



Virginia Information Technologies Agency

Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

January 4, 2012



ISOAG January 2012 Agenda

- | | | |
|------|---|---|
| I. | Welcome & Opening Remarks | Michael Watson, VITA |
| II. | Data Security Challenges
In Public Sectors | Patrick Gray, CISCO Systems |
| III. | Pass the Hash | Eric Taylor, NG |
| IV. | IT Security Audit Standard
Changes SEC502-02 | Michael Watson, VITA |
| V. | Upcoming Events & Other Business | Michael Watson, VITA |
| VI. | Partnership Update | Bob Baskette, VITA
Moses Camacho, Michael Clark,
Brandi Lucas, & Jan Weiner, NG |

Patrick Gray
Principal Security Strategist



DATA SECURITY CHALLENGES IN THE ALL TOO PUBLIC AND NOT SO PRIVATE SECTORS

I want you to take home four points

- Understand that you are a target for the hacking community
- Educate those around you
- Collaborate with your peers
- Prepare for the day that you give up data

It's a great to be here today, but uh, do you know where your data is right now?

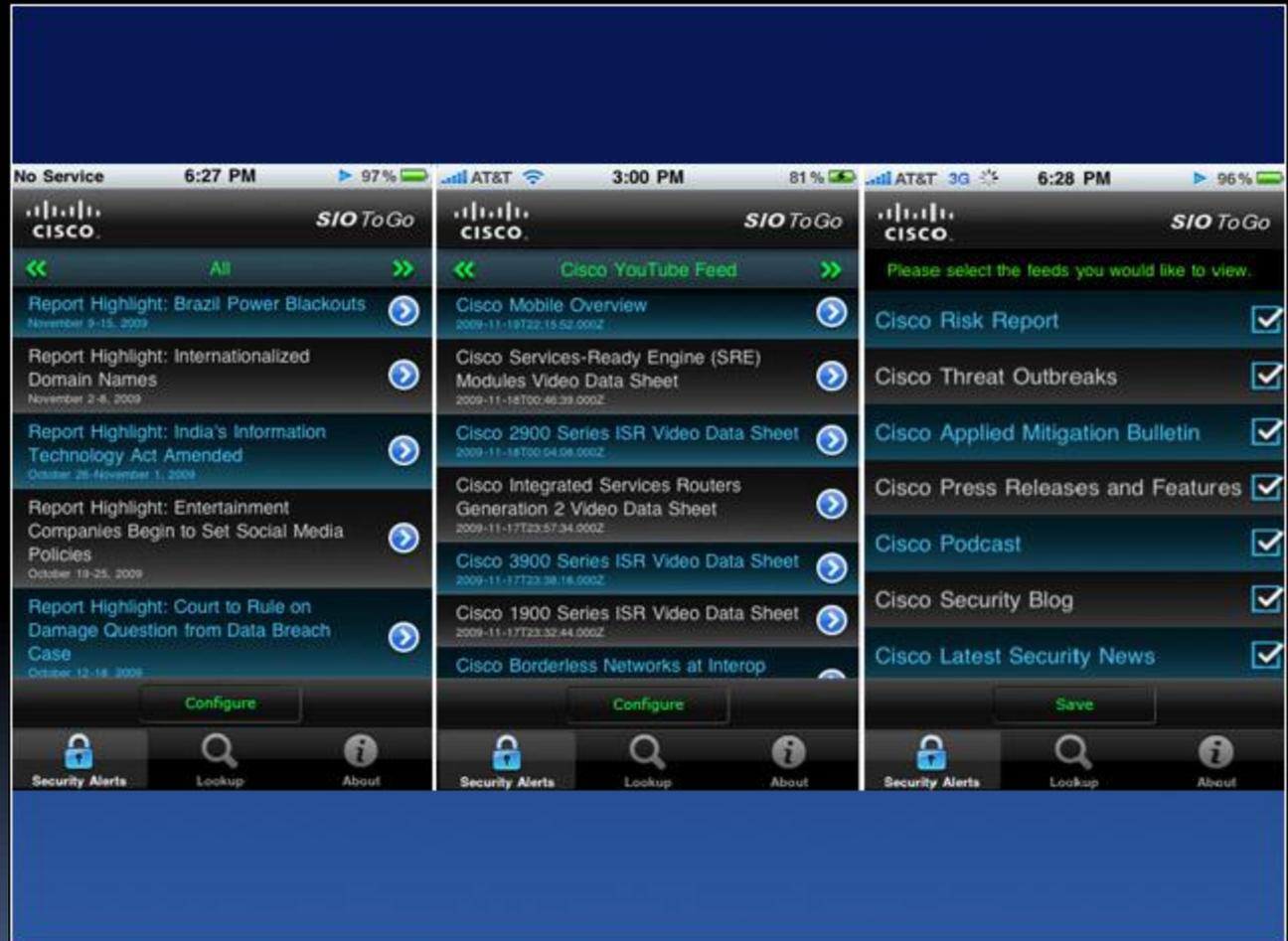
- It's all about data, your data
- The confidentiality
- The integrity
- The availability



It's hard to protect data when we really don't even know where it is!

- So, where is your data today?
- In the cloud
- On any device
- Any place
- Any time
- When “aren't” we working anymore?
- When do we call it a day?
- We don't, do we?

Cisco SIO to Go – Great App



Today, it's about mobility...

- In the past few years we shifted our lives to the PC and the Internet
- Now, it's all about being mobile
- A PC in your pocket
- Our mobile work force is growing and expanding



Where?

- Where does work happen?



It happens wherever we are!

- No longer does business take place solely behind network walls
- The critical work is happening increasingly on social networks, on handheld devices, in the field, and at local cafes



Diminishing Border

- The traditional IT perimeter, with clearly identifiable boundaries, has diminished
- In its place, a network with limitless potential is rising
- One where agencies, businesses and employees, demand access to information whenever and wherever they need it



New Considerations

- It is information technology's role to ensure that the appropriate people, using the correct devices, are accessing the proper resources while having a highly secure yet positive user experience within your networks



A blurring of activities

- In addition, it is common for workers to blend business and personal communications on these social networks, further blurring the network perimeter

Where are we going and what are we doing?



Some bone-jarring statistics

- 50% of Facebook active users log on to Facebook on any given day
- More than 60 million users update their status - daily
- People spend over 500 billion minutes per month on Facebook

Billions

- More than 3 billion photos uploaded to the site each month
- More than 5 billion pieces of content (web links, news stories, blog posts, notes, photo albums, etc.) shared each week



The involvement is viral

- Millions of local businesses and Government Agencies have active Pages on Facebook
- More than 20 million people become fans of Pages each day
- Pages have created more than 5.9 billion fans



Mobility

- There are more than 350 million active users currently accessing Facebook through their mobile devices

I just have to check...

