Web Application Assessment
  - Incident Response & Forensic Investigation
  - Threat Detection

©2016 10-D, Inc. All Rights Reserved.

About The Presenter

Scott Burkhart

- GCIA GIAC Certified Intrusion Analyst
- GCFA GIAC Certified Forensic Analyst
- MCSE Microsoft Certified Systems Engineer
- Former U.S. Army
- Former Kansas Firefighter/EMT

©2016 10-D, Inc. All Rights Reserved.

What We Will Cover Today

- Attackers and their methods
- Security Breach examples
- Breach demonstration
- Defensive countermeasures

©2016 10-D, Inc. All Rights Reserved.

Attackers – Who are we talking about?

- Cyber-criminals
- Hacktivists
- Nation-states and militaries

10-D Security

Securing Information One Client at a Time

©2016 10-D, Inc. All Rights Reserved.

What do they want?

That depends:

- Cyber-criminals – Money
- Hacktivists – Attention/Retribution
- Nation-states – Information/Access/Infrastructure

©2016 10-D, Inc. All Rights Reserved.

“We don’t have anything anyone would want!”

<u>Everyone</u> is a target.

- Intended target
- Opportunity
- Resource

10-D Security

Securing Information One Client at a Time

©2016 10-D, Inc. All Rights Reserved.

Attack Goals

- Installation of Malware
- Direct theft of information, such as passwords
- Direct monetary gain, such as ACH/Wire fraud, Client Data (CC#, PII)
- Information to be used in future attacks
- Denial of Service

©2016 10-D, Inc. All Rights Reserved.

How do you attack a fortress?

Have someone let you in…

©2016 10-D, Inc. All Rights Reserved.

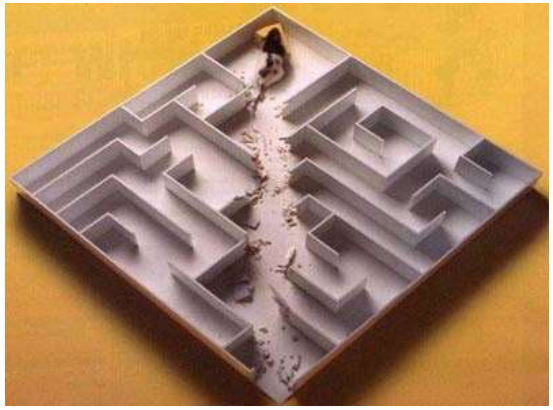
Data Breaches…most start with an email

- Target – 2013
  - Started with phishing attack at vendor
- Home Depot – 2014
  - Started by vendor compromise, likely via email
- Sony – 2015
  - Started with spear-phishing attack directed at employees
- Anthem & Premera Healthcare– 2015
  - Attackers used look-alike domains, using targeted emails to get users to visit them

©2016 10-D, Inc. All Rights Reserved.

Email Attacks – The path of least resistance

- Phishing
- Spear Phishing
- Goal is to trick the user into opening the attachment or clicking the link



©2016 10-D, Inc. All Rights Reserved.

If you click the link, “Bad Things” will happen

- Link points to an “Exploit Server”, which will try to install malware.
- Links can also point to a forged website, trying to get you to log in, giving them your password.
- Attachments can contain malicious code, or redirect to exploit servers.

©2016 10-D, Inc. All Rights Reserved.

What about Antivirus and Antimalware?

- If you are solely relying on AV for protection then you're doing it wrong
- AV catches known\bulk malware only
- Useless against targeted attacks

©2016 10-D, Inc. All Rights Reserved.

How many phishing emails does it take to get to the tootsie-roll center of your network?

- 23% of recipients open phishing emails
- 11% will open an attachment
- A phishing campaign sent to 50 people will net 5-6 victims
- Time-to-first-click generally under two minutes.

Source: Verizon Enterprise, “2015 Data Breach Investigations Report”

10-D Security

Securing Information One Client at a Time

©2016 10-D, Inc. All Rights Reserved.

