



Your New 5 Year Plan-NG!

Well.. This is lazy, it is pretty much the same webcast as last time. But, here is the deal. I was half-dead last time. Some kind of 28 Days-like plague that took out half our intern pool. Thats OK... They were weak. No, that sounds awful. The interns were (mostly) fine. I just don't remember much of it. This is my attempt to do "better."

But seriously, if you were at the last one and you expect me to do better than when I was on 1 gallon of Nyquil.. Boy, are you about to be disappointed. People love me when I am high on cold medication. Which just further confirms that people, as a whole, generally make poor life decisions. Sometimes, they come up to me and I can tell if they are sniffing for Jagermeister-like desperation on my breath. Seriously, Jagermeister is almost exactly like Nyquil. Awful. Who thought that was a good idea? Really? Then they mixed it with Redbull and Vodka. So many bad ideas rolled into one.

Nothing like this webcast. No sir! This is nothing but a good idea that will never get off track.

Ever.

Did I mention we are going to do audience participation this time?

Nope, nothing will get us off track.





My Background

- College
- Accenture
- Northrup Grumman
- SANS
- BHIS



accenture



What Kickstarted It All?



Indian Trust Settlement

[Home](#) [Important Dates](#) [FAQs](#) [Notices](#) [Court Documents](#) [Media](#)

January 27, 2017
Important Update: Final Deadline To Submit Documents Set For Payment In The Cobell Settlement And Court Approval Of Initial Scholarship Payment:

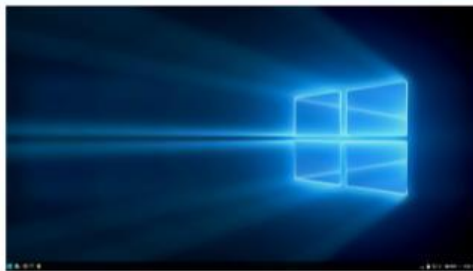
**Whereabouts Unknown:
Help Locate Your Record**



Year One



- Focus on core concepts
 - Windows
 - Linux
 - Networking
 - Python
- Also start looking at security standards
 - CIS
 - NIST 800 documents
 - Most of this is worthless
 - But, people will ask questions



CIS Benchmarks Examples:



Download Free CIS Benchmark PDFs:

Select Platform

Download



Windows TechNet Evaluation



TechNet Evaluation Center

My Evaluations

Evaluate Now ▾

Tech Journeys ▾

Explore

Try

Learn



My Evaluations



Explore

Watch on-demand: Exclusive business application insights—including Dynamics 365, LinkedIn, and Power BI—with CEO Satya Nadella



Explore

DevOps in real life. Geek out over DevOps technical case studies, complete with value stream maps, architectural diagrams, and code.



Explore

Join us for our upcoming Windows Server Security AMA in the Tech Community on August 8 at 9AM PT!



My Experiences ▾

My Actions ▾

My Profile ▾



Evaluations



Virtual Labs



Tech Journeys

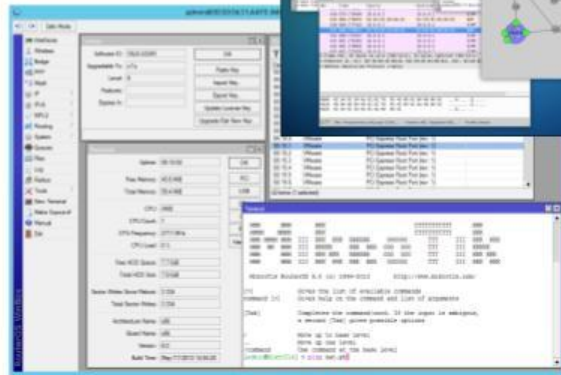
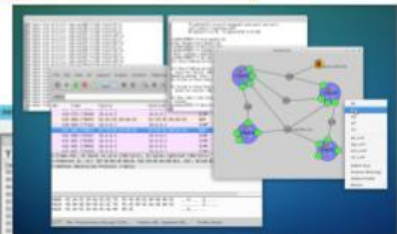
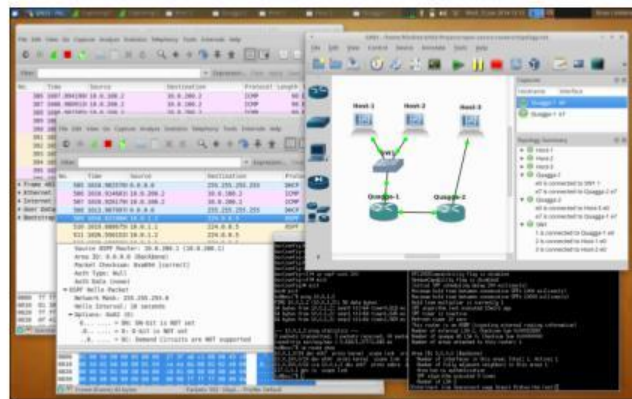