- Just last month, 57 million Americans visited social networking sites from a work computer
- Checking your Facebook account has become the default Water Cooler
- It's the most commonly visited website at the workplace, twice as popular as Google and three times as popular as Yahoo

Cisco on Facebook

The screenshot shows the Facebook interface for the Cisco Systems Security page. The page header includes the Facebook logo, a search bar, and navigation links for Home, Profile, and Account. The main content area features a cover photo with the Cisco logo and the text "Welcome to the human network." Below this is a navigation menu with options like Wall, Info, Photos, Notes, Events, and ACCESS DENIED!. The main post area displays a wall with a post from Cisco Systems Security about network security best practices, including a link to a blog post. The post has 37 likes and a comment from Jude Jesse. The right sidebar contains sections for "You and Cisco Systems Security" (44 friends like this), "Friends' Photos" (tagged Jimmy Ray Purser), and "Sponsored" ads for a painter and Rackspace. The bottom of the page shows a chat window with 9 active chats and a system tray with "Done", "Internet", and "100%" indicators.

facebook Search Home Profile Account

Cisco Systems® Security

Computers/Technology [Create a Page](#)

Wall Cisco Systems® Security · Top Posts

Share: Post

Write something...

Cisco Systems® Security
Best Practices - allowing traffic THROUGH the network, but not TO the network - iACLs and Other Good Security Tricks <http://bit.ly/osIdAd>

Top of Mind: Best Practices and Security Updates
blogs.cisco.com

7 hours ago · Like · Comment · Share

37 people like this.

Jude Jesse Allowing traffic withing network and not allowing incoming from outside is safe but limit internal user to outside.
5 hours ago · Like

Write a comment...

Cisco Systems® Security
India goes after Blackberry (again). Humble smartphones too secure?
<http://bit.ly/nj2mwn>

India cracks down on the Blackberry • The Register
www.theregister.co.uk
The use of the humble Blackberry may be outlawed in India if Research in Motion fails to comply with the government's strict security demands.

13 hours ago · Like · Comment · Share

41 people like this.

You and Cisco Systems® Security
44 friends like this.
TechWiseTV

Friends' Photos [Show More](#)

Tagged: Jimmy Ray Purser
23 Likes · 22 Comments

Tagged: Jimmy Ray Purser
1 Like

Sponsored [Create an Ad](#)

North Atlanta's Painter
certapro-alpharetta.com
We provide the highest quality painting work with the best possible service to our customers.

Rackspace is hiring!
jobs.rackspace.com
Our team continues to grow! Join an organization that values your unique contributions and individual strengths!

Conscious-Universe [Chat \(9\)](#)

Done Internet 100%

Cisco on Twitter

Welcome to #NewTwitter! Read up on what's new. You can still access old Twitter for a limited time. Close x

twitter Search Home Profile Messages Who To Follow pgray525



Cisco Security

@CiscoSecurity Baked into the network.
Cisco Security - product information, industry news and random things that may be of interest to security pros.
<http://www.cisco.com/go/security>

Following

Tweets Favorites Following Followers Lists

Cisco Security Cisco Security
5% of PCs are infected, 7 of Top 10 Threats leverage Java vulnerabilities <http://bit.ly/m3TmYz>
6 hours ago

Cisco Security Cisco Security
Malware brings its own DHCP server <http://bit.ly/iUvIrL> via @TechLOG
8 hours ago

Cisco Security Cisco Security
Govt Spearphishing effective but more persistent than advanced <http://bit.ly/iD7T5X> - says something about low hanging fruit
4 Jun

Cisco Security Cisco Security
Attrition documents Sony breaches <http://bit.ly/iORKjt> via @corq - handy reference
4 Jun

Cisco Security Cisco Security
From Flip Cameras to flippin' grilled cheese sandwiches <http://bit.ly/iwCaMR> here they open in San Jose soon

About @CiscoSecurity

4,015	682	25,311	1,643
Tweets	Following	Followers	Listed

You and @CiscoSecurity
You follow accounts that follow @CiscoSecurity - view

Similar to @CiscoSecurity - view all

- geekgrll** @missa · Follow
□. Breaker of Things. Christian. 633K. Humor=DRY...
- rwestervelt** Robert Westervelt · Follow
Reporter/Editor, News Director for SearchSecurity.c...
- b10w** [-b10w]- · Follow
Hacker, security twit, budding social engineer, digita...

Following - view all

About Help Blog Mobile Status Jobs Terms Privacy Shortcuts Advertisers Businesses Media Developers Resources © 2011 Twitter

Cisco on YouTube



Search

Browse

Upload

Create Account

Sign In



CISCO PR
CSCOPR's Channel

Subscribe

All

Uploads

Favorites

Playlists



Search Uploads

Date Added | Most Viewed | Top Rated



Cisco Announces Webex Connect

155 views
2 days ago



Dialogue Cafe Portuguese

19 views
3 days ago



Dialogo Cafe Launch in Rio de

13 views
3 days ago



Cisco Digital Media Suite

110 views
4 days ago



Jerry Monroe, head of Cisco's

34 views
4 days ago



Cisco TelePresence

303 views
4 days ago



Holyoke Smart+Connected

164 views
4 days ago



Cisco Introduces Flip Prosumer

265 views
4 days ago



Mike Baird, Cisco TTG Director of

114 views
5 days ago



TELUS Changes the Game with

130 views
5 days ago



Marthin De Beer, SVP of Cisco's

101 views
5 days ago



Howard Charney talks from

38 views
6 days ago



Cisco Demos Multi-Vendor, Multi-

613 views
1 week ago



ClearPath Demo

474 views
1 week ago



Cisco Sports and Entertainment:

153 views
1 week ago



Cisco at UTTelecom

113 views
1 week ago



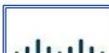
Talk2Cisco Promo: Global Demand for

94 views
1 week ago



Cisco and Apollo to Create Smart

111 views
2 weeks ago



CSCOPR

Subscribe

Friends (13)