Name	Target Groups	Template	Education	Links	Posts	End Time
KBSB-3	KBSB-3	Mailbox migration tool download v2	10-D ASP Redirect [Metasploit Download - mailboxupgrade.hta]	31	0	April 7, 2016, 3:56 pm
CCB Test2	DonB CCB	10-D 8-5-14 Amazon PS4 Shipping Notice	10-D ASP Redirect [SMB Hash Grabber]	0	0	April 7, 2016, 9:11 am
CCB Test1	DonB CCB	KC Banking News JSJ	10-D ASP Redirect [SMB Hash Grabber]	0	0	April 7, 2016, 9:12 am
CCB-Harvest2	ccb-harvest	10-D 8-5-14 Amazon PS4 Shipping Notice	10-D ASP Redirect [SMB Hash Grabber]	11	0	April 6, 2016, 9:50 am
KBSB-2	KBSB-2	Banking News - Iowa	10-D ASP Redirect [SMB Hash Grabber]	38	0	April 6, 2016, 8:54 am
CCB-harvest	ccb-harvest	KC Banking News JSJ	10-D ASP Redirect [SMB Hash Grabber]	36	0	April 5, 2016, 3:33 pm
KBSB-1	KBSB-1	Target In Store Pickup -XBOX One	10-D ASP Redirect [Metasploit Download - invoice.pdf.hta]	37	0	April 5, 2016, 11:44 am
FNBP2	FNBP1	Kansas Banking News JSJ	10-D ASP Redirect [SMB Hash Grabber]	23	0	March 30, 2016, 10:40 am

10-D Security

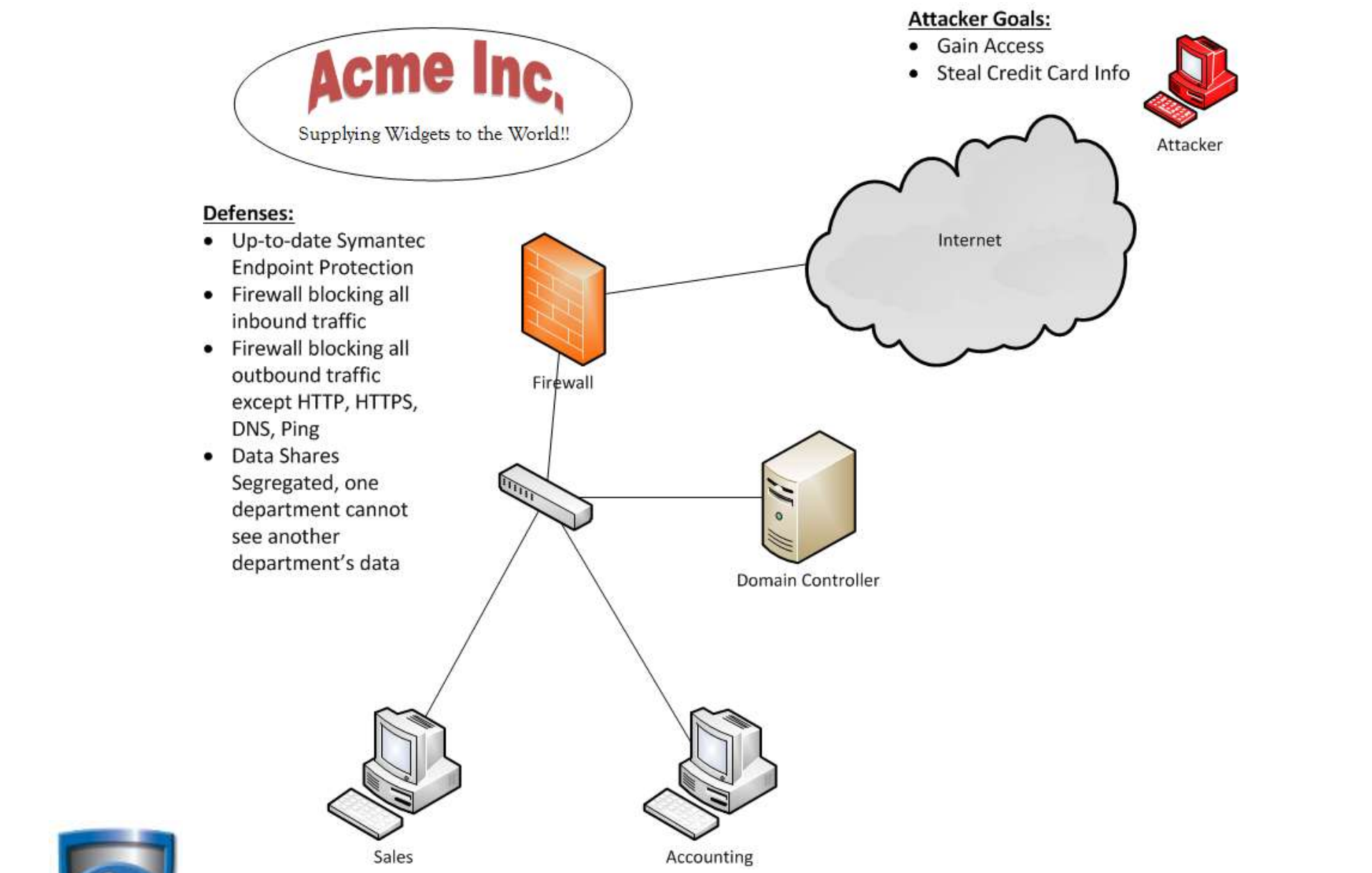
Securing Information One Client at a Time