© Black

Networking



- First, get your stuff at home to work
- Know what it is doing
- Next, get some simulators
 - <http://www.brianlinkletter.com/open-source-network-simulators/>
- Finally, get some gear
 - Old Cisco on ebay
 - MikroTik is cheap and very powerful
 - Full crazy router for ~ \$60



Linux – Install Everything... From Scratch



Step 1
Visit google.com

Step 2
Type your question.

Step 3
Click the button.

That's it!



The above is an illustration for educational purposes.



© Black Hills Information Security | @BHinfoSecurity

Let's Be A bit More Specific...



- Learn bash scripting
- There are other shells
- Bash is the only one that matters
- Anyone who tells you otherwise is not someone you want to hang with in parties
- They are also not your friend



The Linux Command Line: A Complete Introduction Jan 11, 2012

by William E. Shotts Jr.

Paperback

\$29⁴³ ~~\$39.95~~ prime

Usually ships in 1 to 3 weeks

More Buying Choices

\$18.79 (39 used & new offers)

Kindle Edition

\$30⁹⁹

★★★★☆ 307

Trade in yours for an Amazon Gift Card up to \$10.72



Linux Command Line and Shell Scripting Bible Jan 6, 2015

by Richard Blum and Christine Bresnahan

Kindle Edition

\$26²⁹

Paperback

\$11⁰⁷ to rent prime

\$27⁶⁷ to buy prime

More Buying Choices

\$20.91 (62 used & new offers)

★★★★☆ 66



Shell Programming and Bash Scripting: Ultimate Beginners Guide Book Nov 10, 2016

by Robert Collins

Kindle Edition

\$0.00 kindleunlimited

Read this and over 1 million books with Kindle Unlimited.

\$2⁹⁹ to buy

★★★★☆ 3

Paperback

\$12³³ prime

Get it by **Thursday, Aug 10**

More Buying Choices



Learn Python Online



codecademy

Catalog

Log in

Sign up

Learn to code interactively, for free.



SIGN UP AND START CODING IN
SECONDS.

Email

Password

Username

SIGN UP



© Black Hills Information Security | @BHinfoSecurity

Year One.... NG



• 20 Critical Controls..



The CIS Critical Security Controls

In the last couple of years it has become obvious that in the world of information security, the offense is outperforming the defense. Even though budgets increase and management pays more attention to the risks of data loss and system penetration, data is still being lost and systems are still being penetrated. Over and over people are asking, "What can we practically do to protect our information?" The answer has come in the form of 20 information assurance controls known as the CIS Controls.

The CIS Critical Security Controls - Version 7.0:

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs



This stuff will make you an Infosec Trex.. Just like me.



© Black Hills Information Security | @BHinfoSecurity

Year Two



- Time to start projects
- It is possible you started some already
- That is fine
- You should also start the following:
 - Start a security group
 - At work
 - At school
 - Start learning PowerShell
 - This is going to take a while
- Keep up on security news



GitHub



Microsoft®
PowerShell



And... Henry Rollins...



Year Two.. NG



This guy sucks at parenting!