ideas.
insights.
information

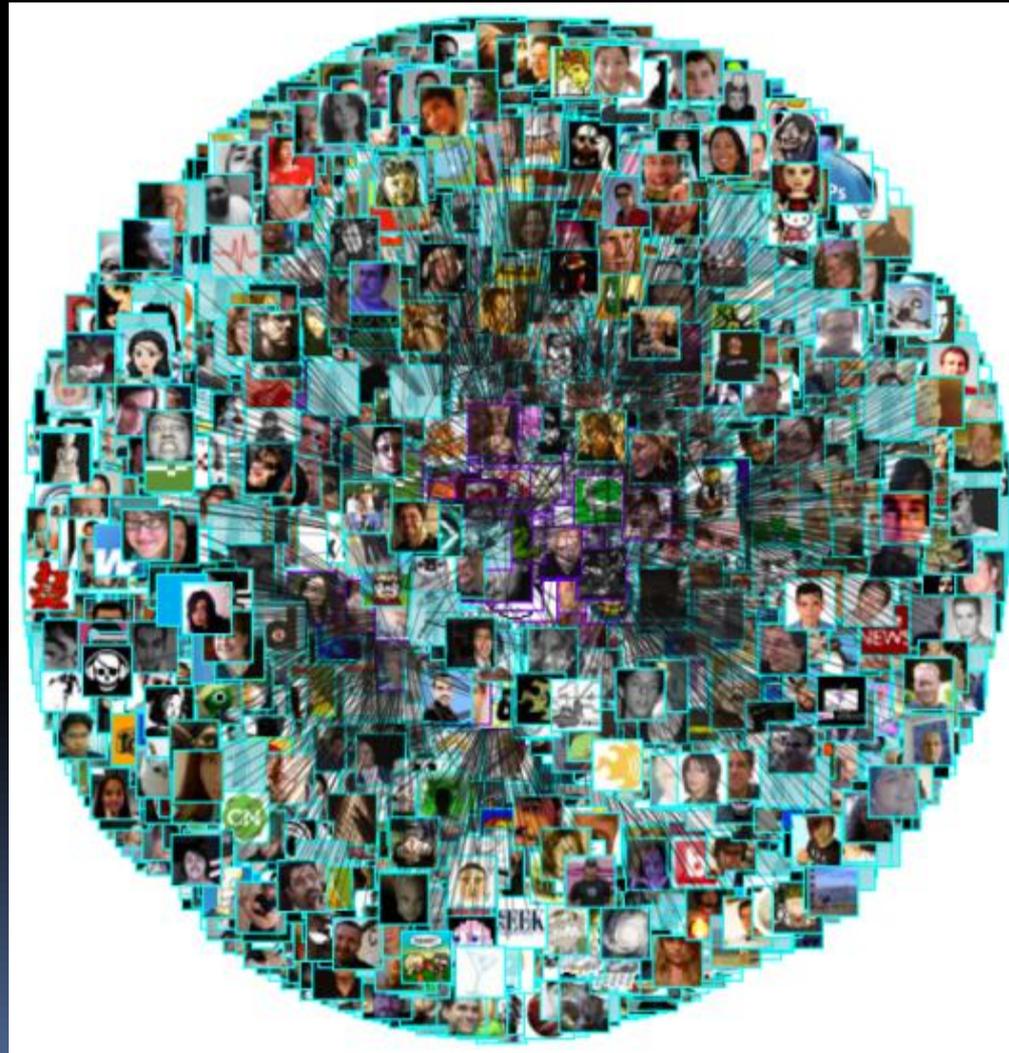


This is viral

- Overall, 54 percent of Americans said they keep in touch via social networking websites such as Facebook and LinkedIn

It's no longer just close relationships

- Our employees are going places they've never gone before and are touching technology daily
- That which they are touching is touching our networks as well



That being said...

- There are things we really need to be aware of
- The bad guys know what we're doing, where we're going and want to make the trip a wee bit more difficult

With Web 2.0

- A new breed of malware is evolving
- Google Mashups, RSS feeds, search, all of these can be misused by hackers to distribute malware, attack Web surfers and communicate with botnets

Risk – it's everywhere

- And no one knows that better than IT security professionals
- Disgruntled employees, students, fired employees, clueless employees who succumb to social engineering, passwords left on Post-it notes, wide-open instant messaging and increasingly powerful hacker tools in the hands of teenagers, Web Mobs and Organized Crime targeting Social Media sites

Objective?

- The key objective, of course, is to recognize risk, safeguard your reputation and not reveal sensitive or confidential information that may prove quite harmful to your business

Malware

- Historically, malware has plagued e-mail, hidden in malicious attachments
- While that's still happening, more malware writers are putting their efforts into malicious Web sites
- The goal in developing malware is not to simply infect as many systems as possible but to specifically steal usage information and other data from compromised systems
- Use of polymorphic code that constantly mutates

Two biggest vectors for Malware

- Email
- Web-based

The Human Firewall – an invaluable tool

- A good *human firewall employee* is one who filters good security practices and rejects any others—much like a network firewall only allows authorized traffic and rejects any other
- The only way to build a good human firewall is to raise people's awareness; to teach them good habits, to make them recognize bad practices and change them into good practices
- Your cyber security is only as good as the people who manage it and those who use it

So Patrick, why do we really need that Human Firewall?

- Because, 'Friend' has become a verb
- Social media users believe there is protection in being part of a community of people they know
- Criminals are happy to prove this notion wrong

Causation

- The threats and security issues that come with social media aren't usually caused by vulnerabilities in software
- More commonly, these threats originate from individuals who place an unwarranted amount of "transitive trust" in the safety of these communities

Remember...

- On social sites –
 - Your privacy is history
 - They don't have your best interests in mind
 - Social engineering attacks are getting more targeted

Trust?

- Users will trust something or someone because a user they know has also expressed trust in that person or subject
- We trust because we are curious and curiosity...

Curious? This is why! Out of date???

The screenshot shows a Mozilla Firefox browser window displaying a YouTube page titled "Secret video by Tom". The browser's address bar shows a URL with a search parameter. The page content includes a video player area that is currently displaying a message: "Your version of Flash player is out of date. Please download this update." with a "Download" button. To the right of the video player, there is a user profile for "Tom" with a cartoon image of Tom and Jerry, and details: "From: Tom", "Joined: 1 year ago", "Videos: 5", and "Subscribe". Below the profile, it says "Added: August 09, 2007 (more info)" and "Embed: Customize". There are also links for "More From user" and "Related Videos".

At the bottom of the browser window, a Windows dialog box titled "Opening flash_update.exe" is open. The dialog box contains the following text: "You have chosen to open", "flash_update.exe", "which is a: Application", "from: http://www.sdkpc.org", and "Would you like to save this file?". There are "Save File" and "Cancel" buttons at the bottom of the dialog box.

Comments on the page include:

- Commentary Statistics & Data
- Video Responses: 10 Text Comments: 70
- [babachat](#) (4 hours ago) 0
- Marked as spam
- Reply
- Funniest thing EVER!!
- [cmith1199](#) (6 hours ago) 0

The unknown... DO NOT TOUCH THIS!!!

WARNING!!! Quick System Scan Results 



XP antivirus Online Scanner detected dangerous spyware on your system!

Detected malicious programs can damage your computer and compromise your privacy. It is **strongly recommended** to remove them immediately.

Name	Type	Risk level
 Spyware.IEMonster.b	Spyware	CRITICAL
 Zlob.PornAdvertiser.Xplisit	Spyware	High
 Trojan.InfoStealer.Banker.s	Trojan	Medium

Protection Center

Security Status
manage security modules

System Scan
scan & fix your computer

Firewall
protect your network security

Advanced Cleaner
optimize system performance

Check for updates
update virus definitions

Settings
manage your preferences

System scan

Scan & fix your computer

Scan type: Quick Deep Memory Scan



#	Vendor	Type	Location	Threat Level
<input checked="" type="checkbox"/>	Trojan-Cookie.Win3...	Malware	C:\Documents and Settings\Hool_K...	Medium
<input checked="" type="checkbox"/>	GayCodec.lookAlert	Malware	C:\WINDOWS\System32\wshatn.dll	Medium
<input checked="" type="checkbox"/>	webSearch.Win32	Malware	C:\WINDOWS\System32\Drivers\es...	Medium
<input checked="" type="checkbox"/>	PORN_perversion.R30	Malware	C:\WINDOWS\System32\Drivers\s...	Medium
<input checked="" type="checkbox"/>	Virus.Win32.Gpco...	Viruses	C:\WINDOWS\System32\Wbe...	High
<input checked="" type="checkbox"/>	Email-Worms.Win...	Network ...	C:\WINDOWS\System32\Wbe...	High
<input checked="" type="checkbox"/>	Net-Worms.Win32...	Network ...	C:\WINDOWS\Fonts\85855.fon	High
<input checked="" type="checkbox"/>	Net-Worms.Win32...	Network ...	C:\WINDOWS\Fonts\small.fon	High
<input checked="" type="checkbox"/>	Trojan-Downloader...	Trojan Prog...	C:\WINDOWS\Help\camera.hp	Medium

Scan complete.