©2016 10-D, Inc. All Rights Reserved.

Anatomy of a Compromise

1. Recon
2. Phishing and Initial Breach
3. Credential and Information Gathering
4. Increase Access and Lateral Movement
5. Execute Objectives

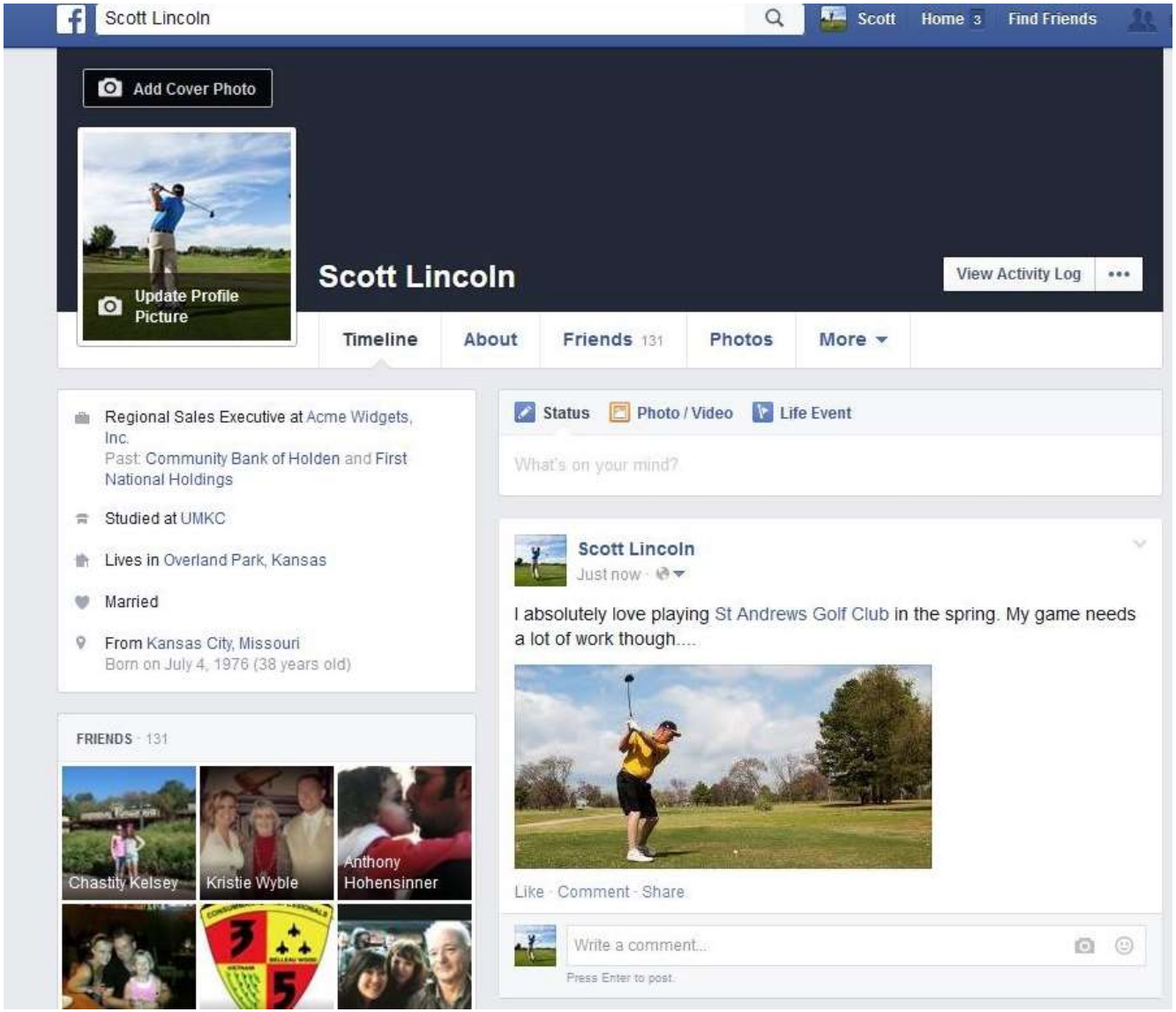
©2016 10-D, Inc. All Rights Reserved.



