

Cyber Security Technologies

Session 1c – Security Overview

Shawn Davis
ITMS 448 – Spring 2016

Overview

1. Important Security Concepts
2. Core Security Principals (CIA)
3. Inside Threats
4. Outside Threats
5. Recent Popular Security Threats

Definition of Computer Security



**National Institute of
Standards and Technology**
U.S. Department of Commerce

“Measures and controls that ensure confidentiality, integrity, and availability of information system assets including hardware, software, firmware, and information being processed, stored, and communicated.”

Part 1

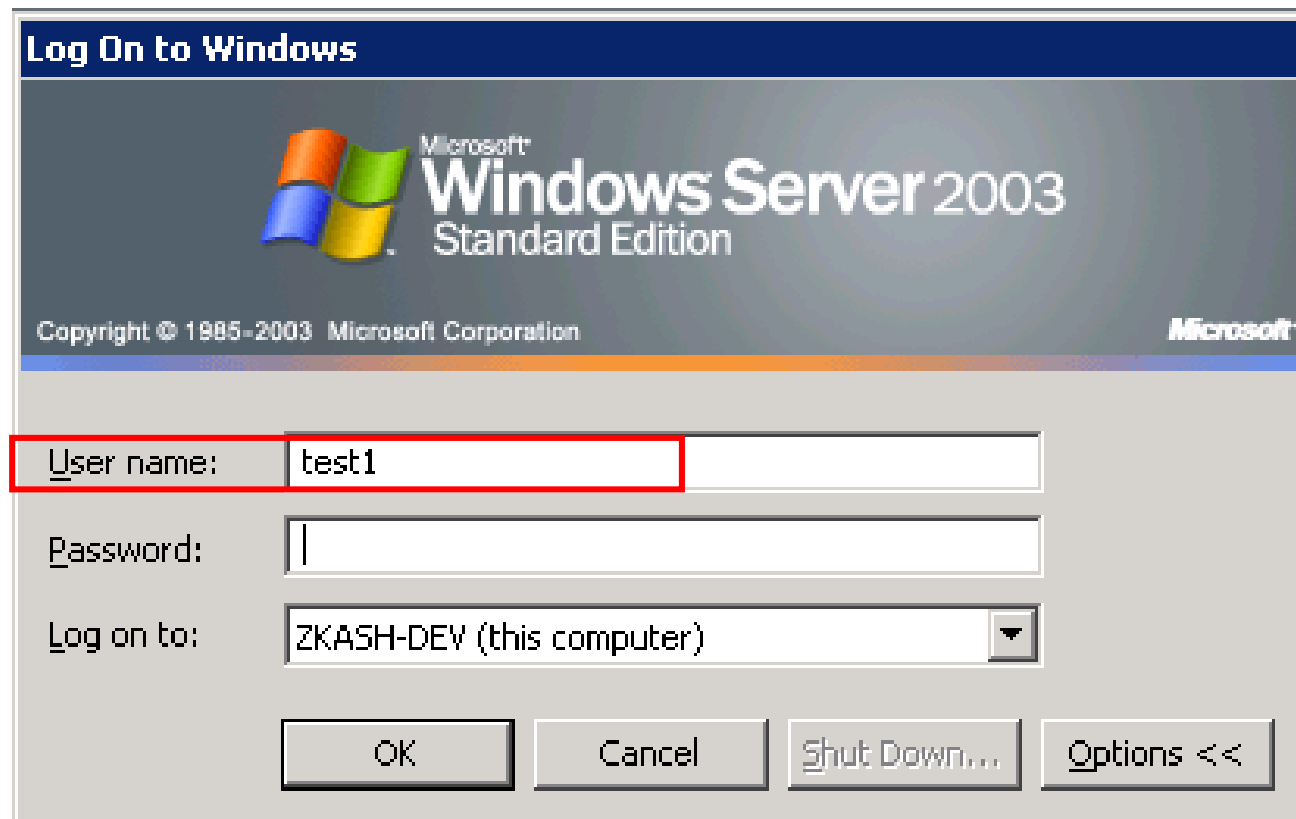
Important Security Concepts

Important Security Concepts

- Identification
- Authenticity
- Authorization
- Access Control
- Accountability
- Non-repudiation

Identification:

- Professing an identity:



The image shows a screenshot of the 'Log On to Windows' dialog box from Windows Server 2003. The dialog box has a blue header bar with the text 'Log On to Windows'. Below the header, there is a large area with the Windows logo and the text 'Microsoft Windows Server 2003 Standard Edition'. Below this, it says 'Copyright © 1985-2003 Microsoft Corporation' and the Microsoft logo. The main area of the dialog box is light gray and contains three input fields: 'User name:' with the text 'test1', 'Password:', and 'Log on to:' with a dropdown menu showing 'ZKASH-DEV (this computer)'. At the bottom, there are four buttons: 'OK', 'Cancel', 'Shut Down...', and 'Options <<'. A red rectangular box highlights the 'User name:' label and the 'test1' text in the input field.

Log On to Windows

Microsoft Windows Server 2003 Standard Edition

Copyright © 1985-2003 Microsoft Corporation

Microsoft





User name: test1

Password:

Log on to: ZKASH-DEV (this computer)

OK Cancel Shut Down... Options <<

Authenticity

- Property of being genuine, verifiable, and trusted
 - Something you know:
 - 
 - 
 - Something you have:
 - 
 - Something you are:
 - 

Authentication

- Confirming an identity in order to access an object

Profess Identity

Verify Identity

Object

Log On to Windows

Microsoft Windows Server 2003 Standard Edition

Copyright © 1985-2003 Microsoft Corporation

Microsoft

User name: test1

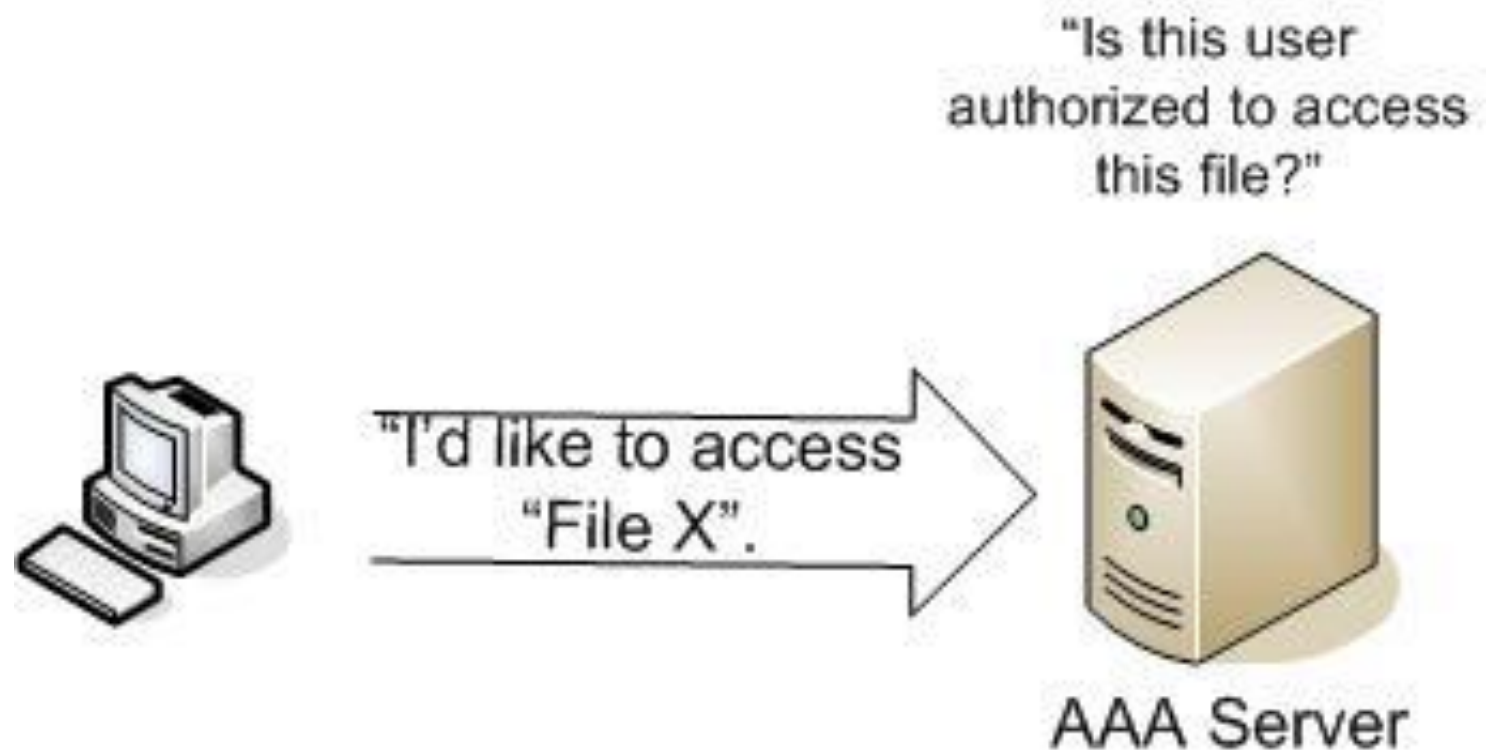
Password: |

Log on to: ZKASH-DEV (this computer)

OK Cancel Shut Down... Options <<

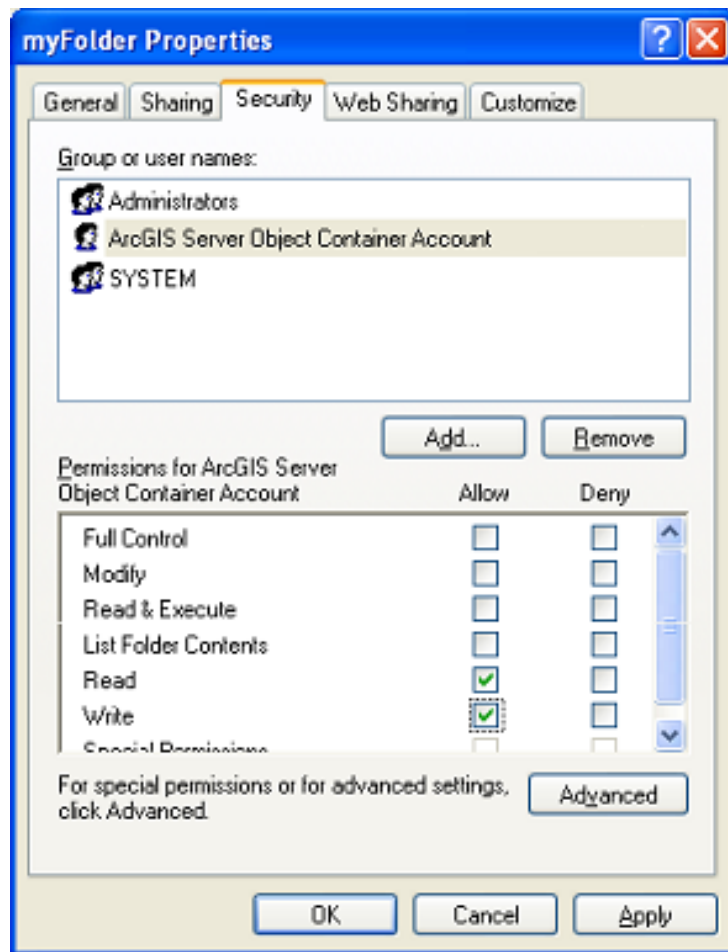
Authorization

- What is Authorization?
- Permission to access a resource after authentication:



Access Control

- Measures taken to restrict access to a resource:



```
[jsmith@localhost home]$ ls -l
total 8
drwx-----. 3 bderek bderek 4096 Jun 14 17:04 bderek
drwx-----. 17 jsmith jsmith 4096 Jun 14 17:03 jsmith
[jsmith@localhost home]$ cd bderek
bash: cd: bderek: Permission denied
```

```
[jsmith@localhost etc]$ cat hosts.deny
#
# hosts.deny      This file contains access rules which are used to
#                deny connections to network services that either use
#                the tcp_wrappers library or that have been
#                started through a tcp_wrappers-enabled xinetd.
#
#                The rules in this file can also be set up in
#                /etc/hosts.allow with a 'deny' option instead.
#
#                See 'man 5 hosts_options' and 'man 5 hosts_access'
#                for information on rule syntax.
#                See 'man tcpd' for information on tcp_wrappers
#
ALL: 188.42.4.5
ALL: maliciouswebsite.net
```

Accountability

- Requirement for actions of an entity to be traced uniquely to that entity.

```
[jsmith@localhost ~]$ cat .bash_history
uname -r
sudo yum install kernel-devel-3.9.5-301.fc19.x86_64
sudo yum install dkms kernel-devel-3.9.5-301.fc19.x86_64
cd /mnt
ls
cd ..
cd /run
ls
cd media/
ls
```

```
[root@localhost httpd]# cat access_log-20140427
127.0.0.1 - - [26/Apr/2014:17:35:50 -0500] "GET / HTTP/1.1" 403 4609 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:26.0) Gecko/20100101 Firefox/26.0"
127.0.0.1 - - [26/Apr/2014:17:35:50 -0500] "GET /icons/apache_pb2.gif HTTP/1.1" 200 4234 "http://127.0.0.1/" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:26.0) Gecko/20100101 Firefox/26.0"
127.0.0.1 - - [26/Apr/2014:17:35:50 -0500] "GET /icons/poweredby.png HTTP/1.1" 200 3034 "http://127.0.0.1/" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:26.0) Gecko/20100101 Firefox/26.0"
127.0.0.1 - - [26/Apr/2014:17:35:50 -0500] "GET /favicon.ico HTTP/1.1" 404 209 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:26.0) Gecko/20100101 Firefox/26.0"
127.0.0.1 - - [26/Apr/2014:17:39:22 -0500] "GET / HTTP/1.1" 200 166 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:26.0) Gecko/20100101 Firefox/26.0"
70.194.100.244 - - [26/Apr/2014:18:56:51 -0500] "GET / HTTP/1.1" 200 166 "-" "Mozilla/5.0 (Linux; Android 4.1.2; DROID RAZR HD Build/9.8.1Q-94) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/34.0.1847.114 Mobile Safari/537.36"
```