Objects scanned: 30329

Threats detected: 19

Removed: 0

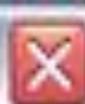
Upgrade to full version now!
Easy one-click registration



Your Computer is not protected
[click here to fix security problems](#)



Windows Security Alert



To help protect your computer, Windows Firewall has detected activity of harmful software.

Do you want to block this software from sending data over the Internet?



Name: **Trojan-Spy.Win32.GreenScreen**

Risk Level: **CRITICAL**

Description: This is spy trojan that installs itself to the system, hides itself and then captures screen images and saves them to disk files in encrypted form. Thus it allows to a hacker to watch screen images.

Keep Blocking

Unblock

Enable Protection

Windows Firewall has detected unauthorized activity, but unfortunately it cannot help you to remove viruses, keyloggers and other spyware threats that steal your personal information from your computer, including your Credit Card data and access passwords to the online resources you use. [Click here to pick recommended software to resolve this issue.](#)



SystemDefender

[HOME](#)

[DOWNLOAD](#)

**YOUR SYSTEM MAY BE
INFECTED!**

Scanning:

Internet threats and viruses found:

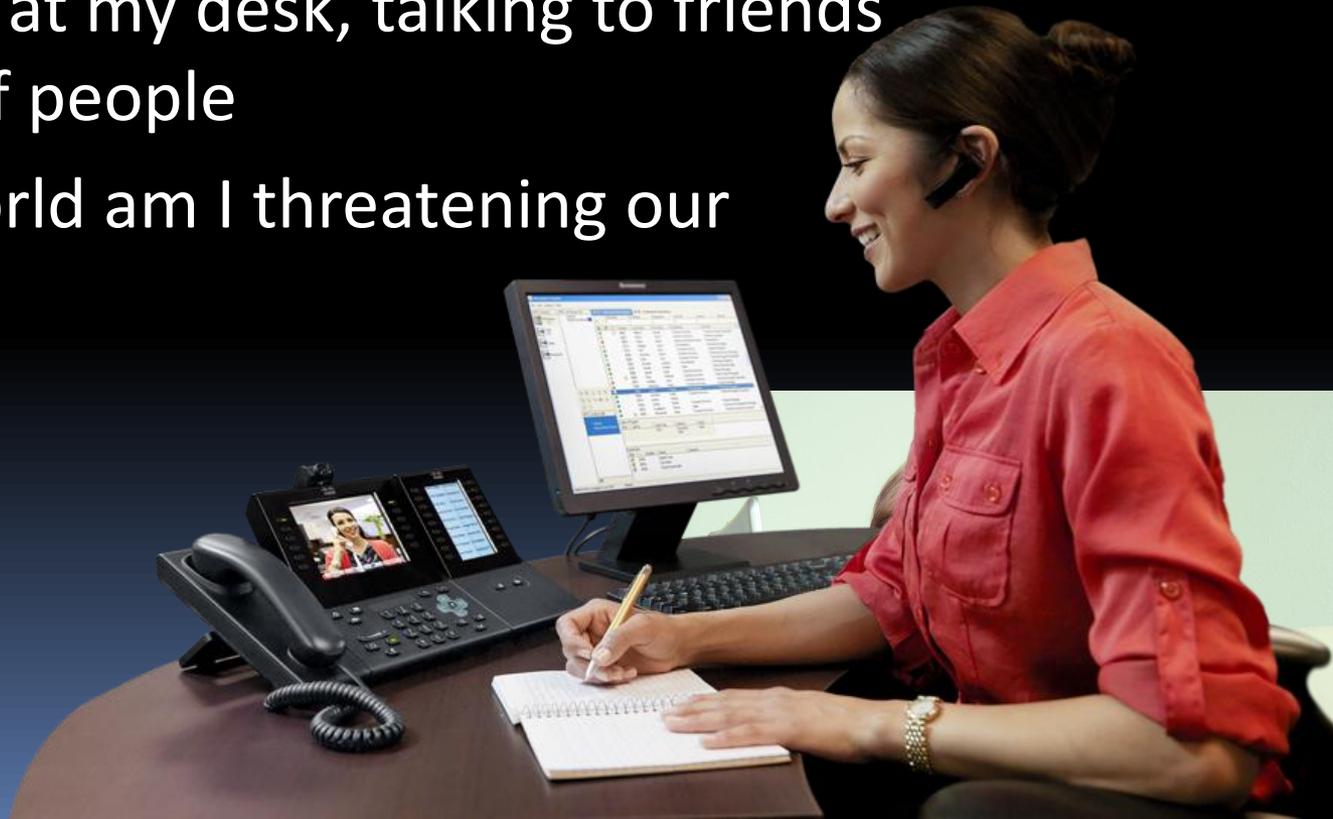
FREE SCAN NOW!

This is what our users are up against...
Malware popping up out of nowhere !

- Don't go there
- Stay on the path you know well
- Okay to trust but please verify
- Have fun, but monitor...
- Be a bit more vigilant
- And manage appropriately

But what does all this mean?

- I am just a user and am not an engineer or a technician or a programmer or a geek!
- I'm just sitting at my desk, talking to friends and all sorts of people
- How in the world am I threatening our network???



2 Reasons...

- You probably do not understand policies, procedures, best practices and standards
- If you do understand them, they are violated because there are no consequences – the policies are not enforced
- Who, me?

Education is Critical

- Few executives grasp the case for investing in safeguards against hackers, malware, and the like
- Education starts at the top and works its way down the food chain throughout the entire business
- Before any employee puts their fingers on the keyboard they must understand that it is not their computer

The Seven Deadly Sins of Network Security

1. Not measuring risk
2. Thinking compliance equals security
3. Overlooking the people
4. Lax patching procedures
5. Lax logging, monitoring
6. Spurning the K.I.S.S.
7. Too much access for too many

The Opposing Team

- The Hackers
- Disgruntled Insiders
- Clueless employees
- Foreign Governments
- Terror organizations

Biggest Players in the Global Black Market

- Russia
- China
- Brazil
- Israel
- U.S.

Top 8 Perceived Threats

- System penetration
- Sabotage of data
- Theft of proprietary information
- Denial of service
- Viruses and Worms
- Unauthorized insider access
- Laptop theft
- Insider abuse of the Internet

System Penetration

- It is an unfortunate reality that you will suffer a breach of security at some point
- To bypass security, an attacker only has to find one vulnerable system within the entire network
- But to guarantee security, you have to make sure that 100 percent of your systems are invulnerable -- 100 percent of the time

Whether you get hacked depends...

- Do you assume the posture of, “It can’t happen here.”
- Do you hear, “We haven’t heard of any worm outbreaks and all seems quiet. Why upgrade those devices?”
- “We have no budget.”
- “We’re just hanging out in the office!”
- “They’re only going after the US Government and those really big banks.”
- Then my question is, “Can you really afford to give up data today?”

So, what are they really after?

- Your data
- Your student's data
- Your employee's data
- Your personal data
- Your paycheck
- Your friends
- Your family

You are the last line of Defense! Step up!

- Understand
- Educate
- Collaborate
- Prepare

Thank You!