"At least I don't let my kids watch American Idol"

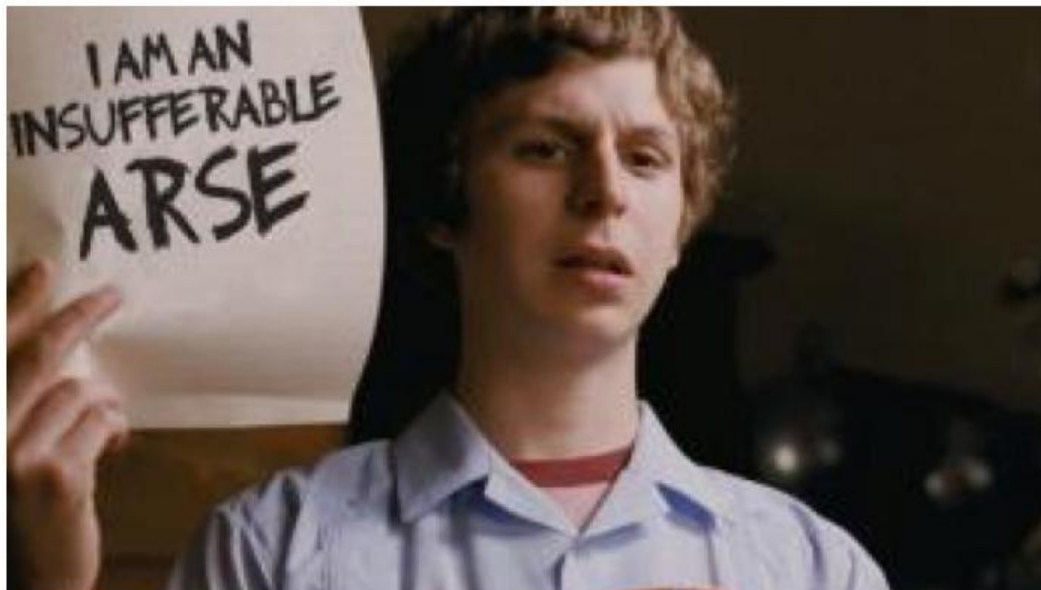


That's better...



© Black Hills Information Security | @BHinfoSecurity

I am an arse...



"So, like, I don't have a TV and it frees me from the shackles of a consumerist capitalist society."



© Black Hills Information Security | @BHinfoSecurity

But....



Holy Crap!! Dragons you guys!!

© Black Hills Information Security | @BHinfoSecurity



Year Three



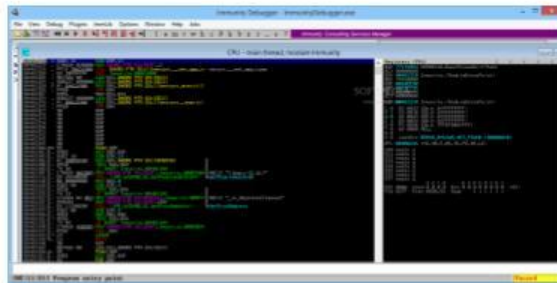
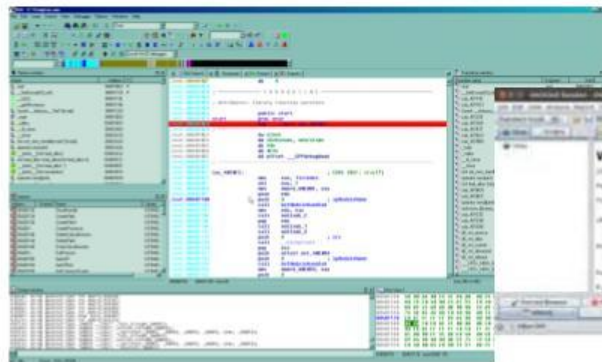
- The year of web apps
- Start with PHP and ASP.NET
 - Don't get distracted with other crap just yet
- Feel free to branch out to networked iOS and Android Apps
- But develop something
- Learn to code badly
 - Trust me.. You will suck.



Year Four



- Time to start hacking stuff
- Learn IDA and Immunity Debugger
- Pick a protocol
- Understand that protocol
- Hit online challenges
- I know you would have played with Metasploit the whole time...
- ZAP from OWASP



Y4-NG Learn all of this...