Non-Repudiation

- Repudiation = Denying an event occurred
- Non-Repudiation = Can't deny an event occurred



```
*** PGP Signature Status: good
*** Signer: Alison Aiton <aa4@st-andrews.ac.uk>
*** Signed: 01/05/01 15:01:25
*** Verified: 01/05/01 15:01:37
*** BEGIN PGP VERIFIED MESSAGE ***
```

This is simply the text of the message. It has not been encrypted, simply signed. You can use this sort of procedure [called clearsigning] for Word files, but not for other file types such as Excel.

```
*** END PGP VERIFIED MESSAGE ***
```

Part 2

Core Security Principals

Core Security Principles - The CIA Triad

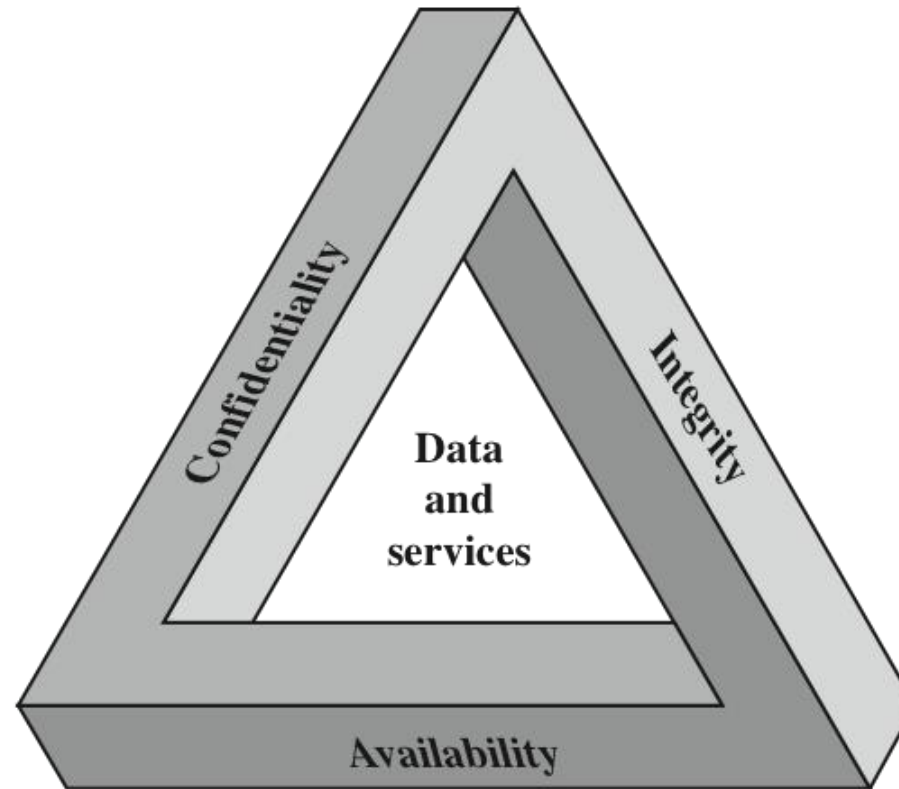


Figure 1.1 The Security Requirements Triad

1. Confidentiality (CIA Triad)

- Prevents unauthorized disclosure of information through:
 - Authentication/Access Controls/Authorization
 - Cryptography / Encryption
- Protects:
 - Privacy of personal information
 - Proprietary company information
 - Health information (HIPAA)



Cryptography

- “Art or science concerning the principles, means, and methods for rendering plain information unintelligible and for restoring encrypted information to intelligible form.”

Encryption

- “Conversion of plaintext to ciphertext through the use of a cryptographic algorithm.”
- Cryptographic algorithm = Cipher
- Well known Ciphers: AES, DES, 3DES, RC4
- Two main techniques:
 - Symmetric (Private) key encryption
 - Asymmetric key (Public) encryption

Attacks Against Confidentiality

Anthem data breach could be 'lifelong battle' for customers



Shari Rudavsky, shari.rudavsky@indystar.com

4:54 p.m. EST February 7, 2015

Impact of OPM breach could last more than 40 years

Intelligence and security experts say recovering from the massive data breach at the Office of Personnel Management won't happen until most retire.



By Dan Verton

JULY 12, 2015 4:43 PM

Business | Health | Local News

Premiera negligent in data breach, 5 lawsuits claim

Originally published March 27, 2015 at 8:18 pm

The computer-security breach that hit the Mountlake Terrace-based health insurer continues to reverberate as the insurer attempts to answer questions over what happened and how it's responding.

SECTION SPONSOR



By Coral Garnick

Seattle Times business reporter



Analyst sees Target data breach costs topping \$1 billion

By Tom Webb

twebb@pioneerpress.com

Click to know what happens next with this story



Attacks Against Confidentiality (Cont.)

Advocate Health slapped with lawsuit after massive data breach



Advocate "flagrantly disregarded" privacy of 4 million patients, lawsuit says

DOWNERS GROVE, IL | September 6, 2013

[Tweet](#) 50 [+1](#) 6 [Recommend](#) 41 [Share](#) 55

Advocate Health Care – who in August reported the second largest HIPAA data breach to date after four unencrypted laptops were stolen from its facility, compromising the protected health information and Social Security numbers of more than 4 million people – has now been slapped with a class action lawsuit filed by affected patients.

6.5 Million LinkedIn Passwords Reportedly Leaked, LinkedIn Is “Looking Into” It

Posted Jun 6, 2012 by [Chris Velazco \(@chrisvelazco\)](#)

How Heartbleed was linked to the CHS data breach

By [Joseph Conn](#) | August 22, 2014

Snowden used USB flash drive to breach NSA's security

June 18, 2013 | By [Paul Mah](#)

Breach Notification

- How do companies find out they have been breached?
 - Not aware until news story leaked
 - Internal security team or external third party contractor discovers breach from review of internal host/network/server data
 - Internal/external teams notice breach data has been posted on the web

Where is Breach Info Posted?

- A security team member can potentially discover leaked data about their company from:
 - Surface Web
 - Internet pages indexed by search engines
 - Deep Web
 - Internet pages NOT indexed by search engines
 - Ex: Medical and Financial Records, Subscription Info
 - Dark Web
 - .onion network only accessible via Tor

Disclaimer

****Don't download any data breach information from IIT systems or from the IIT network****

****I also wouldn't recommend downloading data breach information from home or work unless you are looking for your specific company or organization's information.****

Surface Web Breach Info

- leakforums.net / Leaks / Other Dumps



Sponsor 1337 Crew Hacked Database (Pages: 1 2 3 4 5) ⌚ 11M
Cocaine



Tons of leaked DBs! Free! (Pages: 1 2 3 4 ... 59) ⌚ 1Y
XBOX-BING



Leak -3- 50k EmailPass RUSSIAN [Origin, Minecraft, WarZ, Skype, PSN, Uplay, Steam, PayPal (Pages: 1 2 3 4 ... 6) ⌚ 4M
Foksi











Elite iCloud Accounts { German + US } (Pages: 1 2 3 4 ... 6) ⌚ 6M
Joker



Amazon [43] Account's (Pages: 1 2 3 4) ⌚ 2d
v4hl

Surface Web Breach Info (Cont.)


- www.sinister.ly/ Hacking / Website & Server Hacking / Compromised

		tiltedmill.com forum 18k usernames, passwords & salts by lola
		Ideas? *Compromised* (Pages: 1 2 3) by eclipse():
		READ by demon
		Diversebox.net's DB (Pages: 1 2 3) by Charon


Surface Web Breach Info (Cont.)

- pastebin.com

PASTEBIN | #1 paste tool since 2002


 **PASTEBIN** [Follow @pastebin](#) [Like](#) 203k

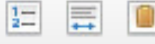
[create new paste](#) [trending pastes](#)

 **LIZARDSTRESSER DATABASE DUMP**

BY: A GUEST ON FEB 2ND, 2015 | SYNTAX: NONE | SIZE: 67.94 KB | VIEWS: 1,808 | EXPIRES: NEVER

[DOWNLOAD](#) | [RAW](#) | [EMBED](#) | [REPORT ABUSE](#) | [PRINT](#) | [QR CODE](#) | [CLONE](#)





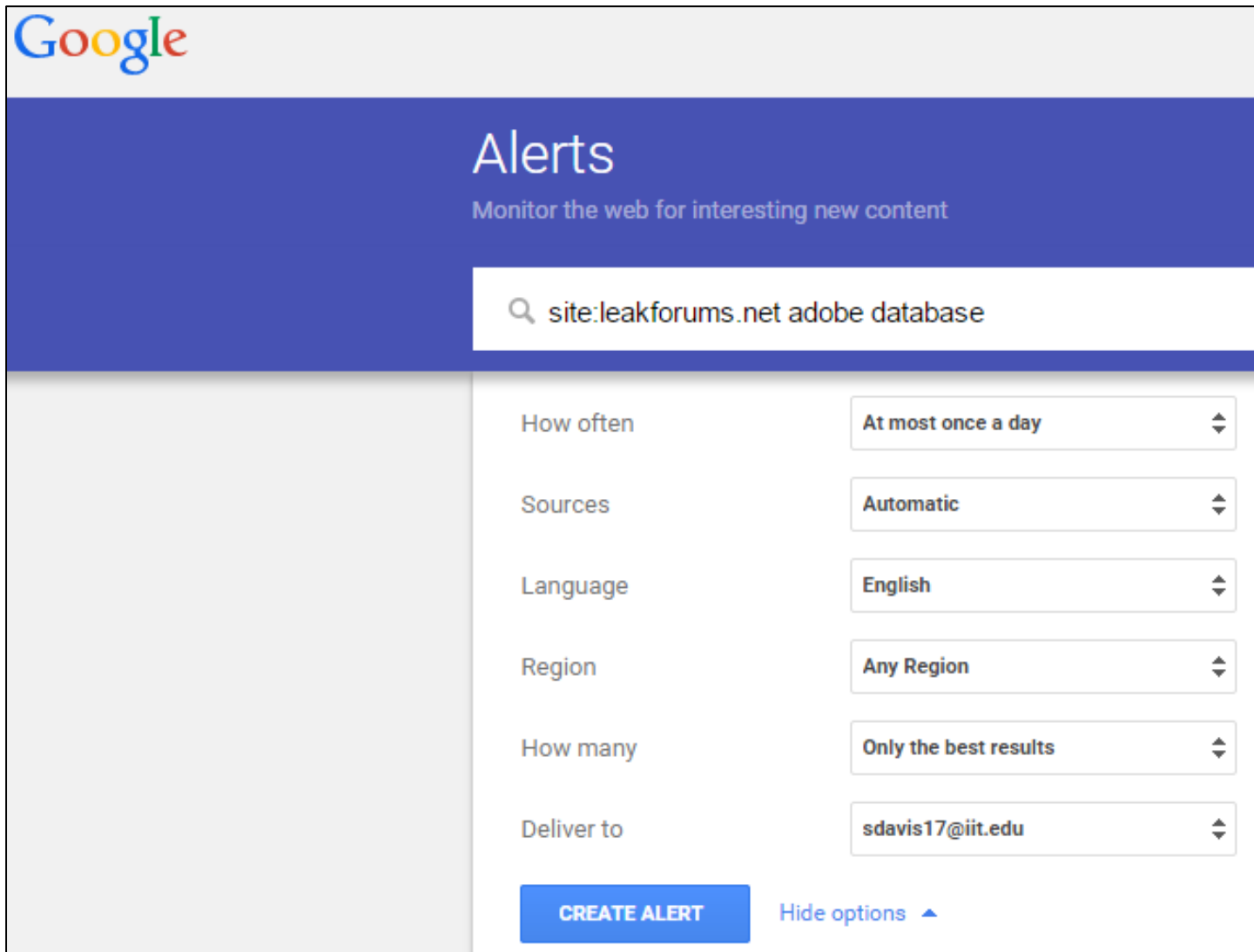
```
1. 132928, 'XxFlashBackxX', 'Kev2911', '[REDACTED]@hotmail.com', 0, 0, 0, 0, 0, ''
2. 132929, 'Tteol', 'John12345', '[REDACTED]@live.com', 0, 0, 0, 0, 0, ''
3. 132930, 'Fallenwun', 'slick123', '[REDACTED]@yahoo.com', 0, 0, 0, 0, 0, ''
4. 132931, 'vanchrist666', 'peluche03', '[REDACTED]@gmail.com', 0, 0, 0, 0, 0, ''
5. 132932, 'Dorky', 'ilovenate123', '[REDACTED]@live.com', 0, 0, 0, 0, 0, ''
```

What is a Better Way to Find Surface Web Breach Info???

- Google site search operator:

site:leakforums.net adobe database	site:sinister.ly adobe database
<p>Web Images Videos News Shopping More ▾ Search tools</p> <p>About 447 results (0.40 seconds)</p> <p>Adobe Database Leak - users.tar.gz - LeakForums leakforums.net/thread-574047 ▾ Jul 12, 2015 - In October 2013, 153 million Adobe accounts were breached with each containing an internal ID, username, email, encrypted password...</p> <p>Adobe database - 15k users. - LeakForums leakforums.net/thread-40829 ▾ Hello, Today I will release Adobe's database. Before downloading you press the thanks button!...</p>	<p>Web Images Videos News Shopping More ▾ Search tools</p> <p>About 15 results (0.60 seconds)</p> <p>40+ Compromised databases - Sinisterly https://www.sinister.ly/Thread-40-Compromised-databases ▾ Dec 20, 2013 - RuneHQ DB Decrypted.txt RunePlanet DB.txt ... Team Influence etc. on another server.</p>
	<p>site:pastebin.com adobe database</p> <p>Web Images Videos News Shopping More ▾ Search tools</p> <p>About 6,900 results (0.55 seconds)</p> <p>Top 100 password hints from Adobe database leak ... pastebin.com/8wg2LZvw ▾ Top 100 password hints from Adobe database leak. By: ScottHelme on Nov 12th, 2013 syntax: None size: 3.38 KB views: 553 expires: Never. download ...</p>

Even Better Way to Find Surface Web Breach Info???