- pagray@cisco.com



Pass the Hash

*Eric Taylor, Cyber Security Architect
IT Infrastructure Partnership Team*



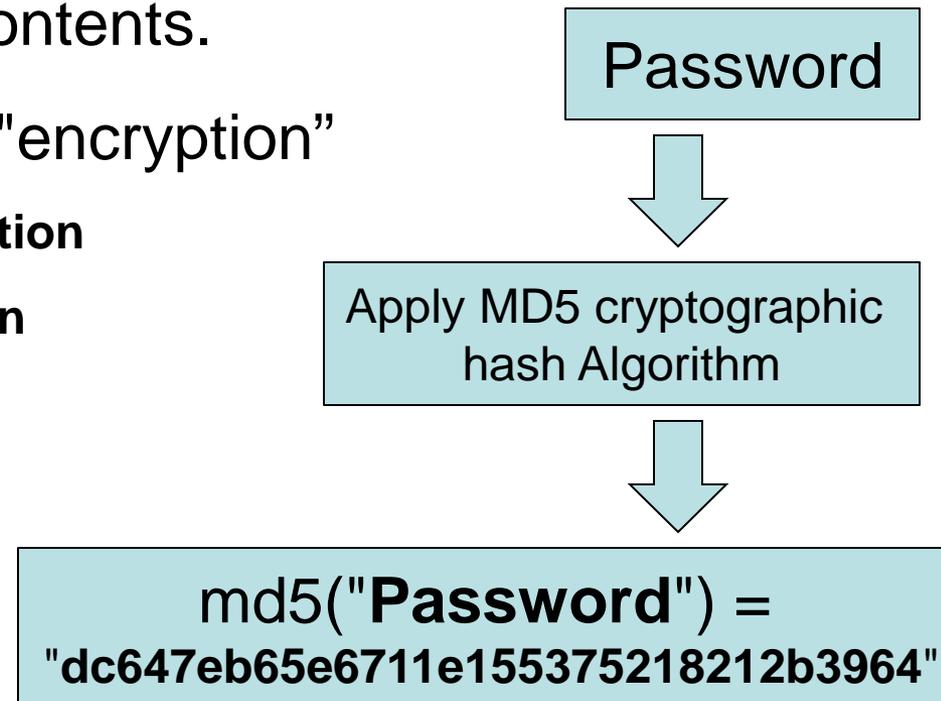
NORTHROP GRUMMAN

‘Pass-The-Hash’

- Pass-The-Hash is a password attack; passwords are not cracked, but it's the use of the precomputed hashes in the Windows authentication design.
- The weakness in the Windows design is the use of unsalted password hashing algorithms
- Pass-the-hash attacks work against very long passwords, passphrases, smart cards, two factor authentication (some types), etc.
- 1997 when Paul Ashton posted on Bugtraq a Windows exploit named "NT Pass the Hash"

What is a Hash

- A cryptographic hash function that takes an arbitrary block of data and returns a fixed-size bit string
- Simple terms: is a kind of "signature" for a stream of data that represents the contents.
- Hashes are "digests", not "encryption"
 - Encryption - a two-way operation
 - Hashing - a one-way operation
- How are Hashes used?
 - Verifying file integrity
 - Digitally Signed Documents
 - **Hashing passwords**

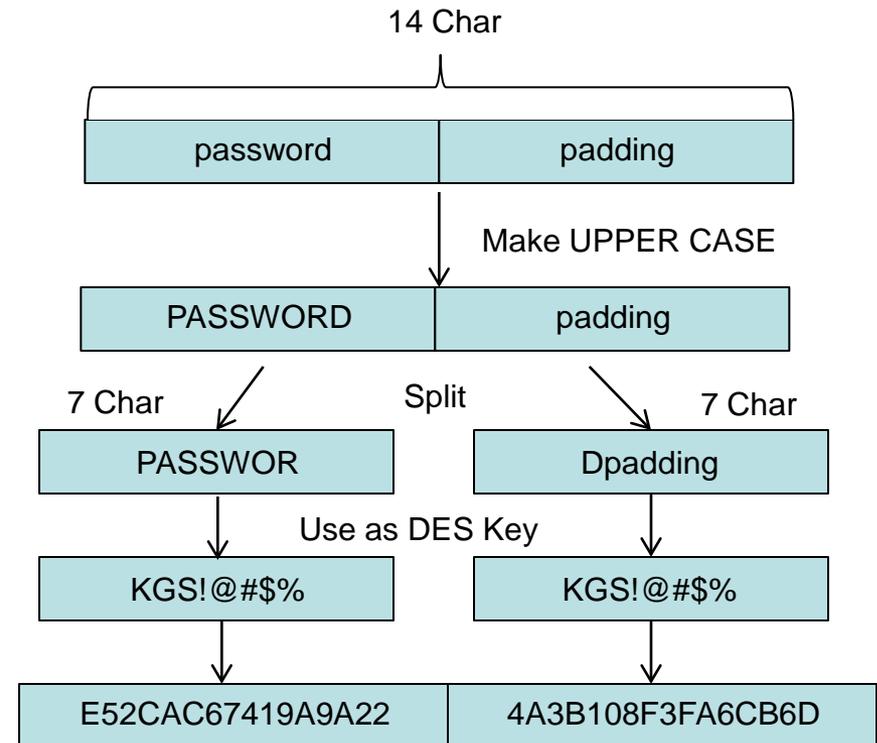


Windows Password Hash

- Two types of password hashes that are used:
 - LAN Manager (LM)
 - Windows NT hash (NTLM)
- LM hash is only used in conjunction with the LM authentication protocol
- Windows NT hash is **used** with NTLM, NTLMv2 and Kerberos authentication protocols
- By default, both are stored in NT, 2000, XP and 2003
 - LANMAN Hashes are not stored in Vista, Windows 7 and 2008 by default (although that can be altered)

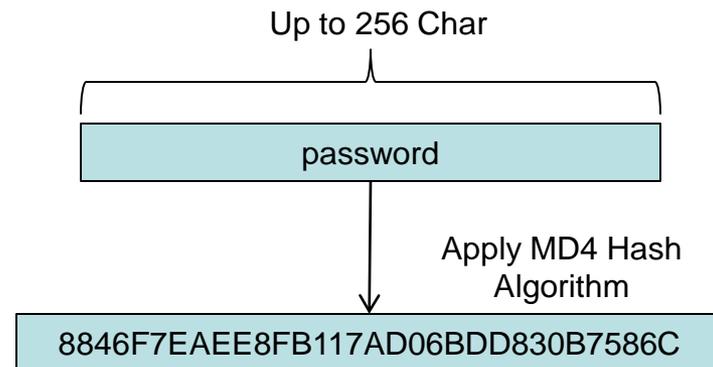
LANMAN Hash Algorithm

- If passwords < 15 characters, pad it to exactly 14 characters
- Convert to upper case
- Break into two 7 character pieces
- Use each piece as a DES key to encrypt a constant of KGS!@#\$\$%
- Concatenate two pieces



NT Hash Algorithm

- The full password is hashed using MD4
 - Case is preserved
 - Passwords up to 256 characters long
- Neither LANMAN nor NT hashes are salted
 - Makes Rainbow Table attacks much more feasible.