10-D Security

Securing Information One Client at a Time

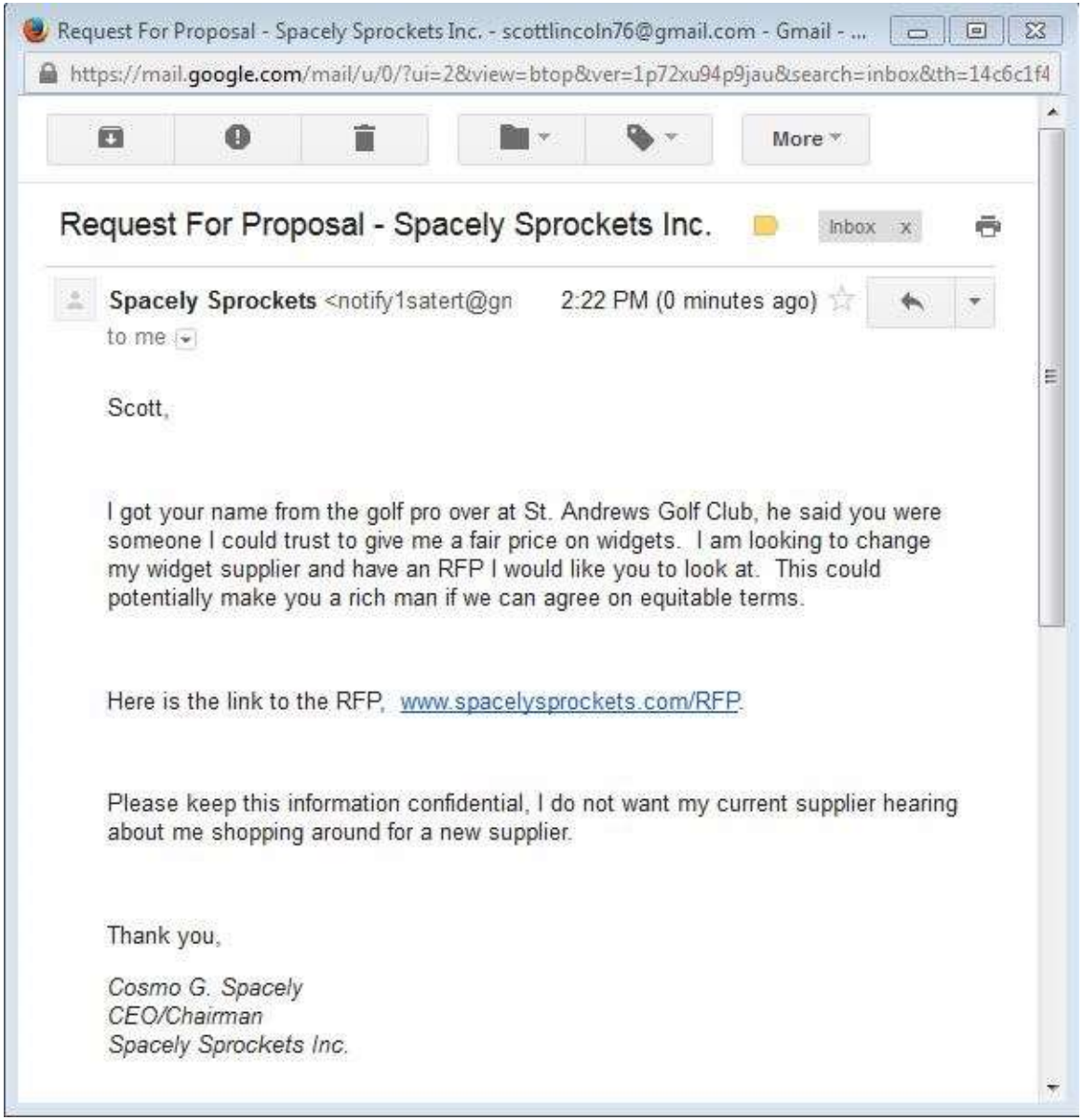
©2016 10-D, Inc. All Rights Reserved.