The screenshot shows the Google Alerts interface. At the top left is the Google logo. Below it, the word "Alerts" is displayed in a large font, followed by the subtitle "Monitor the web for interesting new content". A search bar contains the text "site:leakforums.net adobe database". Below the search bar, there are several settings: "How often" is set to "At most once a day", "Sources" is set to "Automatic", "Language" is set to "English", "Region" is set to "Any Region", "How many" is set to "Only the best results", and "Deliver to" is set to "sdavis17@iit.edu". At the bottom left is a blue button labeled "CREATE ALERT", and to its right is a link labeled "Hide options" with a small upward-pointing triangle.

How often	At most once a day
Sources	Automatic
Language	English
Region	Any Region
How many	Only the best results
Deliver to	sdavis17@iit.edu

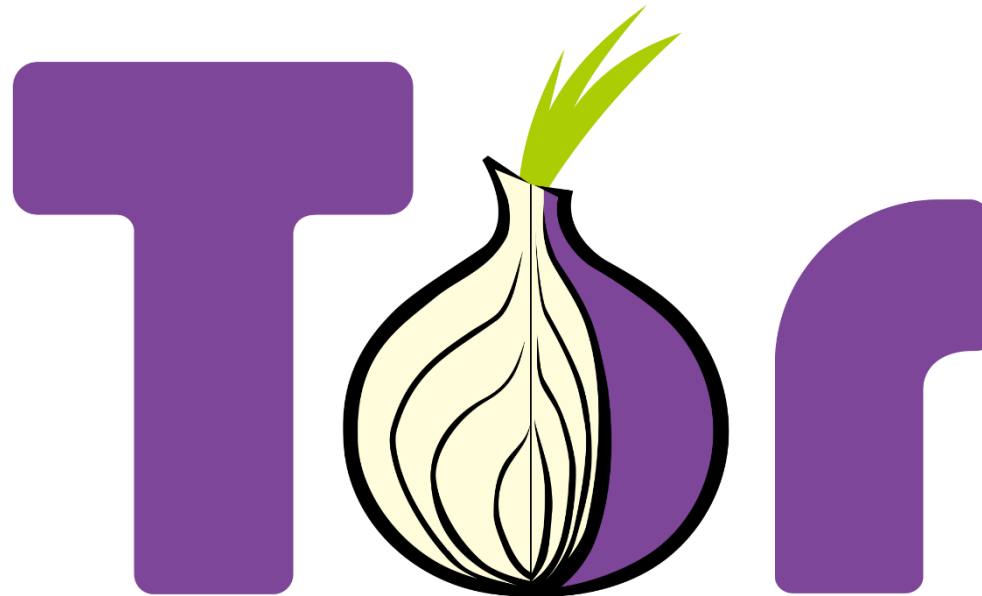
[CREATE ALERT](#) [Hide options](#)

Deep Web Breach Info

- You may find links to breach info on other subscription based sites or sites not indexed by search engines.

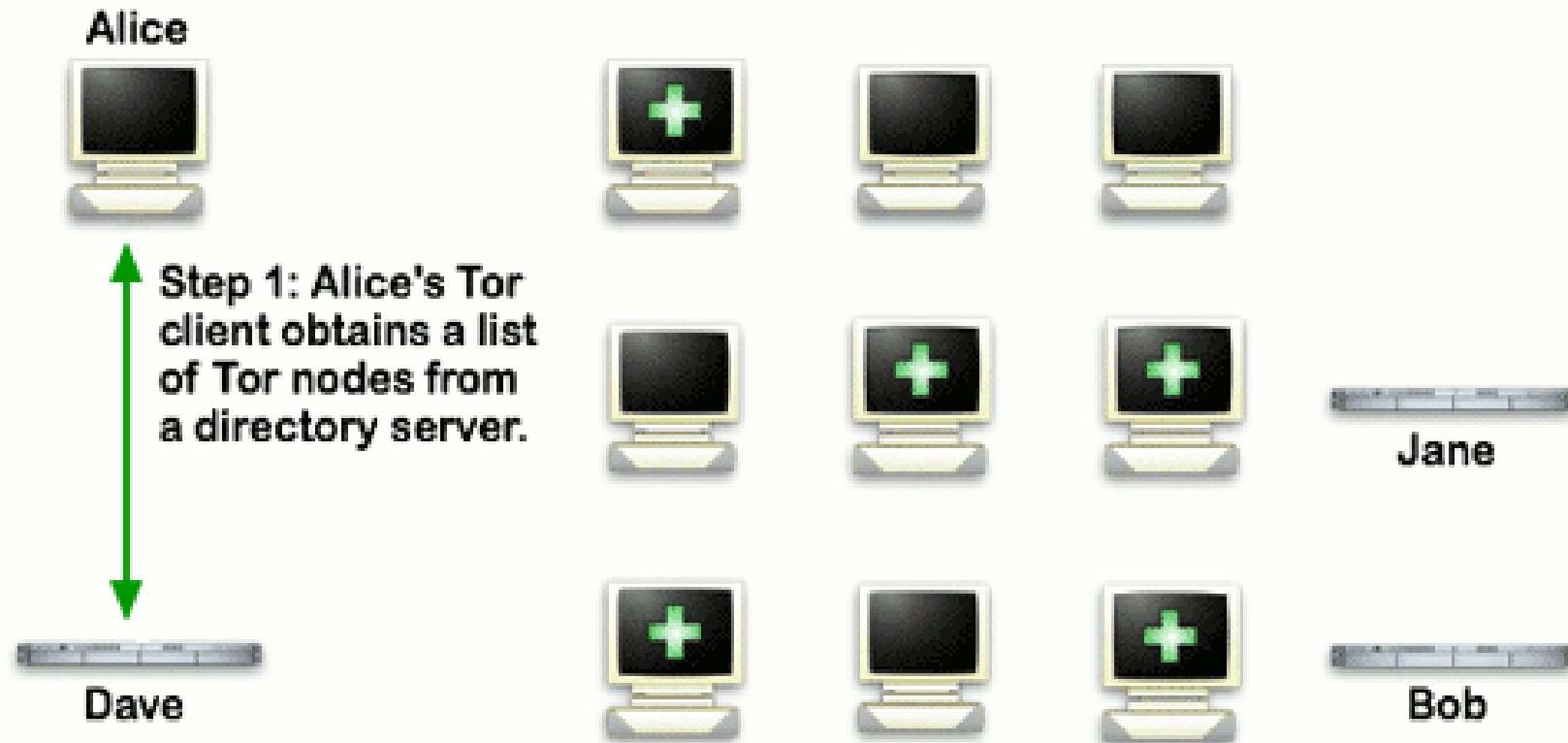
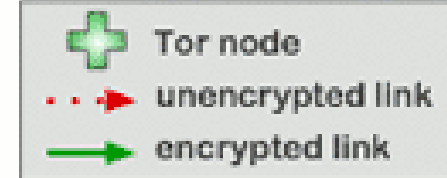
Dark Web Breach Info - TOR

- Created by U.S. Naval Research Laboratory employees

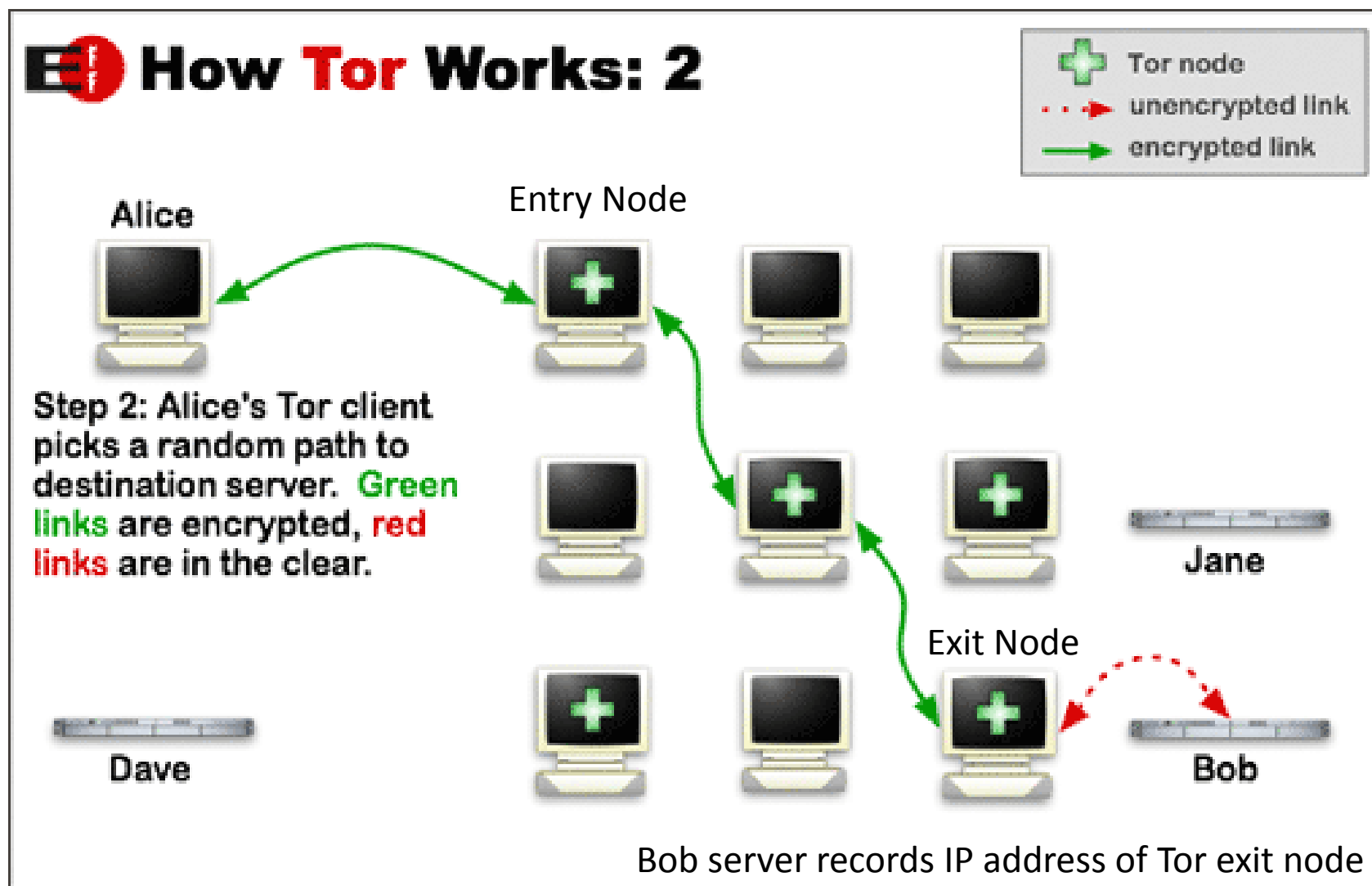


How Tor Works

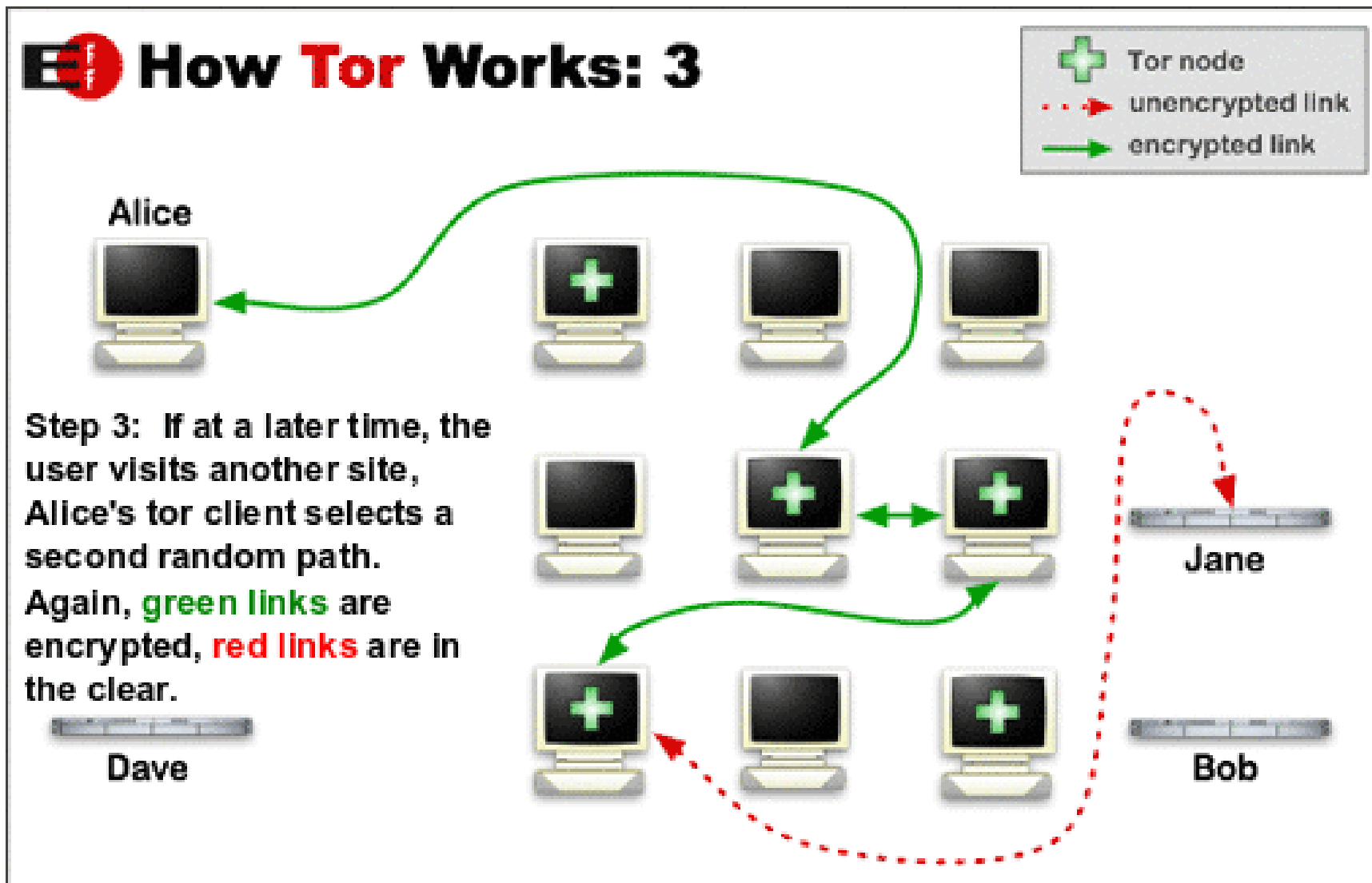
How Tor Works: 1



How Tor Works (Cont.)