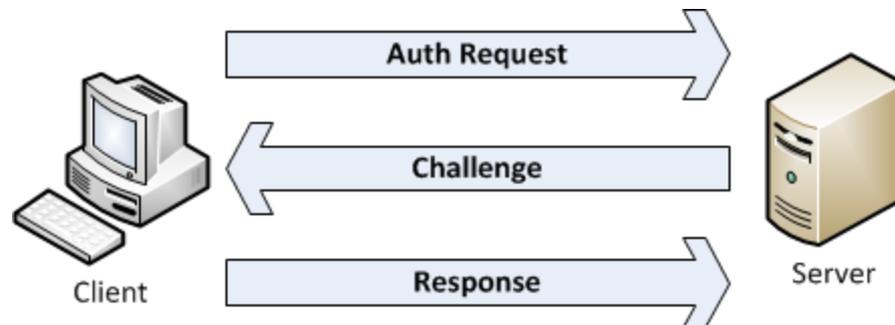


Challenge Response Protocol

- From a the network perspective, Windows supports multiple forms of cryptographic authentication:
 - LANMAN Challenge/Response
 - NTLMv1
 - NTLMv2
 - Microsoft Kerberos
- Response differs depending on authentication protocol version used
- LM, NTLM hashes not sent over the wire.
- Having LM/NTLM Hashes allows to calculate response

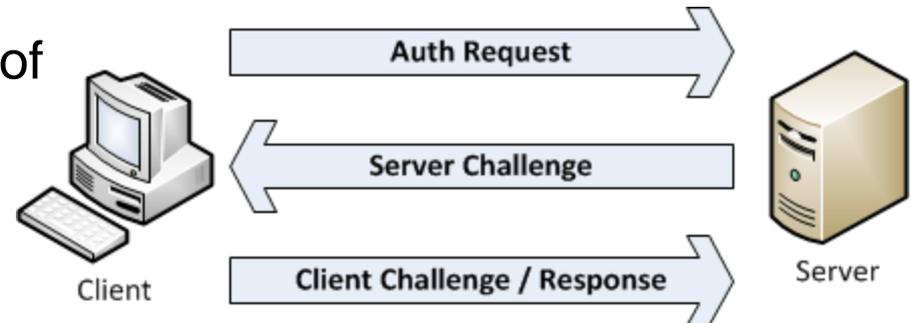
LANMAN Challenge/Response

- Client initiates authentication
- Server sends challenge
- Client formulates response from challenge by:
 - Padding LANMAN hash to 21 bytes
 - Splitting LANMAN hash into 3 seven-byte pieces
 - Using each piece as a DES key to encrypt challenge
- NTLMv1 does the same thing, except it uses NT hash as starting point for this operation



NTLMv2 Challenge/Response

- Much more sophisticated form of authentication
- Client initiates authentication
- Server sends server challenge
- Client formulates response from challenge by:
 - Creating the HMAC-MD5 of User name and Domain name with NT hash as the key
 - The results is called the NTLMv2 One-Way Function (OWF)
 - Then, the response is created from the HMAC-MD5 of the server's challenge, timestamp, client challenge, and other items, using the NTLMv2 OWF as the key



How Password Hash Are Stored

- There are five primary ways that the Windows operating system stores passwords to authenticate users
 - **LM Hash (Security Accounts Manager database)**
 - **NTLM Hash (Security Accounts Manager database)**
 - **Cached Credentials -**
 - **Memory (lsass.exe process)**
 - **Reversibly Encrypted (disabled by default)**

How Hashes are Obtained?

- Hashes/credentials can be dumped from the SAM by anyone who has Administrator-level privileges on a machine.
- Sniffing LM and NTLM challenge-response dialogues between client and servers
 - Requires brute forcing the captured encrypted hashes
- Dumping authenticated users' credentials stored by Windows in the memory of the lsass.exe process

Pwdump Tools

- Remotely accessible share is used to copy the code, then run it, grabbing hashes from memory of running processes and sends them back via named pipe to attacker.
- Many tools rely on DLL injection into the LSASS process
- Pwdump2 to pwdump3
 - move hashed across the network in clear text.
 - They may also crash LSASS due to Windows DEP forcing a reboot
- Pwdump3e to pwdump6
 - Added Encryption
 - Less likely to crash LSASS

Pwdump Tools

- Fgdump adds new functionality to the pwdump code set by remotely disabling AV tools
- Fgdump also integrates cachedump
 - Windows machines store information about the last 10 logon names and passwords in the Registry
 - They are encrypted with an LSA key created for each system
- Cachedump tools pull the LSA key from LSASS memory, and grab the cached NT and LANMAN credentials from the Registry
- These credentials are stored in encrypted form, salted with the username in Unicode format
- Extracted cache credentials can be cracked using a tool called John the Ripper..

Metasploit Priv Module Hashdump

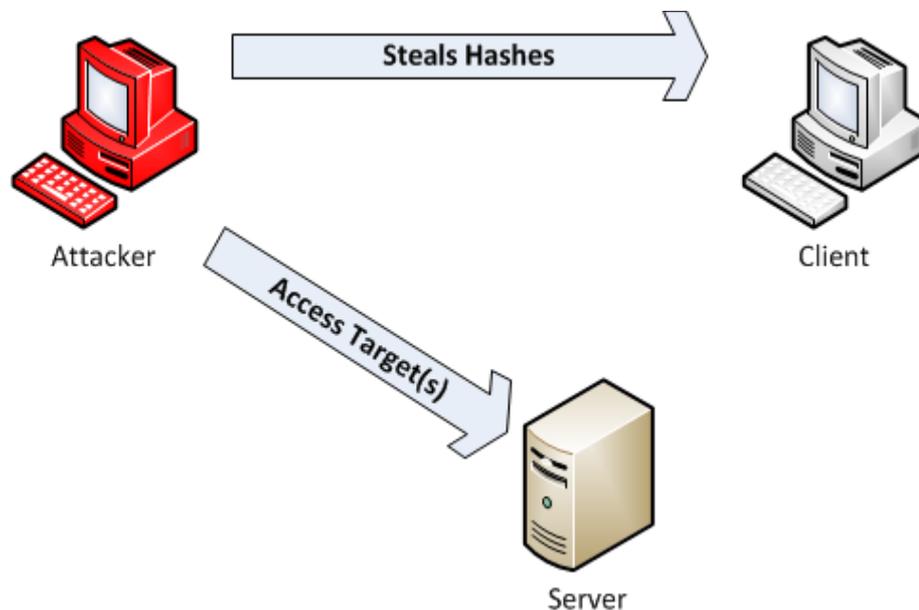
- The Metasploit Priv Module can dump hashes from a local Windows machine
- Requires the Meterpreter to run from within a admin or SYSTEM-level process
- Does not require remote NetBIOS or SMB access
- Does not copy files to the target's file system
 - Entirely memory resident, with a DLL running inside of exploited process
- Does not have issues with DEP

Sniffing Windows Challenge/Response

- The attacker could sniff the Challenge/ Response from the network
- The attacker would have to be located on the path between a victim machine and the system to which it authenticates
- Or, the attacker would use Spoofing to send responses to name queries.
- ...Or trick the user into doing challenge/response authentication with the attackers machine
 - This allows for downgrade attacks in the protocols, if the client allows for it.

