



# Getting Started With BHIS: Pentesting

John Strand



© Black Hills Information Security | @BHInfoSecurity

# What We Are Covering

- BHIS Testers and What We Do
- Lots of Lessons Over The Years
- How a Pentest Really Works
- Kill Some Confusion
- Give Pointers
- Avoid Pitfalls
- 22 Years of Experience



What?!? No 0-days?



© Black Hills Information Security | @BHInfoSecurity

# What This Class Is Not

- Detailed step-by-step tech walkthroughs
  - It is a 2 day class...
- Full breakdown of tools
  - But, there will be labs
  - There will be a lot of links...
- Pay What You Can... Sorry. It is Offensive



# Who This Class Is For



- Testers
- Owners
- Customers
- BHIS New Employees
- Internal Teams
- There is way too much here
- Guideposts



A class... For all seasons.



© Black Hills Information Security | @BHInfoSecurity

# Lab Environment: MetaCTF



- Why MetaCTF?
- HackTheBox
- TryHackMe
- Counterhack
- CTF Vrs. Certs
- Every 35-40 min



© Black Hills Information Security | @BHInfoSecurity



# Labs: You Have 350 Of Them



- May or may not have nothing to do with the topic at hand
- The primary goal is communication
- How to communicate if you have no idea?
- How to communicate if you do have an idea?
- Challenge Based
- Do not care who finishes first
- Let's try to get everyone through

#whoami

James Lee

@egyp7

Metasploit Developer

Community Manager



Legend





# Your New 5 Year Plan!

Ok, so five is just a made up number. Most people are more likely to click on articles with simple numbers in them. Think of all the Cracked and BuzzFeed articles that have easy to digest numbers in the title. This is kind of like that. Yes, I know it is a marketing ploy. And, to be honest, I feel bad about it. I just want you to know that I know it is a bit weird. Please, please do not hold this against me. If you have been coming to these things for a while, you know that I try to stay away from things like this.

Ok.. I lied. I put five in the title simply so I could write this up at the beginning of the presentation. It is kind of a meta-meta joke that I am pretty sure is only funny to myself. But that is kind of the point. The first thing you need to do is find a way to enjoy things. Yes, that will entail doing odd things that only you and possibly one other person in the whole world will get. For example, I like to tell jokes about James Joyce. No one gets them. And, the people who would, don't find them funny at all. That does not stop me. Are you still reading this? Wow.. Bet you regret it. I am starting to feel a bit bad about this joke.

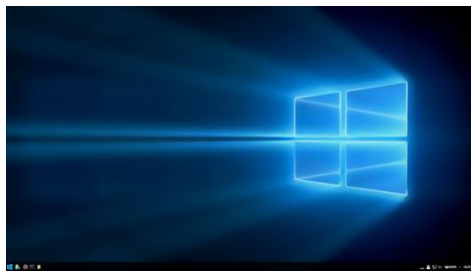




# Year One



- 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



Evaluation Center

Windows ▾

Windows Server ▾

SQL Server ▾

System Center ▾

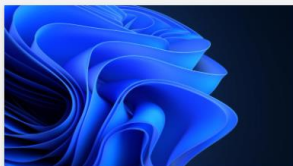
Microsoft Security ▾

Additional products ▾

All Microsoft ▾

## Start your evaluation today

From signing up for a free trial to exploring technical documentation, virtual labs, and demos, the Evaluation Center has the tools you need to evaluate Microsoft products and services.



### Windows 11 Enterprise

Windows 11 Enterprise is designed for hybrid work, offering features and enhancements focused on productivity, collaboration and security.

[Evaluate now >](#)



### Windows Server 2022

Windows Server 2022 introduces advanced multi-layer security, hybrid capabilities with Azure, and a flexible application platform.

[Evaluate now >](#)



### SQL Server 2022

SQL Server 2022 integrates with Azure Synapse Link and Azure Purview to enable customers to drive deeper insights, predictions, and governance from their data at scale.

[Learn more >](#)



### System Center 2022

System Center 2022 offers the latest innovation and security in enterprise-class datacenter management.

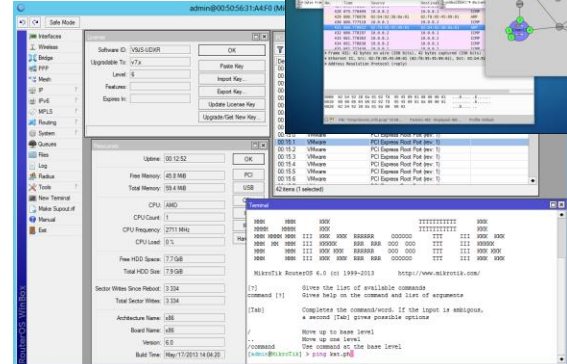
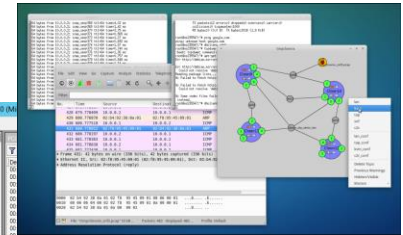
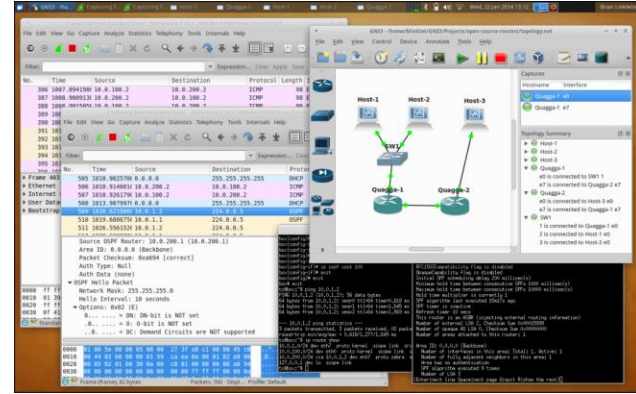
[Evaluate now >](#)