How Tor Works (Cont.)



Lab - Tor

- We are going to use Tor to look at some Dark Web sites
- Connect to RADISH Win8.1 VM with VMware client on Desktop
- Open your Kali VM from the VNC shortcut on the Win8.1 VM Desktop

Lab - Tor

- Let's install the tor package.
- Open a terminal in Kali
apt-get -y install tor

Lab - Tor

- Tor requires accurate time/date for use
- Click on your clock at the top and select “Date & Time Settings”
- Turn “Automatic Date & Time” and “Automatic Time Zone” to the ON position
- Change the “Time Format” to AM/PM
- Close the Date & Time window

Lab - Tor

- Once your clock shows the correct time...
- Start tor with: **tor &**
- Once you see “Bootstrapped 100%: Done, Tor is ready
- Hit Enter
- Let's check our normal current ip address not using tor

curl http://ipecho.net/plain

Lab - Tor

- How can we run curl through tor???
 - torsocks allows you to run normal shell programs through tor to make them anonymous
- **torsocks curl http://ipecho.net/plain**
- Notice the difference between your normal public IP and tor public IP

Lab – Tor: How to Browse the Dark Web

- Option 1: Set Firefox Proxy to localhost and port 9050 under SOCKS Host with option SOCKS v5

Connection Settings

Configure Proxies to Access the Internet

☐ No proxy

☐ Auto-detect proxy settings for this network

☐ Use system proxy settings

☒ Manual proxy configuration:

HTTP Proxy: Port:

☐ Use this proxy server for all protocols

SSL Proxy: Port:

FTP Proxy: Port:

SOCKS Host: Port:

☐ SOCKS v4 ☒ SOCKS v5

No Proxy for:

Example: .mozilla.org, .net.nz, 192.168.1.0/24

☐ Automatic proxy configuration URL:

Lab – Tor: How to Browse the Dark Web

- Option 2: torsocks with Firefox
torsocks firefox
- We'll go with this option for the lab.

Lab - Tor

- Let's check to make sure Firefox is really using tor.
- Browse to: `check.torproject.org`



Congratulations. This browser is configured to use Tor.

Your IP address appears to be: **46.29.248.238**

However, it does not appear to be Tor Browser.

[Click here to go to the download page](#)

Lab - Tor

- Tor allows you to visit hidden services in addition to Surface Web sites
- What is a hidden service?
 - A web site with a non-routable domain ending in .onion

Lab - Tor

- Types of hidden service sites:
 - Hacking
 - Database Dumps
 - Credit Card Dumps
 - Drugs
 - Pornography
 - Security Research
 - Etc.

Lab – Tor

- Example of a hidden site:
- Use tor enabled Firefox to browse to the 0Day Forum:

qzbkwsfv5k2oj5d.onion

- What are some of the topics you see???

Lab – Tor Warning

- Tor can be a great resource for security professionals to learn more about their adversaries
- **It is illegal to browse hidden services which show illicit underage images or videos
- **It is not illegal to browse most other hidden services but it is illegal to purchase illegal items and content

Lab – Tor

- Close tor enabled browser
- Now, we need to kill the tor process running in the background.
- **ps -ef**

```
root      14351      2   0  11:42 ?        00:00:00 [kworker/0:1]
root      14408      2   0  11:47 ?        00:00:00 [kworker/0:2]
root      14410     6962   0  11:48 pts/0    00:00:00 tor
root      14419     6962   0  11:51 pts/0    00:00:00 ps -ef
```

- **kill 14410** or whatever your PID listed is for tor

Lab - Tor

- There is also a Tor Browser Bundle (TBB) for various operating systems which provides a pre-configured Firefox browser which uses Tor.
- In comparison, the tor package in linux installs tor, tor-geoipdb, and torsocks and is more useful for scripting and running command through tor

Confidentiality

- That concludes the first core security principal of the CIA triad.
- We will learn more about how to protect confidentiality as the course progresses.

2. Integrity (CIA Triad)

- Guards against modification or destruction of data that is being stored or in transit.
- Techniques for verifying data integrity:
 - Message Digests (MD5, SHA-1, SHA-2)
 - Message Authentication/Integrity Codes (MAC/MIC)
 - Checksums (Cyclic Redundancy Check (CRC), Frame Check Sequence (FCS))
 - Comparisons (diff in Linux, FC in Windows)

Integrity Example:

Package Information

- Download (HTTP): <http://nmap.org/dist/nmap-6.46.tar.bz2>
- Download MD5 sum: 5a36ad3a63d5b7ea5514f745a397436a

```
[jsmith@localhost Downloads]$ md5sum nmap-6.46.tar.bz2  
5a36ad3a63d5b7ea5514f745a397436a  nmap-6.46.tar.bz2
```



Attacks Against Integrity

By CBSNEWS / CBS/AP / November 29, 2010, 3:19 PM

Iran Confirms Stuxnet Worm Halted Centrifuges

The Inside Story of Mt. Gox, Bitcoin's \$460 Million Disaster

BY ROBERT MCMILLAN 03.03.14 | 6:30 AM | PERMALINK

Swedish schoolkids hack computers to change grades, fend off alerts to parents

Thirty-one students are believed to have had their midterm grades altered in some way after the trio of alleged perps gained access to the school's intranet, reports Swedish media. The kids are accused of upping grades for pay — or lowering them for people they disliked.

BY LEE MORAN / NEW YORK DAILY NEWS / Friday, April 11, 2014, 11:29 AM

A A A

Integrity Lab

- In Kali, open a terminal.
- How do we figure out the path to the tor binary we downloaded through apt-get?

which tor

- How do we check the current hash?

md5sum /usr/sbin/tor

```
df6d0347a7f08404d39737f955bc84f1 /usr/sbin/tor
```

Integrity Lab

- What is a hash?
 - One way mathematical function to map a fixed value to arbitrary data.
 - If one bit of a file changes, the files hash changes completely

Integrity Lab

- Copy tor to the /root directory.

```
cp /usr/sbin/tor .
```

```
md5sum ./tor
```

```
df6d0347a7f08404d39737f955bc84f1  ./tor
```

- Make another copy of tor and check that both hashes match.

```
cp tor tor2
```

```
df6d0347a7f08404d39737f955bc84f1  ./tor  
df6d0347a7f08404d39737f955bc84f1  ./tor2
```

```
md5sum ./tor ./tor2
```

Integrity Lab

- How could we modify a single bit of the tor2 file?
- (Below command is all one line)

**`printf "\x01" | dd of=tor2 bs=1 seek=0x100
count=1 conv=notrunc`**

- Compare the hashes of the two files again

`md5sum ./tor ./tor2`

```
df6d0347a7f08404d39737f955bc84f1  ./tor  
39b73cd55ccba9bdad40b8ab26e6174  ./tor2
```

Integrity Lab

- Find where the files differ:

cmp -b tor tor2

```
tor tor2 differ: byte 1, line 1 is 177 ^? 1 ^A
```

Integrity Lab

- Since tor was downloaded through a package manager, where can we find the original hash???

cat /var/lib/dpkg/info/tor.md5sums

```
df6d0347a7f08404d39737f955bc84f1  usr/bin/tor
5d624f7c20b8dc66694c1dc44c528a51  usr/bin/tor-gencert
7c622c03f561411c20c148ce2a61ef94  usr/bin/tor-resolve
d7e3e170a75611f864b243fc37640a59  usr/bin/torify
```


Integrity Lab

- Debsums can check current binaries against the stored values in dpkg/info

apt-get -y install debsums
debsums tor

```
/usr/bin/tor OK  
/usr/bin/tor-gencert OK  
/usr/bin/tor-resolve OK  
/usr/bin/torify OK
```

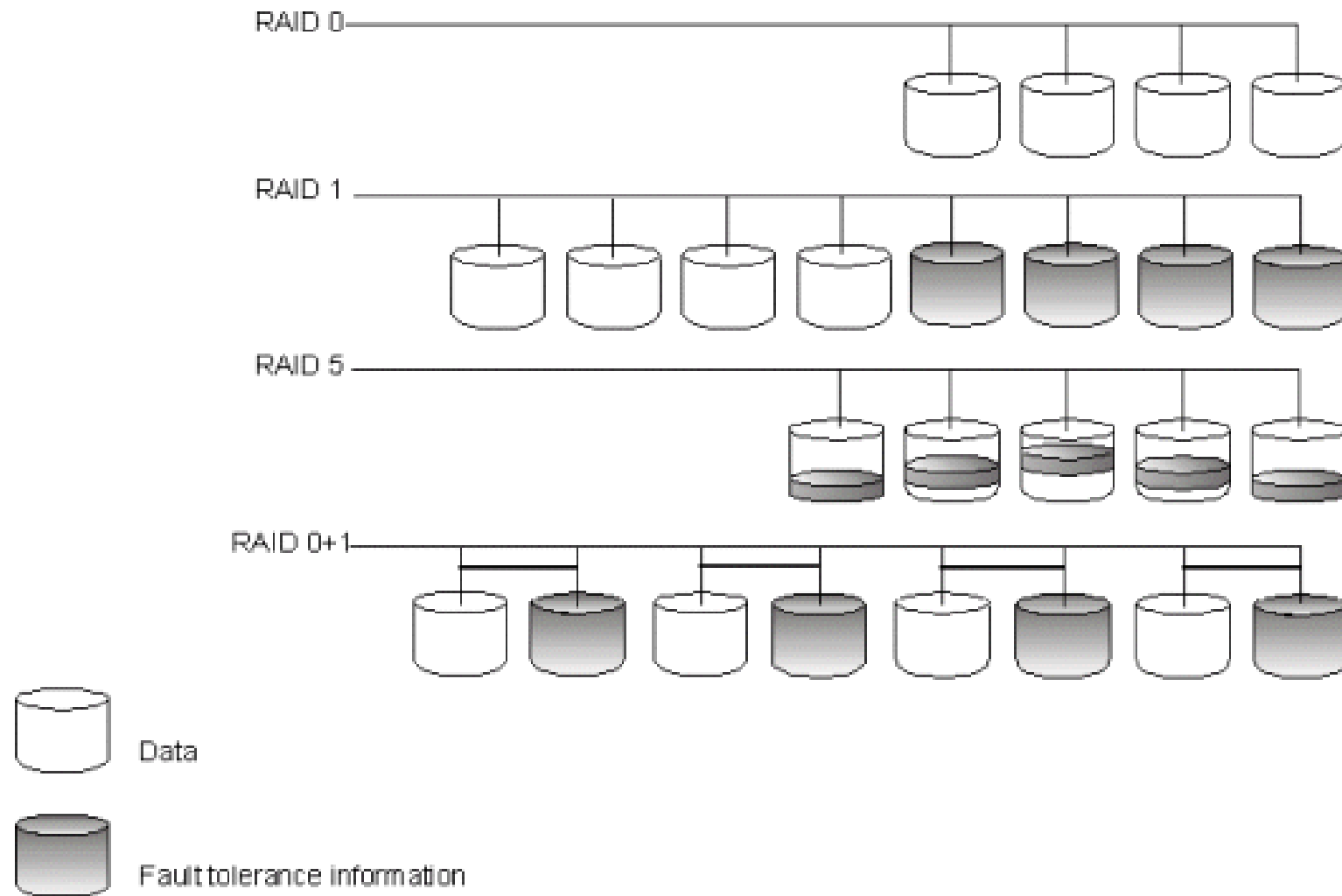
Integrity Lab

- What problem remains with this method of integrity checking?
 - An attacker that has access to modify a binary may have access to just edit the md5 hash value in dpkg/info...
- What is a potential solution to that problem?
 - Use a host based IDS such as Tripwire

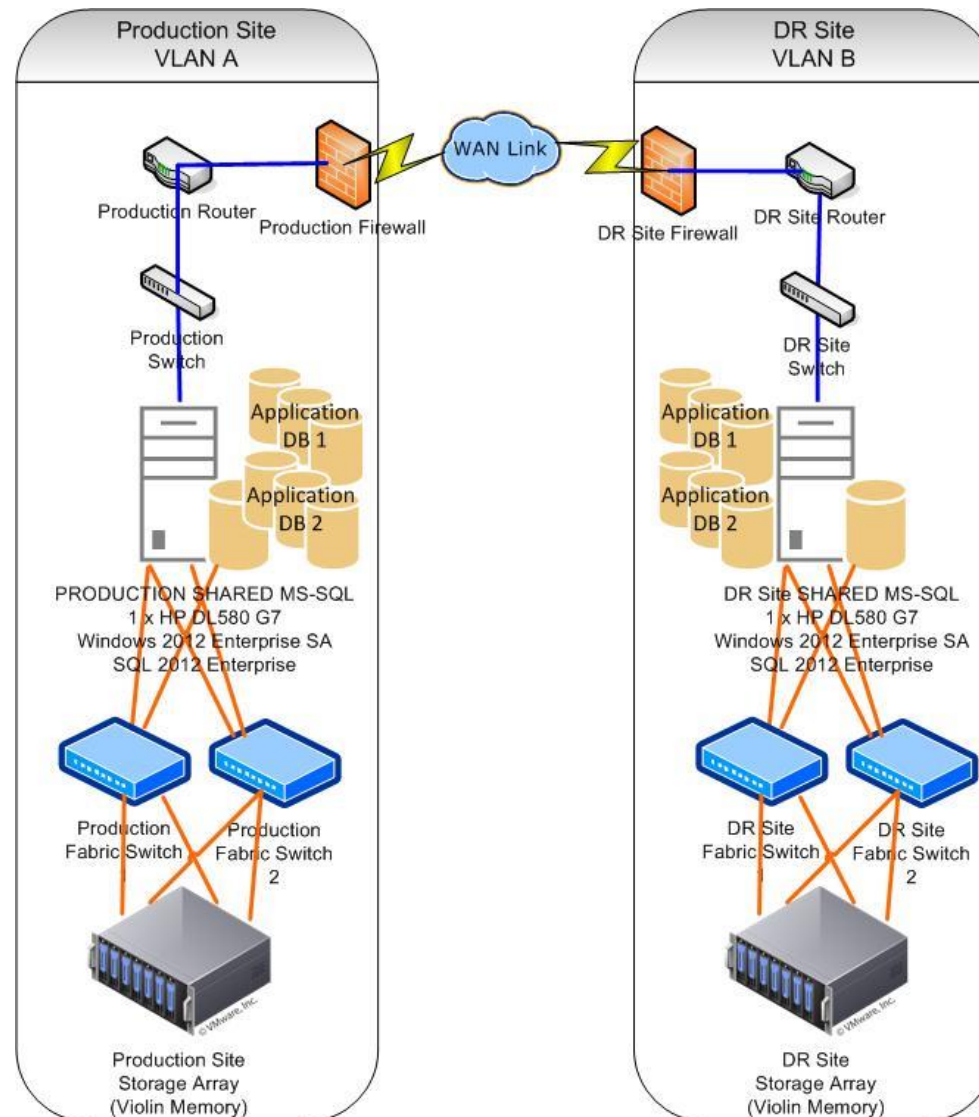
3. Availability (CIA Triad)