10-D Security

Securing Information One Client at a Time

©2016 10-D, Inc. All Rights Reserved.

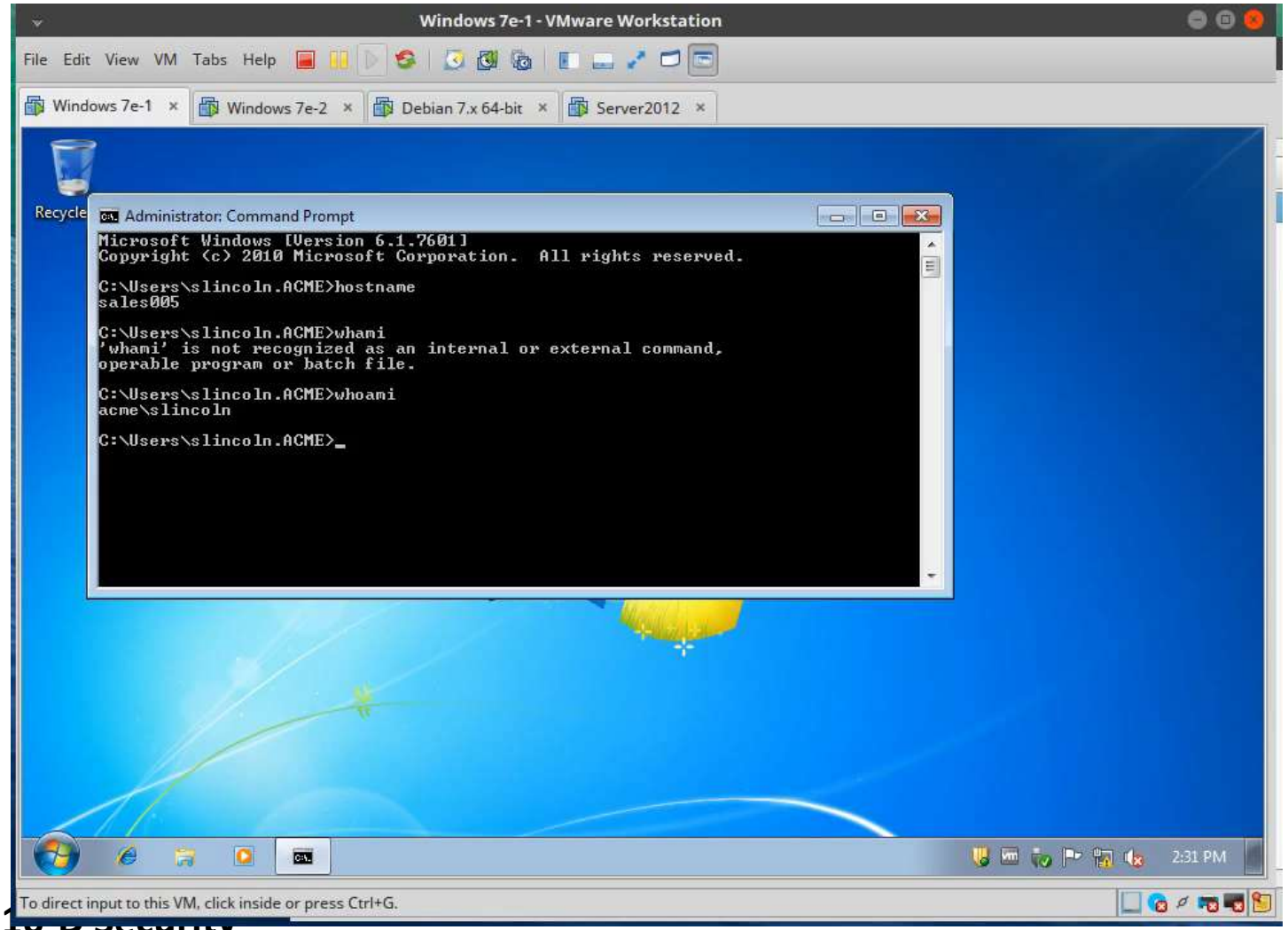


10-D Security

Securing Information One Client at a Time

©2016 10-D, Inc. All Rights Reserved.