Pass the Hash Technique

- Now that we have the hash.. Not need to crack
- We could then use a hash directly...
- Its time-consuming to crack passwords
- Brute Forcing may cause password lockout
- This gives access as the users priv – possibly admin??



Windows Attack Tools

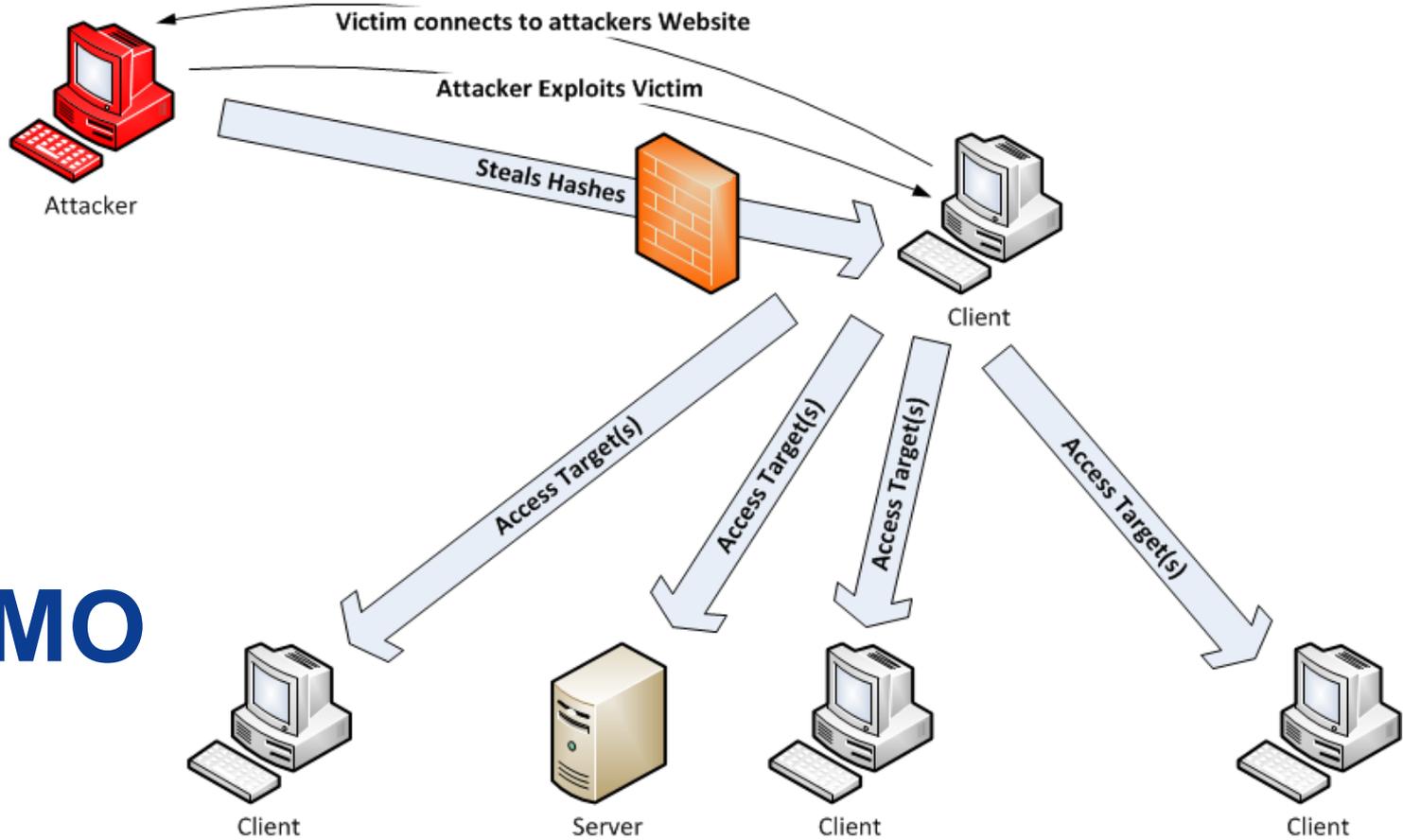
- Pass-the-Hash Toolkit (pshtoolkit) by Hernan Ochoa from Core Security
- Free at <http://pss.coresecurity.com/projects/pshtoolkit.htm>
 - **whosthere.exe**: Dumps current user session information from LSASS
 - **genhash.exe**: Generates LANMAN and NT hash
 - **iam.exe**: Changes existing hashes in memory to chosen values

Linux / Unix Attack Tools

- Modified SAMBA code from JoMo-kun of Foofus
- Uses a patches version of SAMBA code to authenticate using a environment variable SMBHASH with LANMAN:NT
- Modification allow attacker to:
 - Mount shares
 - Add Users
 - Change group membership
 - Runs a program

Metasploit's PsExec tool

- PsExec tool from Microsoft allows a user with admin credentials to make a remote Windows machines run a command via SMB connections
- Metasploit includes a psexec exploit with similar features
 - Provides UserID and password from admin group and it will run any Metasploit payload
 - Includes built-in pass the hash functionality..



DEMO

Mitigations

- Standard defense in depth practices
- Least user access (LUA) approach
- Pro-active security patching
- Prevent Windows from storing cached credentials
- Disable debug privileges for all users
- Configuring systems not to use LM or NTLM
- SMB signing to prevent some man in the middle attacks

QUESTIONS



IT Security Audit Standard SEC502-02 Changes

Michael Watson
Acting Chief Information Security Officer



IT Security Audit Standard SEC502-02 Changes

- ***Effective Date: December 5, 2011***
- ***Compliance Date: January 1, 2012***
(starting with all audits completed in FY12)
- *Note: If need be an agency can request an exception for an audit not compliant prior to compliance date.*



1.4 IT Security Audits of *IT Systems*

- Each Agency shall establish an IT Security Audit Program. The program shall include assessing the risks associated with the state *IT systems* for which it is the Data Owner and conducting IT Security Audits at a frequency relative to the risk identified by the Agency. At a minimum, *IT systems* that contain sensitive data, or reside in a system with a sensitivity of high on any of the criteria of confidentiality, integrity, or availability, shall be assessed at least once every three years. *All IT security audits must follow either the generally accepted government auditing standards GAGAS Yellow Book (**Generally Accepted Government Auditing Standards**) or the international standards for the professional practice of internal auditing IIA Red Book (Institute of Internal Auditors' Standards).*



2.1 Planning for IT Security Audits

Annually, each Agency shall develop an IT security audit plan or review and as necessary, update an existing one for the IT systems for which it is the Data Owner. The IT security audit plan shall be based on the Business Impact Analysis (BIA) and data classification performed by the Agency. Each Agency Head shall submit the Agency IT security audit plan to the CISO, annually.