- Ensuring data and services can be accessed and used in a timely and reliable manner
- Techniques for ensuring Availability:
 - Redundancy
 - Disk, Server, Network, Storage, Site
 - Backups
 - UPS
 - Environmental Controls

Disk Redundancy Example:



Server/Network/Storage/Site Redundancy Example:



<http://social.technet.microsoft.com/forums/windowsserver/en-US/623ccb66-af91-4218-b373-4660bfd9df9b/single-node-different-vlan-clustering-networking-setup>

Downtime/Attacks Against Availability

Amazon Down 15 Minutes, Loses Over \$66,000 Per Minute

Aug 19, 2013 by Shawn Hessioner In Technology Trends 21

amazon.com

Oops!

We're very sorry, but we're having trouble doing what you just asked us to do. Please give us another chance--click the Back button on your browser and try your request again. Or start from the beginning on our [homepage](#).

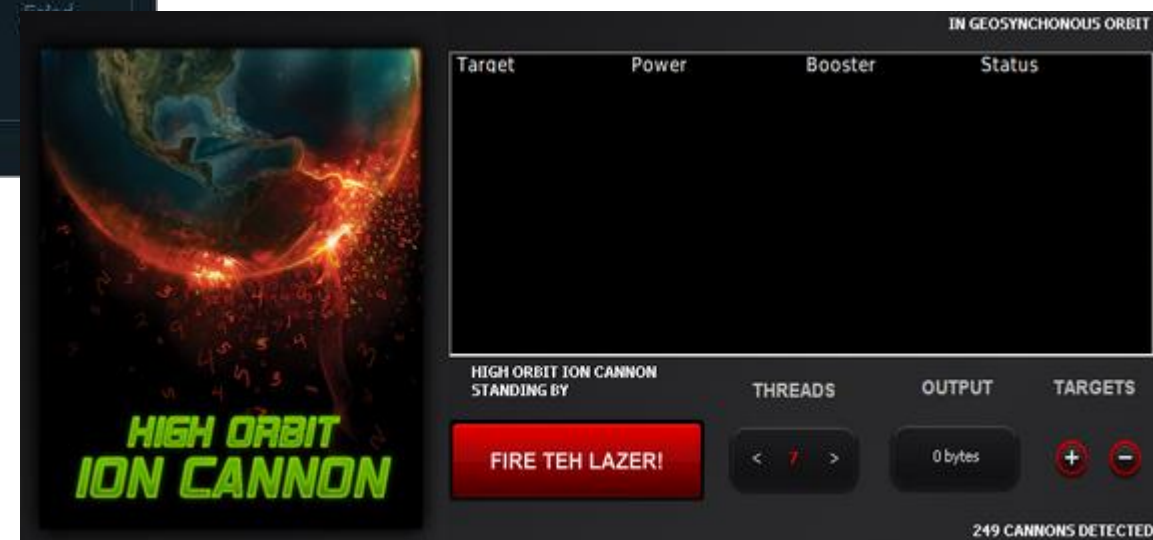
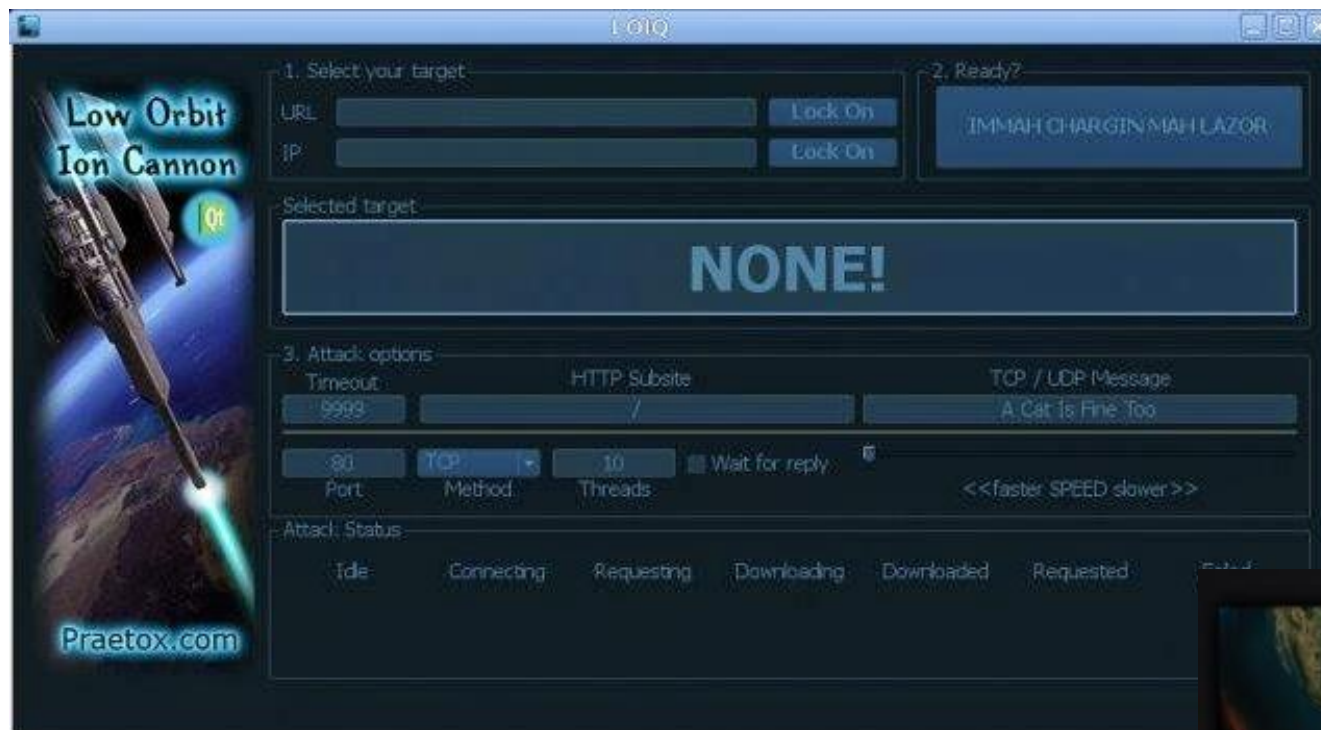


Anonymous Hackers Arrested For Visa, PayPal, Mastercard Attacks

By Talia Ralph | January 25, 2013

Their denial of service (DDoS) assaults on PayPal reportedly cost the company around \$4.6 million dollars, [according to the Guardian](#).

Anonymous DDoS Tools Against Availability



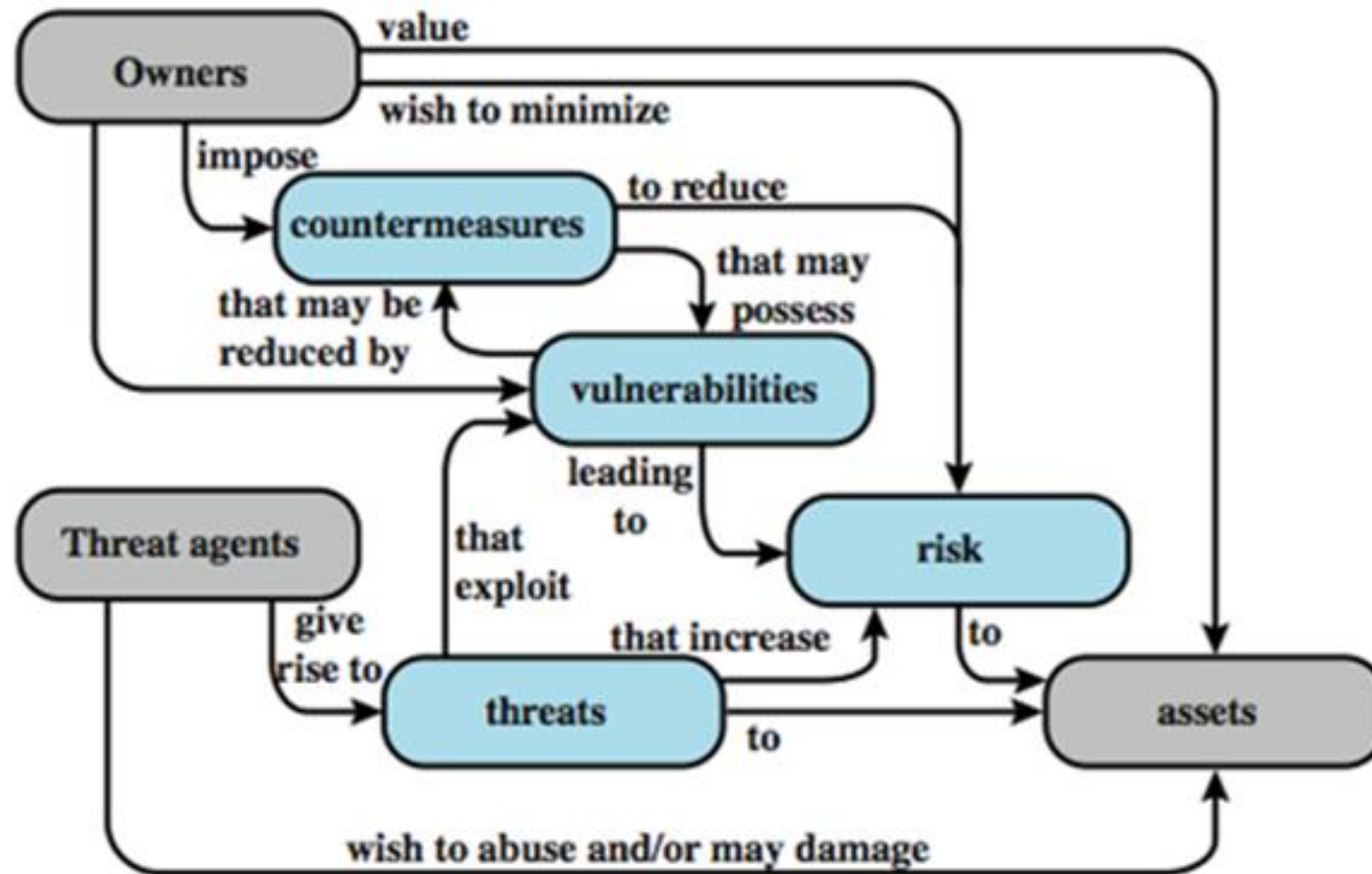
Availability

- We will learn more about DoS and DDoS methods in a later lecture.

Security Challenges

- Maintaining Availability while keeping the organization safe.
- Getting buy-in from upper management
- Users viewing security as an impediment to efficiency
- Staying one step ahead of attackers
- Security infrastructure selection and placement
- Security requires regular and constant monitoring

Security Concepts and Relationships



Part 3

Inside Threats

Inside Threats

- Initiated inside security perimeter:
 - Weak Passwords
 - Logic Bomb
 - Website Defacement
 - User Deletes Data (Accidental or Purposely)
 - Intellectual Property Theft
 - Exceeding Authorization
 - Open File Shares
 - Rogue AP
 - Insecure Coding
 - Uses system as launch pad to attack other organizations
 - Social Engineering & Phishing Victims

Importance of User Education/Awareness Training

- Strong Passwords
- Social Engineering Tactics
- Phishing Tactics

McAfee Phishing Quiz

- <https://phishingquiz.mcafee.com>

Top Themes for Phishing Campaigns



1.
Bank Deposit/Payment Notifications

Notifications for deposits, transfers, payments, returned check, fraud alert.



2.
Online Product Purchase

Product order confirmation, request purchase order, quote, trial.



3.
Attached Photo

Malicious attached photos.



4.
Shipping Notices

Invoices, delivery or pickup, tracking.



5.
Online Dating

Online dating sites.



6.
Taxes

Tax documents, refunds, reports, debt information, online tax filings.

Top Themes for Phishing Campaigns (Cont.)



7.
Facebook

Account status, updates, notifications,
security software.



8.
Gift Card or Voucher

Alerts from a variety of stores
(Apple was the most popular).



9.
PayPal

Account update, confirmation,
payment notification, payment dispute.

Legitimate Email Example

Chase <no-reply@alertsp.chase.com>

to me ▾

Note: This is a service message with information related to your Chase account(s). It may include specific details about transactions, products or online services. If you recently cancelled your account, please disregard this message.



Dear Chase OnlineSM Customer:

We're writing to let you know the statement for your deposit account ending in [REDACTED] is now available online.

To see your statement, log on to www.Chase.com

If you aren't enrolled in Paperless Statements and think you've received this message in error, please call our Customer Support team immediately, using the phone number on the "Contact Us" page on Chase Online.

Please don't reply directly to this automatically-generated e-mail message.

Sincerely,

Online Banking Team

JPMorgan Chase Bank, N.A. Member FDIC
©2014 JPMorgan Chase & Co.