Demo Time



©2016 10-D, Inc. All Rights Reserved.

Acme Inc,

Supplying Widgets to the World!!

April 1st, 2015

Joe Customer
123 Any Street
Small Town, KS 12345

Mr. Customer,

We are contacting you because we have learned of a serious data security incident that occurred on or between January 1st and March 24th 2015 that involved some of your personal information.

The breach involved customer names, mailing addresses, credit card numbers and in some cases card security codes.

We are notifying you so you can take action along with our efforts to minimize or eliminate potential harm. We have also notified several major credit reporting agencies and financial

10-D Security

Securing Information One Client at a Time

©2016 10-D, Inc. All Rights Reserved.

Defense in Depth

- Determined attackers will figure out how to bypass security controls
- Layers of security will slow them down and increase chances of detection
- Shiny new appliances are not the answer
- CIS Critical Security Controls

©2016 10-D, Inc. All Rights Reserved.

Make Reconnaissance Harder

- Be aware of publicly available information
  - Domain Registrations
  - Vendor Case Studies
  - Corporate Websites – No Employee Directories!
  - Social Media
  - Scrub all Metadata

©2016 10-D, Inc. All Rights Reserved.

Prevent the initial breach

- Web Filter Whitelisting
- Security Awareness Training
- Social Engineering Testing
- CIS Critical Security Controls

10-D Security

Securing Information One Client at a Time

©2016 10-D, Inc. All Rights Reserved.

If attackers get in, make them work

- Don’t allow normal users admin rights!
- Use Least Privilege practices on data shares
- Use strong passphrases, > 12 characters complex

©2016 10-D, Inc. All Rights Reserved.

Early Warning

- The Bad Guys will get in, but will you see them?
- Log Everything
  - Inbound
  - Outbound
  - Internal

©2016 10-D, Inc. All Rights Reserved.

Critical Takeaways for Defenders

- An attack will most likely start from the inside
- Attackers will start with access to a user account
- Controls will fail, layers are the key
- You can’t stop what you can’t see – visibility is vital

©2016 10-D, Inc. All Rights Reserved.

CIS Critical Security Controls V.6

(www.cisecurity.org/critical-controls)

- **CSC 1: Inventory of Authorized and Unauthorized Devices**
- **CSC 2: Inventory of Authorized and Unauthorized Software**
- **CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers**
- **CSC 4: Continuous Vulnerability Assessment and Remediation**
- **CSC 5: Controlled Use of Administrative Privileges**
- **CSC 6: Maintenance, Monitoring, and Analysis of Audit Logs**
- **CSC 7: Email and Web Browser Protections**
- **CSC 8: Malware Defenses**
- **CSC 9: Limitation and Control of Network Ports, Protocols, and Services**
- **CSC 10: Data Recovery Capability**
- **CSC 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches**
- **CSC 12: Boundary Defense**
- **CSC 13: Data Protection**
- **CSC 14: Controlled Access Based on the Need to Know**
- **CSC 15: Wireless Access Control**
- **CSC 16: Account Monitoring and Control**
- **CSC 17: Security Skills Assessment and Appropriate Training to Fill Gaps**
- **CSC 18: Application Software Security**
- **CSC 19: Incident Response and Management**
- **CSC 20: Penetration Tests and Red Team Exercises**

10-D Security

Securing Information One Client at a Time

©2016 10-D, Inc. All Rights Reserved.

Questions?

10-D Security

Securing Information One Client at a Time

©2016 10-D, Inc. All Rights Reserved.

THANK YOU!!!

10-D Security

Securing Information One Client at a Time

©2016 10-D, Inc. All Rights Reserved.