The IT Security Audit plan must include the following:

- *The agency name, agency abbreviation and agency number,*
 - *The contact information of individual submitting the plan,*
 - *The system full name and abbreviation,*
 - *The planned auditor,*
 - *The date the system was last audited,*
 - *Scheduled audit completion date.*
- *Note: Scheduled audit completion date is the planned date of the completion of the future audits covering a three year period from the submission date.*
- *Agencies are required to use the [IT Security Audit Plan Template](http://www.vita.virginia.gov/uploadedFiles/Library/PSGs/Word_versions/ITSecurityAuditPlanTemplate.doc) found at: http://www.vita.virginia.gov/uploadedFiles/Library/PSGs/Word_versions/ITSecurityAuditPlanTemplate.doc.*



2.4.5 Reporting IT Security Audit Results to VITA

The Agency Head or designee shall submit to the CISO the following information:

A record of all *completed* IT Security Audits conducted by or on behalf of the Agency, including *the official audit report (in accordance with auditing standards)*, all findings, and whether the Agency concurs or does not concur with each. *IT Security Audits submitted to VITA must be reflected in the IT Security Audit Plan.*

Note: The official audit report submitted needs to include an attestation as to the audit standard used. (yellow or red book)



2.4.5 Reporting IT Security Audit Results to VITA

1. Agencies are required to use the [Corrective Action Plan Template](http://www.vita.virginia.gov/uploadedFiles/Library/CorrectiveActionPlanTemplate.doc) found at: <http://www.vita.virginia.gov/uploadedFiles/Library/CorrectiveActionPlanTemplate.doc>.
2. For each finding with which the Agency concurs:
 - a) *Audit Name;*
 - b) *Audit Finding No.;*
 - c) *Short Title;*
 - d) *Summary;*
 - e) *Agency Concurs;*
 - f) *Planned Corrective Action;*
 - g) *Responsible Person(s);*
 - h) *Status;*
 - i) *Due date (for the corrective action); and*
 - j) *Exception on File (for findings not compliant with COV Information Security Standard (SEC501)).*



2.4.5 Reporting IT Security Audit Results to VITA

3. For each finding with which the Agency does not concur:
 - a) *Audit Name;*
 - b) *Audit Finding No.;*
 - c) *Short Title;*
 - d) *Agency Does Not Concur* (Agency's statement of position); and
 - e) *Mitigating controls* (that are in place and Agency's acknowledgment of their acceptance of the risk).
4. *Any modification to a corrective action for any IT Security Audit conducted by or on behalf of the Agency must be reported.*
5. *Corrective action plans for all findings must be submitted within 30 days of issuing the final audit report. An updated corrective action plan must be submitted quarterly (at the end of the quarter), until all corrective actions are completed. All corrective action plans and quarterly updates submitted must have evidence of agency head approval.*



Summary

- Audit Plan submitted annually using standard template
- NOTE: Agency Audit Plans should be submitted to Commonwealth Security by June 1 of each year
- *Note: Agencies declaring No Sensitive Systems must do so annually as well.*
- The official audit report submitted when completed with an attestation as to the audit standard used. (yellow or red book)
- CAP submitted using standard template
- Quarterly reports using standard template

IT Security Audit Plan Template

Agency Information		Contact Information	
Agency Name	Click here to enter text.	Name	Click here to enter text.
Agency Acronym	Click here to enter text.	Title	Click here to enter text.
Agency Number	Click here to enter text.	E-mail	Click here to enter text.
Date of submission	Click here to enter a date.	Phone	Click here to enter text.

IT System Acronym *	IT System Name	Planned Auditor	Date Last Audited (MM/YY)	Scheduled Audit Completion Date (Minimum once every 3 years)			Areas for Special Emphasis and Additional Audit Requirements
				20xx (MM/YY)	20xx (MM/YY)	20xx (MM/YY)	

* If new system please indicate implementation date in the Areas for Special Emphasis and Additional Audit Requirements column.

NOTE: Agency Audit Plans should be submitted to Commonwealth Security by June 1 of each year.

Corrective Action Plan and *IT Security Audit Quarterly Summary* Template

Date _____

PURPOSE: This Plan describes IT Security Audit findings; documents responsibility for addressing the findings; and describes progress towards addressing the findings. Provide enough information to enable the reader to understand the nature of the finding, the impacts, and the planned remedy.

Audit Name: _____

IT System(s) _____

Audit Finding No.	Short Title	Summary	Agency ¹ Concur	Planned Corrective Action or Mitigating Controls ²	Responsible Person(s)	Status ³	Due Date	Exception on File ⁴

Audit Name: _____

IT System(s) _____

Audit Finding No.	Short Title	Summary	Agency Concur	Planned Corrective Action or Mitigating Controls	Responsible Person(s)	Status	Due Date	Exception on File

¹ Agency Concur: Concur or Does Not Concur

² If the Agency does not concur, the Mitigating Controls and Risk Acceptance must be stated in Planned Corrective Action.

³ Status: NS = Not Started; U = Underway; C = Completed

⁴ Exception on file for findings not compliant with COV Information Security Standard (SEC501): Y = Yes; N = No

NOTE: CAPs must be submitted within 30 days of issuing the final audit report completion. All CAPs should be combined into one cumulative summary agency CAP and submitted to Commonwealth Security quarterly within 30 days of quarter's end date to be counted.



Questions???

For more information, please contact:
CommonwealthSecurity@vita.virginia.gov



Thank You!



Upcoming Events





InfraGard – Richmond Chapter

Election Time!

Positions open:

President, Vice President

Secretary, Treasurer

Membership Chair and Program Chair

Elections will be held at February meeting. Terms are for two years commencing in May.

If interested, send a short bio of yourself by *Jan. 15* to:
Gregory.Bell@TAX.Virginia.Gov



Information Security System Association

ISSA

DATE: Wednesday, Jan 11, 2012

LOCATION: Maggiano's Little Italy

11800 West Broad Street, #2204, Richmond, VA 23233

TIME: 11:30 - 1:00pm. Presentation starts at 11:45.

Lunch served at 12.

COST: ISSA Members: \$20 & Non-Members: \$25

SPEAKER: TBD

TOPIC: TBD



COV Audit Training Offered by DOA

Auditing Wireless Security

This class will be beneficial to those who perform audit-like or IT security functions as part of their job duties. The two day course will address the fundamental security issues related to WLANs.

- When: January 24 & 25
- Time: 8:15am to 4:45pm each day
- Where: James Monroe Building
- Cost: \$320
- Register: <https://hrtraining.doa.virginia.gov/>

Earn 16 CPEs for taking this class.

Questions? Contact: Tim.Sadler@DOA.Virginia.Gov



Future ISOAG's

From 1:00 – 4:00 pm at CESC

Wednesday - February 1, 2011

Speaker: Marc Gaudette, Director, IT Risk Mgmt, Dominion

Wednesday - March 7, 2012

Speaker: Dave Marcus, McAfee on Challenges in today's environment

Upcoming:

April – Laurie Jarrett, VCU on Grant Writing

ISOAG will be held the 1st Wednesday of each month in 2012



Future IS Orientation Sessions

Tuesday - February 7, 2011

1:00 – 3:30p
(CESC)

Email CommonwealthSecurity@VITA.virginia.gov if you are interested in attending.

IS Orientation is now available via webinar!



Submit Events

- If your group or organization is promoting a security related event and would like to have it communicated to the Information Security Officer community:

Please submit all upcoming events to:

CommonwealthSecurity@VITA.Virginia.Gov



ISOAG-Partnership Update

*IT Infrastructure Partnership Team
Bob Baskette*

January 4, 2012



NORTHROP GRUMMAN



ADJOURN