Your personal information is protected by advanced online technology. For more detailed information, view our [Online Privacy Policy](#). To request in writing: Chase Privacy Operations, 451 Florida Street, Fourth Floor, LA2-9376, Baton Rouge, LA 70801

This email was sent to: sd24801@gmail.com

EMLSTMT

Legitimate Email Headers

```
Delivered-To: sd24801@gmail.com
Received: by 10.194.219.73 with SMTP id pm9csp23820wjc;
      Fri, 13 Jun 2014 05:58:57 -0700 (PDT)
X-Received: by 10.229.234.67 with SMTP id kb3mr3410810qcb.6.1402664336107;
      Fri, 13 Jun 2014 05:58:56 -0700 (PDT)
Return-Path: <no-reply@alertsp.chase.com>
Received: from shvf1.jpmpchase.com (shvf1.jpmpchase.com. [159.53.46.193])
      by mx.google.com with ESMTPS id u44sil700988qgd.84.2014.06.13.05.58.55
      for <sd24801@gmail.com>
      (version=TLSv1 cipher=RC4-SHA bits=128/128);
      Fri, 13 Jun 2014 05:58:56 -0700 (PDT)
Received-SPF: pass (google.com: domain of no-reply@alertsp.chase.com designates 159.53.46.193 as
permitted sender) client-ip=159.53.46.193;
Authentication-Results: mx.google.com;
      spf=pass (google.com: domain of no-reply@alertsp.chase.com designates 159.53.46.193 as
permitted sender) smtp.mail=no-reply@alertsp.chase.com;
      dkim=pass header.i=@alertsp.chase.com;
      dmarc=pass (p=REJECT dis=NONE) header.from=alertsp.chase.com
Received: from cigp02a4a010.svr.us.jpmpchase.net ([169.83.182.166])
      by shvf1.jpmpchase.com (Sentrion-MTA-4.3.1/Sentrion-MTA-4.3.1) with ESMTP id
s5DCwtln029959
      for <sd24801@gmail.com>; Fri, 13 Jun 2014 08:58:55 -0400
X-DKIM: OpenDKIM Filter v2.4.3 shvf1.jpmpchase.com s5DCwtln029959
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=alertsp.chase.com;
      s=d2048-1; t=1402664335;
      bh=U6MBXCEJCD4AoO9asDG+JVtqRONWqyDMEKq4HgDrdiU=;
      h=Date:From:To:Message-ID:Subject:MIME-Version:Content-Type:
      Content-Transfer-Encoding;
      b=OGvuO8SkTykKn8BJxQt6GQZnmqEw05Z5Fc2WDqiFiVDox6Ouz/pCZmrURGddF0FzN
      czMjNM04kxmQ2bhUuLywMcZpTIIWf/k5DaeuIcYq72y+UglyBkOVQ3DNUDYt0Ap002
      q+HVpJCkTSgSTkVvzKRbAVU153dQ1F7TGDn/gZuMJayt9IMsL7A6G1joiI6KVUCNPhF
      XYJdEevhXo4Z1rePe51d7JUBmZXP5xUujMeEI9qb/6MDWFm7UimGf5cP/D5L7VD7c8
      cCBxTxF8XbfQFqnOxGf6aWcxoatMXEb4kHuTrmeKa4KSCeZIXTF4cVwogLxPFQJy6K
      QnqBF7PK9GwLQ==
Received: from cigp02a4a010.svr.us.jpmpchase.net (loopback [127.0.0.1])
      by cigp02a4a010.svr.us.jpmpchase.net (AIX6.1/8.14.4/8.11.0) with ESMTP id s5DCwseH49021528
      for <sd24801@gmail.com>; Fri, 13 Jun 2014 08:58:55 -0400
Date: Fri, 13 Jun 2014 08:58:55 -0400 (EDT)
From: Chase <no-reply@alertsp.chase.com>
To: sd24801@gmail.com
Message-ID: <800151945.14236218.1402664335008.JavaMail.root@cigp02a4a010.svr.us.jpmpchase.net>
Subject: Your deposit statement is available online
MIME-Version: 1.0
Content-Type: text/html; charset=us-ascii
Content-Transfer-Encoding: 7bit
APP-SOURCE: PSN
NOTIFICATION-ID: 1555069780
```

Legitimate Email Headers – Bottom to Top

```
Received: from cigp02a4a010.svr.us.jpmchase.net (loopback [127.0.0.1])  
    by cigp02a4a010.svr.us.jpmchase.net (AIX6.1/8.14.4/8.11.0) with ESMTTP id s5DCwseH49021528  
    for <sd24801@gmail.com>; Fri, 13 Jun 2014 08:58:55 -0400  
Date: Fri, 13 Jun 2014 08:58:55 -0400 (EDT)  
From: Chase <no-reply>alertsp.chase.com>  
To: sd24801@gmail.com  
Message-ID: <800151945.14236218.1402664335008.JavaMail.root@cigp02a4a010.svr.us.jpmchase.net>  
Subject: Your deposit statement is available online  
MIME-Version: 1.0  
Content-Type: text/html; charset=us-ascii  
Content-Transfer-Encoding: 7bit  
APP-SOURCE: PSN  
NOTIFICATION-ID: 1555069780
```

Legitimate Email Headers – Bottom to Top

```
Delivered-To: sd24801@gmail.com
Received: by 10.194.219.73 with SMTP id pm9csp23820wjc;
      Fri, 13 Jun 2014 05:58:57 -0700 (PDT)
X-Received: by 10.229.234.67 with SMTP id kb3mr3410810qcb.6.1402664336107;
      Fri, 13 Jun 2014 05:58:56 -0700 (PDT)
Return-Path: <no-reply@alertsp.chase.com>
Received: from shvf1.jpmpchase.com (shvf1.jpmpchase.com. [159.53.46.193])
      by mx.google.com with ESMTPS id u44si1700988qgd.84.2014.06.13.05.58.55
      for <sd24801@gmail.com>
      (version=TLSv1 cipher=RC4-SHA bits=128/128);
      Fri, 13 Jun 2014 05:58:56 -0700 (PDT)
Received-SPF: pass (google.com: domain of no-reply@alertsp.chase.com designates 159.53.46.193 as
permitted sender) client-ip=159.53.46.193;
Authentication-Results: mx.google.com;
      spf=pass (google.com: domain of no-reply@alertsp.chase.com designates 159.53.46.193 as
permitted sender) smtp.mail=no-reply@alertsp.chase.com;
      dkim=pass header.i=@alertsp.chase.com;
      dmarc=pass (p=REJECT dis=NONE) header.from=alertsp.chase.com
Received: from cigp02a4a010.svr.us.jpmpchase.net ([169.83.182.166])
      by shvf1.jpmpchase.com (Sentrion-MTA-4.3.1/Sentrion-MTA-4.3.1) with ESMTP id
s5DCwtln029959
      for <sd24801@gmail.com>; Fri, 13 Jun 2014 08:58:55 -0400
```

Legitimate Email Headers – Verified Sender IP

```
NetRange:      159.53.0.0 - 159.53.255.255
CIDR:          159.53.0.0/16
OriginAS:
NetName:       JMC
NetHandle:     NET-159-53-0-0-1
Parent:        NET-159-0-0-0-0
NetType:       Direct Assignment
RegDate:       1992-03-06
Updated:       2012-02-24
Ref:           http://whois.arin.net/rest/net/NET-159-53-0-0-1

OrgName:       JPMorgan Chase & Co.
OrgId:         JMC-39
Address:        120 Broadway
City:           New York
StateProv:      NY
PostalCode:     10271-1999
Country:        US
RegDate:        2006-11-21
Updated:        2008-08-21
Ref:           http://whois.arin.net/rest/org/JMC-39
```

Legitimate Email Source – Correct Domain

```
<TBODY>
  <TR>
    <TD>
      <P align="right"><IMG height="27"
        src="https://www.chase.com/content/dam/chaseonline/en/alerts/ondemand/evento
      <P><font size="-1"
        face="Verdana, Arial, Helvetica, sans-serif"> Dear Chase
      Online<sup>SM</sup> Customer: </font></P>
      <p><font size="-1"
        face="Verdana, Arial, Helvetica, sans-serif"> We're
      writing to let you know the statement for your deposit account
      ending in [REDACTED] is now available online. <br />
      <br />
      To see your statement, log on to <a href="https://www.chase.com">www.Chase.com</a>
      <br />
      <br />
      If you aren't enrolled in Paperless Statements and think you've
      received this message in error, please call our Customer Support
      team immediately, using the phone number on the "Contact Us" page
      on Chase Online. <br />
      <br />
      Please don't reply directly to this automatically-generated e-mail
      message. <br />
      <br />
      Sincerely, <br />
      <br />
      Online Banking Team <br />
      <br />
      </font></p>
    </TD>
  </TR>
</TBODY>
```

How Could a Phisher Use This Email in an Attack?

- Copy the HTML from the legitimate email and spoof the headers!

How Could a Phisher Use This Email in an Attack? (Cont.)

```
root@PRK105:~# telnet localhost 25
Trying ::1...
Connected to localhost.
Escape character is '^]'.
220 PRK105 ESMTP Exim 4.80 Sat, 21 Jun 2014 16:07:51 -0500
mail from: accounts@chasebankus.com
250 OK
rcpt to: sdavis17@iit.edu
250 Accepted
data
354 Enter message, ending with "." on a line by itself
From: Chase Accounts <accounts@chasebankus.com>
To: Shawn Davis <sdavis17@iit.edu>
Subject: Your deposit statement is available online

MIME-Version: 1.0
Content-Type: text/html; charset=us-ascii
Content-Transfer-Encoding: 7bit
APP-SOURCE: PSN
NOTIFICATION-ID: 1555069780

<TABLE cellSpacing="0" cellPadding="0" width="610" border="0"><tr><td><font face
="Arial, Helvetica, sans-serif" size="1">Note:This is a service message with inf
ormation related to your Chase account(s). It may include specific details about
t transactions, products or online services. If you recently cancelled your acco
unt,please disregard this message. </font></td></tr></TABLE>

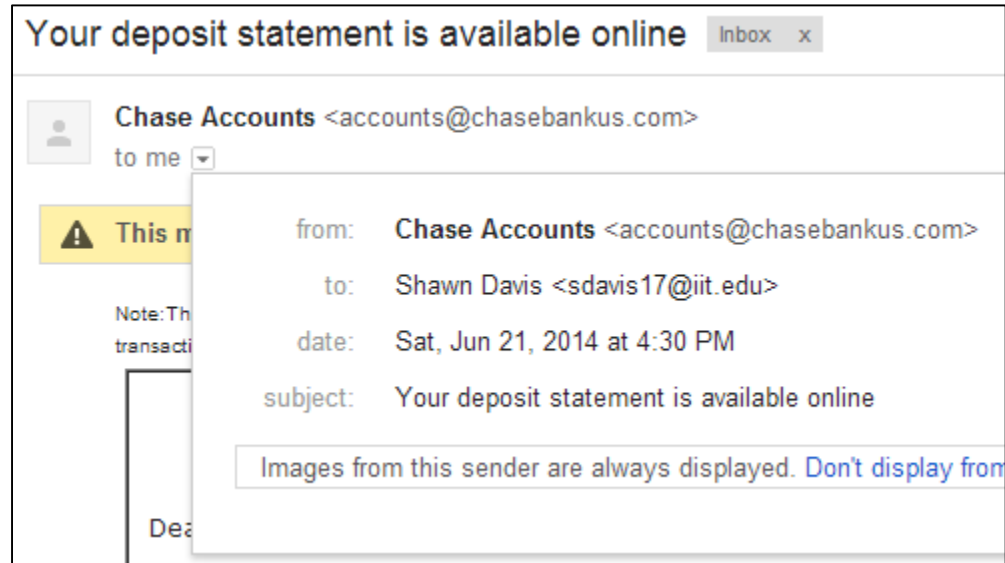
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">

<TABLE cellSpacing="0" cellPadding="5" width="590" border="0">
  <TBODY>
```


How Could a Phisher Use This Email in an Attack? (Cont.)

```
<P align="right"><IMG height="27"
      src="https://www.chase.com/content/dam/chaseonline/en/alerts/ondemand/event$
<P><font size="-1"
      face="Verdana, Arial, Helvetica, sans-serif"> Dear Chase
Online<sup>SM</sup> Customer: </font></P>
<p><font size="-1"
      face="Verdana, Arial, Helvetica, sans-serif"> We're
writing to let you know the statement for your deposit account
ending in  is now available online. <br />
<br />
To see your statement, log on to <a href="https://www.evilsite.com">www.Chase.com</a>
<br />
<br />
If you aren't enrolled in Paperless Statements and think you've
received this message in error, please call our Customer Support
team immediately, using the phone number on the "Contact Us" page
on Chase Online. <br />
<br />
```

How Could a Phisher Use This Email in an Attack? (Cont.)



Note: This is a service message with information related to your Chase account(s). It may include specific details about transactions, products or online services. If you recently cancelled your account, please disregard this message.



Dear Chase OnlineSM Customer:

We're writing to let you know the statement for your deposit account ending in [REDACTED] is now available online.

To see your statement, log on to www.Chase.com

If you aren't enrolled in Paperless Statements and think you've received this message in error, please call our Customer Support team immediately, using the phone number on the "Contact Us" page on Chase Online.

Please don't reply directly to this automatically-generated e-mail message.

Sincerely,

Online Banking Team

JPMorgan Chase Bank, N.A. Member FDIC
©2014 JPMorgan Chase & Co.