Windows ATT&CK for Enterprise Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	CMSTP	Accessibility Features	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	Application Deployment Software	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	Command-Line Interface	AppCert DLLs	Accessibility Features	BITS Jobs	Brute Force	Application Window Discovery	Distributed Component Object Model	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Control Panel Items	Applet DLLs	AppCert DLLs	Binary Padding	Credential Dumping	Browser Bookmark Discovery	Exploitation of Remote Services	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Dynamic Data Exchange	Application Shimming	Applet DLLs	Bypass User Account Control	Credentials in Files	File and Directory Discovery	Logon Scripts	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Execution through API	Authentication Package	Application Shimming	CMSTP	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Information Repositories	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Execution through Module Load	BITS Jobs	Bypass User Account Control	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Local System	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Exploitation for Client Execution	Bootkit	DLL Search Order Hijacking	Component Firmware	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Data from Network Shared Drive	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Graphical User Interface	Browser Extensions	Exploitation for Privilege Escalation	Component Object Model Hijacking	Hooking	Peripheral Device Discovery	Remote File Copy	Data from Removable Media	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	InstallUI	Change Default File Association	Extra Window Memory Injection	Control Panel Items	Input Capture	Permission Groups Discovery	Remote Services	Email Collection	Scheduled Transfer	Failback Channels
Valid Accounts	LSASS Driver	Component Firmware	File System Permissions Weakness	DCShadow	Kerberoasting	Process Discovery	Replication Through Removable Media	Input Capture		Multi-Stage Channels
	Marta	Component Object Model Hijacking	Hooking	DLL Search Order Hijacking	LLMNR/NBT-NS Poisoning	Query Registry	Shared Webroot	Man in the Browser		Multi-hop Proxy
	PowerShell	Create Account	Image File Execution Options Injection	DLL Side-Loading	Network Sniffing	Remote System Discovery	Tampered Shared Content	Screen Capture		Multiband Communication
	Regsvcs/Regasm	DLL Search Order Hijacking	New Service	Decrypt/decode/Decode Files or Information	Password Filter DLL	Security Software Discovery	Third-party Software	Video Capture		Multilayer Encryption
	Regsvr32	External Remote Services	Path Interception	Disabling Security Tools	Private Keys	System Information Discovery	Windows Admin Shares			Remote Access Tools
	Rundll32	File System Permissions Weakness	Port Monitors	Exploitation for Defense Evasion	Two-Factor Authentication Interception	System Network Configuration Discovery	Windows Remote Management			Remote File Copy
	Scheduled Task	Hidden Files and Directories	Process Injection	Extra Window Memory Injection		System Network Connections Discovery				Standard Application Layer Protocol

© Black Hills Information Security | @BHInfoSecurity



SANS Ultimate Pentest Poster



- <https://www.sans.org/security-resources/posters/pen-testing>

The collage consists of four distinct posters from SANS:

- Top Left: Future Pen Testing Events**
Announces the **SANS Pen Test Austin** (Nov 18-23, 2013) and the **Pen Test Hackfest** (Nov 24-25, 2013). It lists various sponsors and provides contact information for registration.
- Top Right: COIN-A-PALOOZA**
A circular infographic titled "COIN-A-PALOOZA" featuring various security-related icons and text about a "Coin-A-Palooza" event.
- Bottom Left: SANS Penetration Testing**
A poster titled "SANS Penetration Testing: Attack Surfaces, Tools, and Techniques" (5th Edition, Spring 2013). It includes a list of topics and a "Resources" section.
- Bottom Right: Penetration Testing Practice Labs**
A large, detailed infographic titled "Penetration Testing Practice Labs: Vulnerable Apps/Systems". It features a central hub with numerous branches leading to specific vulnerable applications and systems, categorized by type (e.g., Web, Mobile, IoT).



Year Five... Present.



© Black Hills Information Security | @BHinfoSecurity

In Closing



- Feel free to do the following....

- Indulge in distractions
- Stick to my plan
- Ignore my plan
- Develop your own plan
- Get good at just one thing
- Get a degree
- Don't get a degree
- Get certifications
- Don't get certified

- Do not do the following....

- Sink into video games
- Waste your time figuring out the cube
- Binge watch shows on Netflix
- Use Bing for anything
- Just barely learn Metasploit to impress women/men
- Spend more time on the hacker "look" than learning
- Get angry
- Blame others