Your personal information is protected by advanced online technology. For more detailed information, view our [Online Privacy Policy](#). To request in writing: Chase Privacy Operations, 451 Florida Street, Fourth Floor, LA2-9376, Baton Rouge, LA 70801

This email was sent to: sdavis17@iit.com

EMLSTMT

Phishing Email Headers

```
Delivered-To: sdavis17@iit.edu
Received: by 10.140.101.67 with SMTP id t61csp463961qge;
        Sat, 21 Jun 2014 14:31:03 -0700 (PDT)
X-Received: by 10.50.66.241 with SMTP id i17mr14555457igt.49.1403386262893;
        Sat, 21 Jun 2014 14:31:02 -0700 (PDT)
Return-Path: <accounts@chasebankus.com>
Received: from PRK105 (dupage11.rice.iit.edu. [64.131.110.120])
        by mx.google.com with ESMTPS id r12s1229567091cg.4.2014.06.21.14.31.02
        for <sdavis17@iit.edu>
        (version=TLSv1.2 cipher=RC4-SHA bits=128/128);
        Sat, 21 Jun 2014 14:31:02 -0700 (PDT)
Received-SPF: fail (google.com: domain of accounts@chasebankus.com does not designate 64.131.110.120 as
permitted sender) client-ip=64.131.110.120;
Authentication-Results: mx.google.com;
        spf=hardfail (google.com: domain of accounts@chasebankus.com does not designate 64.131.110.120 as
permitted sender) smtp.mail=accounts@chasebankus.com
Received: from localhost (:::1)
        by PRK105 with smtp (Exim 4.80)
        (envelope-from <accounts@chasebankus.com>)
        id 1WySr3-0003RY-EV
        for sdavis17@iit.edu: Sat, 21 Jun 2014 16:30:22 -0500
From: Chase Accounts <accounts@chasebankus.com>
To: Shawn Davis <sdavis17@iit.edu>
Subject: Your deposit statement is available online
```

What Happens if the User Clicks on a Phishing Link?

- Malicious site with exploit kit
 - We will talk about these in a few slides.
- Cross-site scripting (XSS)
 - Attackers inject client-side script into a legitimate web page
 - Will execute because site is trusted due to same-origin policy.
- User tricked into visiting imposter site that captures credentials

What Happens if the User Clicks on a Phishing Link?

- We'll learn more about XSS and Exploit Kits in later lectures.
- Now we'll look into creating imposter sites that capture user credentials.

SET – Social Engineering Toolkit

- Pre-installed in Kali Linux
- Creates realistic templates of websites
 - Google, Facebook, Twitter, Yahoo
- Clones any existing website

SET – Social Engineering Toolkit

- SET can be used to:
 - Launch a Java Applet attack
 - Launch Metasploit attack to deliver a reverse shell
 - Harvest user credentials
 - TabNabbing
 - Waits for user to move to a different tab which can contain a malicious page
 - Web jacking
 - Uses iframe replacements to send link which will redirect to site of attacker's choosing

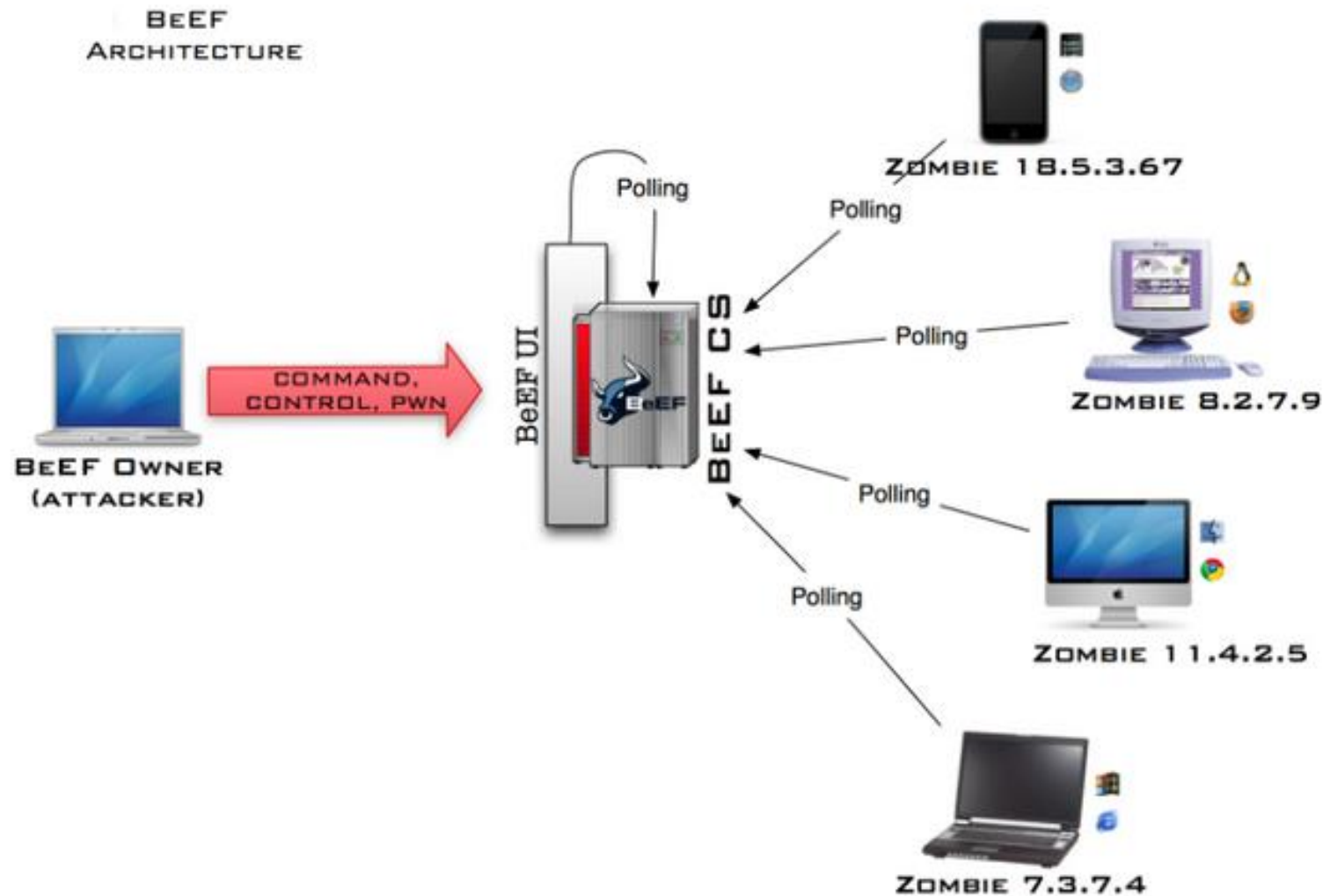
SET - Demo

- Just watch on this one
- I will use SET to use a pre-existing template of Gmail's site in order to capture credentials.

BeEF - Browser Exploitation Framework

- Penetration testing tool for web browsers
- Will help you to understand:
 - How XSS attacks occur
 - What exploits can be used against a browser

BeEF Architecture



Social Engineering / BeEF Lab – Homework 1

- In this week's homework lab:
 - You are going to use the Social Engineering Toolkit (SET) to clone a website
 - You will embed a JavaScript “hook” into the cloned page
 - Your browser (the victim) will connect to the cloned site (after receiving a phishing email)
 - You will then use BeEF to launch various attacks against your browser (the victim).


Part 4

Outside Threats

Outside Threats

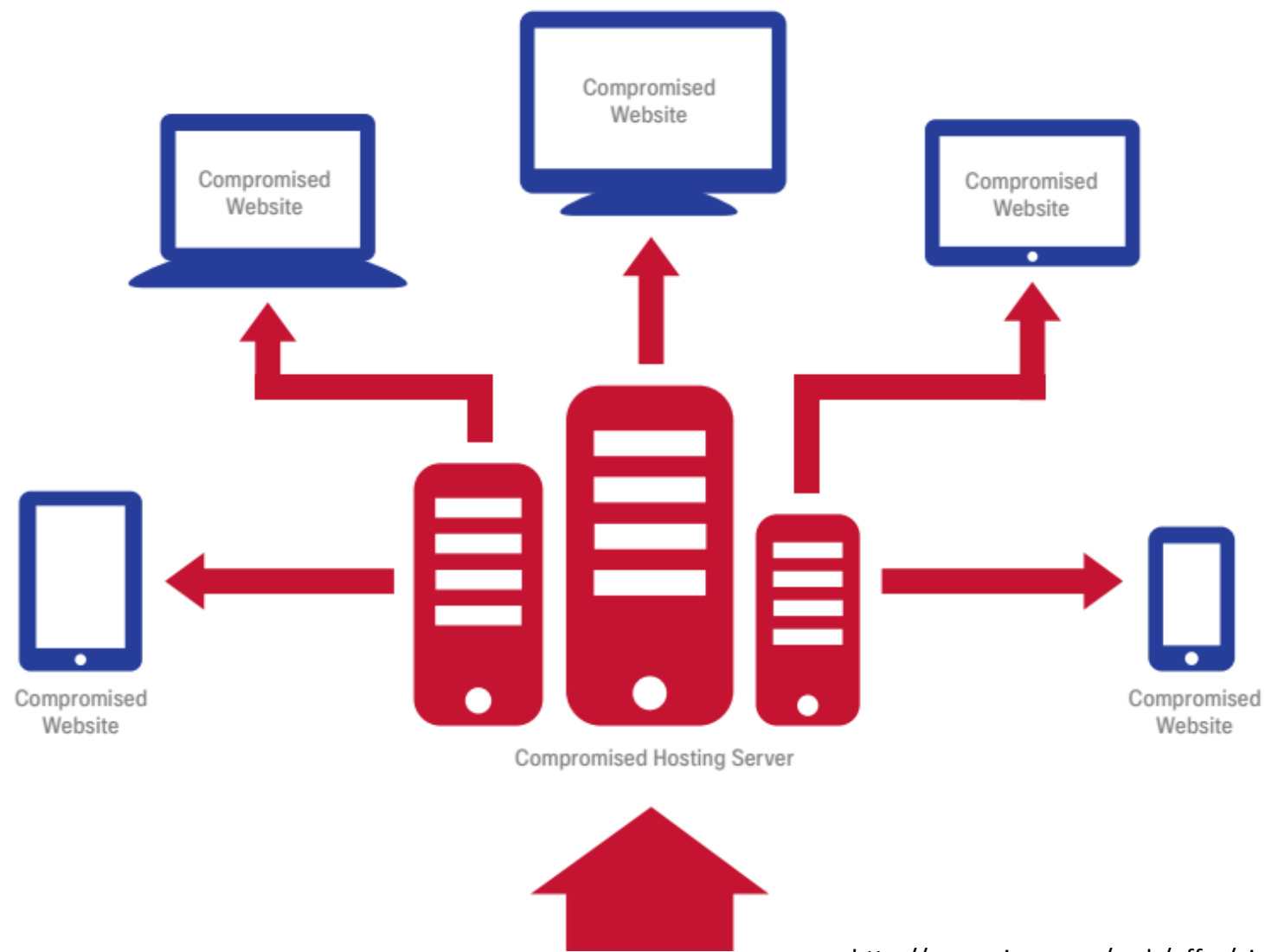
- Initiated outside security perimeter:
 - Web Exploit Kits / Malicious Websites
 - Malware (Rootkits, Viruses, Worms, etc.)
 - Social Engineering or Phishing Attempts
 - Tailgating
 - DoS / DDoS
 - Attacker Breach / Elevates Access / Backdoor

Outside Attackers



The end goal
of many cybercrime
campaigns is to
reach the data center
and exfiltrate
valuable data.

Web Exploit Kits



Common Web Exploit Kits

- We will learn more about these next week:
 - Darkleech
 - Blackhole
 - Crimeboss
 - Nuclear
 - Sweet Orange
 - Cool Exploit Kit
 - Redkit
 - Neutrino
 - Rig
 - Angler
 - Fiesta
 - Magnitude
 - Neosploit
 - FlashPack

Malware types we will learn about next week

- Virus
- Worm
- Trojan
- Bot/Botnet
- Rootkit
- Adware
- Spyware
- Keylogger
- Backdoor
- Logic Bomb
- Ransomware
- Fake A/V Trojan
- Downloader Trojan

Malware Testing

- Make sure you only test live malware inside of a virtual machine (VM) with networking turned off
- Take a clean snapshot of your VM that you can revert to after each test
- If you do need to let your malware access the internet, do not use the campus wired or wireless network
- Use TOR as a proxy if you do not want to alert the malware author to your testing

Security Tools

- Also, be careful when downloading security tools from disreputable sources
- Always download in a VM (then disable the network interface) and test the tool for malware before using on a system on your network
- You can use FakeNet to easily see outbound traffic and DNS requests that the tool may be making

Common 5 Phases of an Attack

1. Reconnaissance
2. Scanning
3. Gaining Access
 - Network Level
 - OS/App Level
 - Elevating Access
 - Denial of Service
4. Maintaining Access
5. Covering Tracks

“Anatomy of an Attack”

- Mandiant 10 common steps
 - <https://www.mandiant.com/threat-landscape/anatomy-of-an-attack/>
- SANS GIAC whitepaper on above steps but with case study on Sally Beauty breach
 - <https://www.sans.org/reading-room/whitepapers/casestudies/breach-simulating-detecting-common-attack-36157>

Common Defenses Against Reconnaissance

- Anonymous Domain Registration
- Disable DNS zone transfers
- Limit info on Social Media and Search Engines
- Limit info on technology job postings

Common Defenses Against Scanning

- Remove or secure modems
- Wireless IDS
- Disable ICMP requests
- Block Ips
- Disable unused ports/services

Common Defenses Against Gaining Access

- Network Level:
 - IDS/IPS
 - Firewalls
 - Hard coded ARP tables
 - Detect sniffers
 - Port level security on switches
 - SSH

Common Defenses Against Gaining Access

- OS/App Level:
 - Patches
 - DEP in Windows
 - Check size of user input in applications
 - Code reviews
 - Watch outbound traffic
 - A/V

Common Defenses Against Gaining Access

- Elevating Access:
 - Strong Passwords
 - Monitor sudo/admin usage
 - Check for setuid/setgid apps with root access
 - Utilize Least Privilege
 - Disable unused user accounts

Common Defenses Against Gaining Access

- Denial of Service:
 - Patches
 - IPS
 - Disable unneeded services
 - Anti-spoof filters at gateways
 - Contact ISP to block attacks upstream

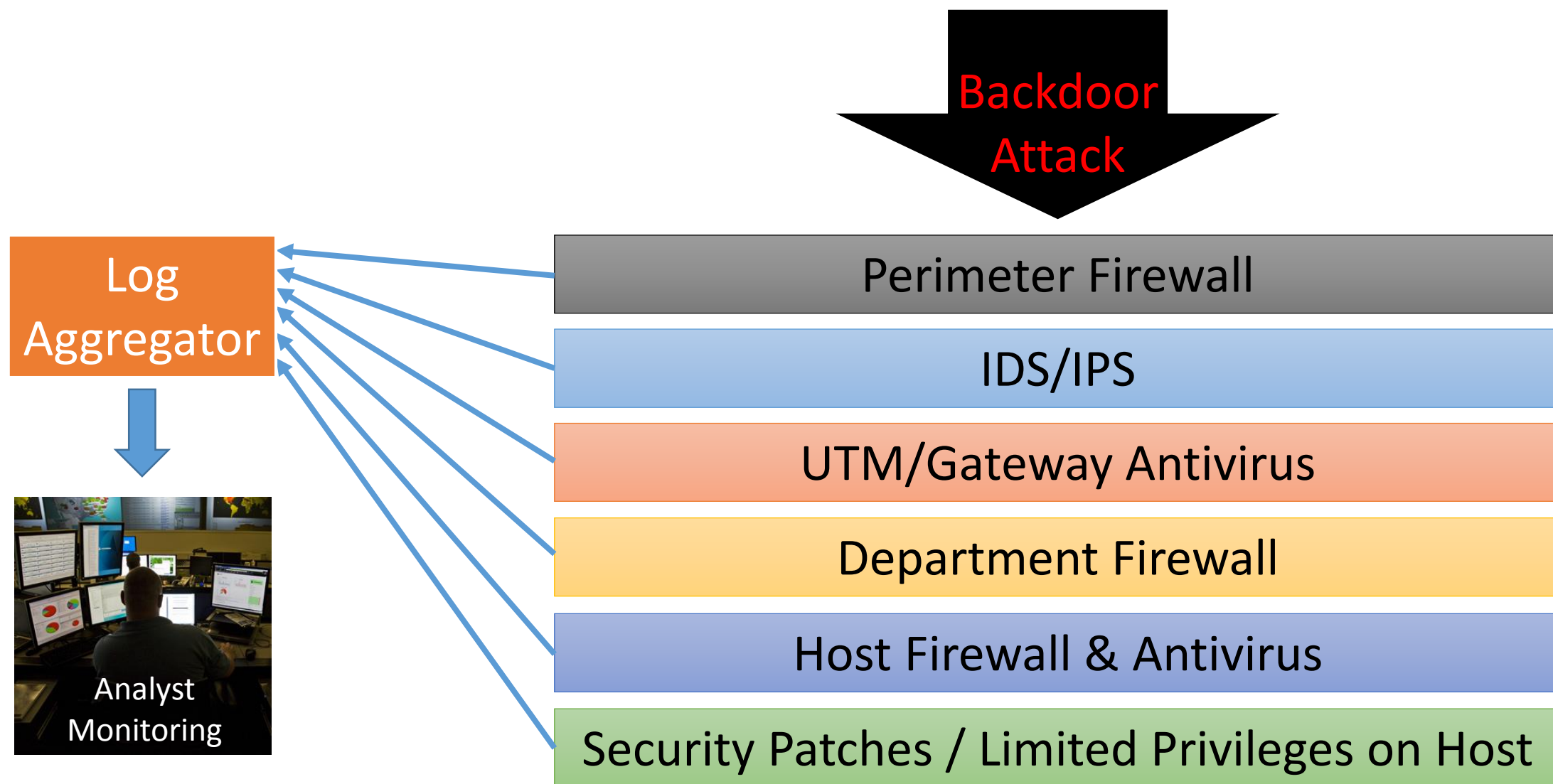
Common Defenses Against Maintaining Access

- Harden systems
- Monitor traffic (IDS Alerts, SIEM)
- Look for modified registry keys or new services
- Delete backdoors on systems
- Monitor for return of attacker

Common Defenses Against Covering Tracks

- Send logs to separate server
- Integrity checks of log files

Defense in Depth



What Defense in Depth Step is Often Missed?

- Monitoring!
 - Companies often pay millions of dollars on security appliances but don't perform timely review of alerts (if at all)

What Defense in Depth Step is Often Missed?

- Sometimes monitoring is performed but actually ignored!
 - Target installed a 1.6 million dollar FireEye malware detection system and had an overseas group to review the alerts
- Guess what happened?
 - Overseas team alerted Target corporate that malware had been installed.
 - Target corporate ignored alerts
 - 40 million debit/credit card details stolen!

You've Been Attacked

- You have done well creating policy, preparing and hardening your network/systems but you are attacked.
- What happens next?
- An Incident is declared and an established team goes through several phases to resolve the situation.

SANS Security Incident Handling Phases

1. Preparation
2. Identification
3. Containment
4. Eradication
5. Recovery
6. Lessons Learned

Part 5

Recent Popular Security Threats

Recent Popular Security Threats

- Heartbleed
- Shellshock
- POODLE
- GHOST
- Freak
- BEAST

Recent Popular Security Threats

- For each threat we will cover:
 - How it works
 - How to tell if your system is vulnerable
 - How to remediate the vulnerability
 - Example(s) of companies affected

****Don't run the update or upgrade commands on your Kali VM**

Heartbleed



Heartbleed - Overview

- Vulnerability in OpenSSL discovered in April 2014
- Issue with heartbeat extension's keep-alive functionality
- Versions 1.0.1 – 1.0.1f and 1.0.2-beta1 are vulnerable
- Allows an attacker to repeatedly read 64K chunks of memory (RAM) from a vulnerable server

Heartbleed – Overview (Cont.)

- Attackers could steal the following from RAM:
 - Server's Private Key!
 - Passwords
 - Usernames
 - Cookies
 - Etc.
- Affects any OS or device with vulnerable version of OpenSSL
 - Linux, Unix, OSX, etc.

Heartbleed – Is System Vulnerable?

- In Kali, open a terminal and run:
dpkg -l | grep openssl

```
ii  openssl                                1.0.1k-3+deb8u1  
amd64 Secure Sockets Layer toolkit - cryptographic utility
```

- Version 1.0.1k is not vulnerable

Heartbleed – Remediation

1. Upgrade version of OpenSSL to 1.0.1g or above
 - apt-get update
 - apt-get install openssl
2. Take server offline
3. Generate new private/public keys
 - Submit new public keys to certificate authority
 - Install new certificate on server
 - Ensure old key pairs are no longer being used
4. Bring server online

Heartbleed – Remediation (Cont.)

5. Revoke old certificates
 6. Force password changes for users on server
 7. Invalidate session keys
- Keep in mind if server's private key was compromised:
 - Attackers can decrypt pre-recorded packet captures

Heartbleed – Example of Compromise

- Attackers breached Community Health Systems via a Juniper VPN device vulnerable to Heartbleed
- Read enough memory to obtain active session tokens for users that were currently authenticated
- Hijacked user sessions
- 4.5 million health records stolen...

Shellshock



Shellshock - Overview

- Vulnerability in GNU Bash shell discovered in September 2014
- Versions 1.14 – 4.3 are vulnerable
- Allows an attacker access to run remote commands on a vulnerable system to gain unauthorized access
- Works by attaching malicious code in environmental variables used by the OS

Shellshock – Overview (Cont.)

- An attacker could cause a vulnerable server to:
 - Serve a reverse shell
 - Steal files
 - Create a botnet
 - DDoS

Shellshock – Overview (Cont.)

- An attacker could also cause a vulnerable server to ping back to them for example:

```
target-ip = 0.0.0.0/0
port = 80
banners = true
http-user-agent = shellshock-scan
(http://blog.erratasec.com/2014/09/bash-shellshock-scan-of-
internet.html)
http-header[Cookie] = () { ;; }; ping -c 3 209.126.230.74
http-header[Host] = () { ;; }; ping -c 3 209.126.230.74
http-header[Referer] = () { ;; }; ping -c 3 209.126.230.74
```


Shellshock – Is System Vulnerable?

- Shellshocker tool to test for vulnerability:
- Could download shellshock_test.sh

```
CVE-2014-6271 (original shellshock): not vulnerable
CVE-2014-6277 (segfault): not vulnerable
CVE-2014-6278 (Florian's patch): not vulnerable
CVE-2014-7169 (taviso bug): not vulnerable
CVE-2014-7186 (redir_stack bug): not vulnerable
CVE-2014-7187 (nested loops off by one): not vulnerable
CVE-2014-//// (exploit 3 on http://shellshocker.net/): not vulnerable
```

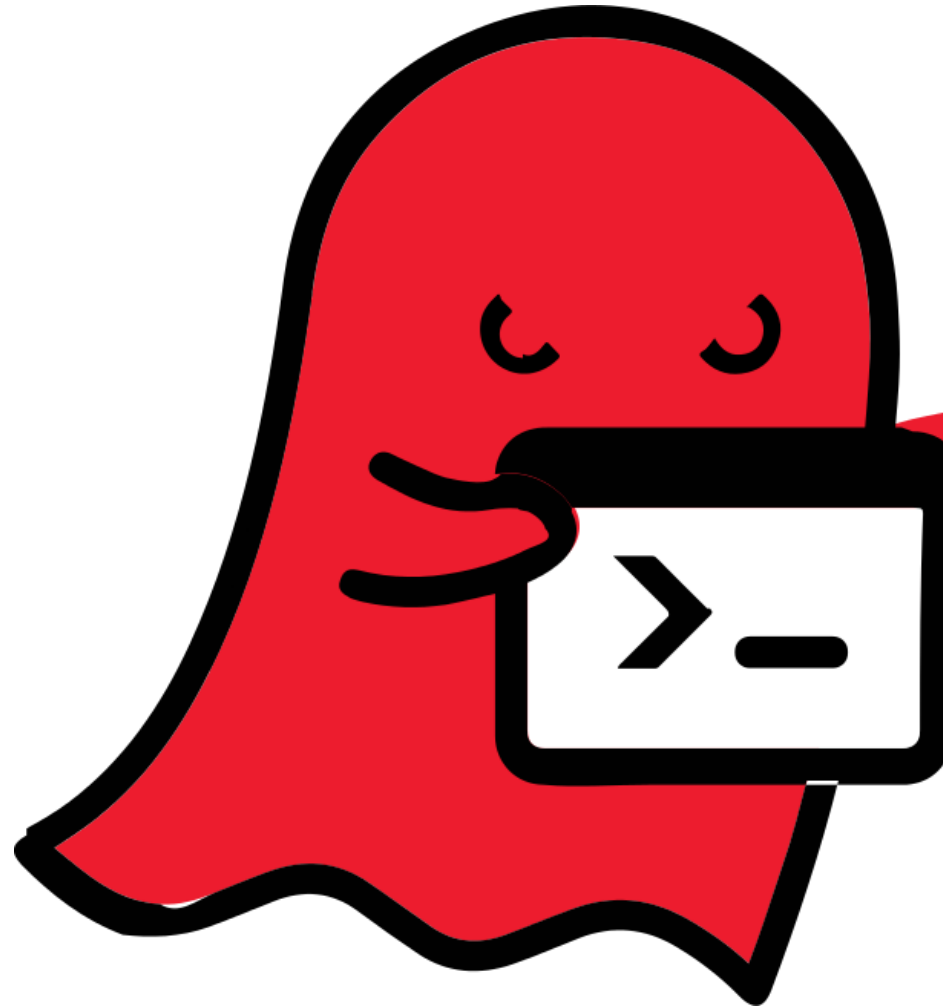
Shellshock – Remediation

1. Update repos
 - `apt-get update`
2. Upgrade bash
 - `apt-get install --only-upgrade bash`

Shellshock – Attack Examples

- Used for DDoS against Akamai Technologies and U.S. DoD
- Attack examples seen in the wild:
 - <https://isc.sans.edu/forums/diary/Shellshock+A+Collection+of+Exploits+seen+in+the+wild/18725>
- Exploit examples:
 - <http://resources.infosecinstitute.com/practical-shellshock-exploitation-part-2/>

GHOST



GHOST - Overview

- Vulnerability in glibc library used in most Linux distros discovered in January 2015
- Versions 2.2 and other 2.x versions before 2.18 are vulnerable
- Allows a remote attacker ability to take control of vulnerable system via remote code execution
- Caused by buffer overflow in gethostbyname functions that do IP to host name lookups

GHOST – Overview (Cont.)

- An attacker could create a message or network request to overflow the buffer to potentially take control of the system

GHOST – Is System Vulnerable?

- GHOST.c tool to test for vulnerability:

```
wget https://webshare.uchicago.edu/orgs/ITServices/  
itsec/Downloads/GHOST.c
```

```
cat GHOST.c
```

```
gcc GHOST.c -o GHOST
```

```
./GHOST
```

```
not vulnerable
```

GHOST – Remediation

1. Update repos
 - `apt-get update`
2. Upgrade bash
 - `apt-get install --only-upgrade libc6`

GHOST – Attack Examples

- Metasploit exploit created for remote code execution against Exim mail server on vulnerable systems:
 - <https://community.qualys.com/blogs/laws-of-vulnerabilities/2015/03/17/ghost-remote-code-execution-exploit>

Other Recent Popular Security Threats

- We will cover POODLE, Freak, and BEAST after the Cryptography lecture

Useful Security Sites

- SANS Internet Storm Center
 - <https://isc.sans.edu/>
- US-CERT
 - <http://www.us-cert.gov/>
- Mitre
 - <https://cve.mitre.org/>
- NIST
 - <http://www.nist.gov/information-technology-portal.cfm>
- Nice list of 100+ Cyber Security Blogs and Infosec Resources:
 - <http://ddosattackprotection.org/blog/cyber-security-blogs/>

Text References

- Skoudis, E., & Liston, T. (2006). Counter Hack Reloaded (2nd ed.). Boston, MA: Pearson Education, Inc.
- Whitman, M., & Mattord, H. (2010). Management of Information Security (3rd ed.). Boston, MA: Course Technology.

Homework / Project Info

- Review and understand this slide deck on Blackboard
- Email me before 1/18 if you would like me to consider a specific service for your individual project
- Complete Homework1 located on Blackboard under “Homework Assignments.”
 - Due before midnight on Jan. 24th
 - This is no class next week due to Martin Luther King Jr. Day

Questions???