# 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

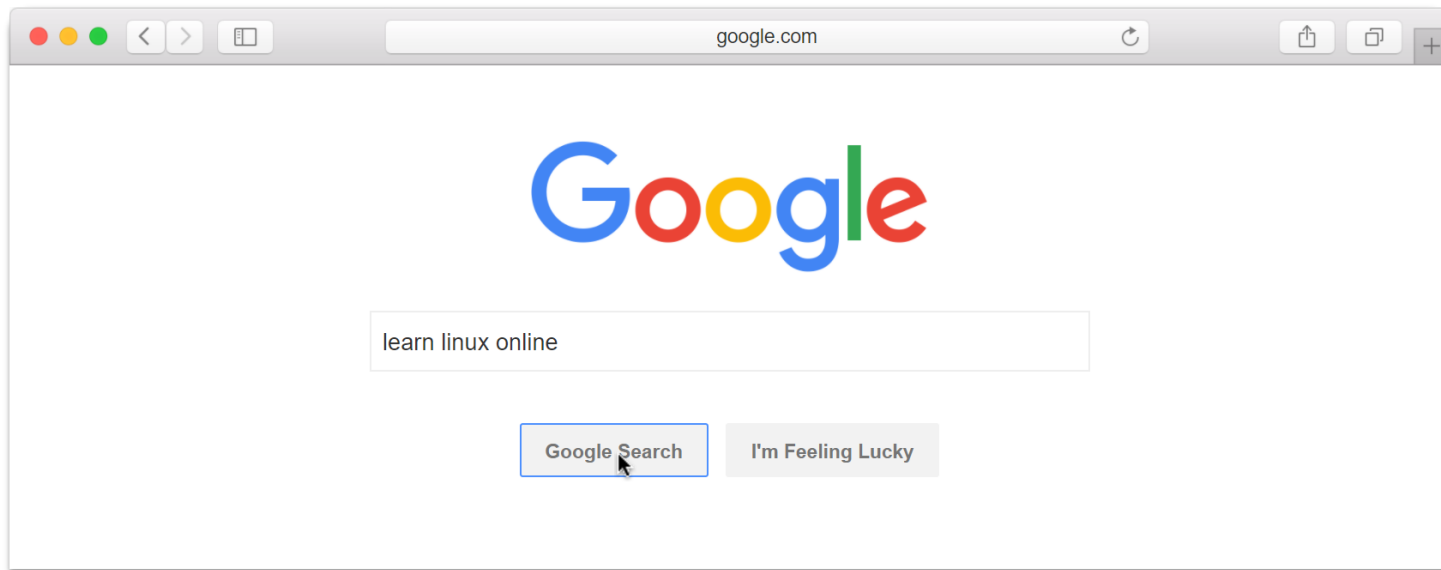


Step 1  
Visit google.com

Step 2  
Type your question.

Step 3  
Click the button.

That's it!



The above is an illustration for educational purposes.

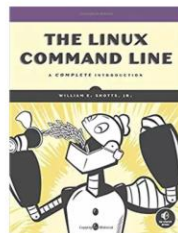


© Black Hills Information Security | @BHinfoSecurity

# 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

\$29<sup>43</sup> ~~\$39.95~~ ✓prime

Usually ships in 1 to 3 weeks

More Buying Choices

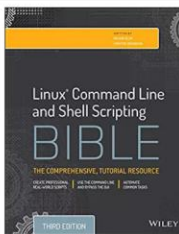
\$18.79 (39 used & new offers)

Kindle Edition

\$30<sup>99</sup>

★★★★☆ 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

\$26<sup>29</sup>

Paperback

\$11<sup>07</sup> to rent ✓prime

\$27<sup>67</sup> 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 ~~kindle unlimited~~

Read this and over 1 million books with Kindle Unlimited.

\$2<sup>99</sup> to buy

Paperback

\$12<sup>33</sup> ✓prime

Get it by Thursday, Aug 10

More Buying Choices

★★★★☆ 3



# Learn Python Online



codecademy Catalog Resources ▾ Community ▾ Pricing ▾ Business Solutions

Log In Sign Up

Languages ^

- HTML & CSS
- Python
- JavaScript
- Java
- SQL
- Bash/Shell
- Ruby
- C++
- R
- C#
- PHP
- Go
- Swift
- Kotlin
- C

Subjects ^

- Web Development
- Data Science

Not sure where to begin? [Take our quiz →](#)

### Most popular

Explore All  
**Python**

**PRO** Career Path  
**Front-End Engineer**  
● Beginner friendly, 129 Lessons

Course  
**Learn JavaScript**  
● Beginner friendly, 11 Lessons

Language Fluency

Course  
**Learn HTML**  
● Beginner friendly, 6 Lessons

Language Fluency

Explore All  
**Web Development**

**PRO** Course  
**Learn Python 3**  
● Beginner friendly, 14 Lessons

Language Fluency

Explore All  
**Data Science**

**PRO** Career Path  
**Data Scientist: Machine Learning Specialist**  
● Beginner friendly, 78 Lessons



# 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

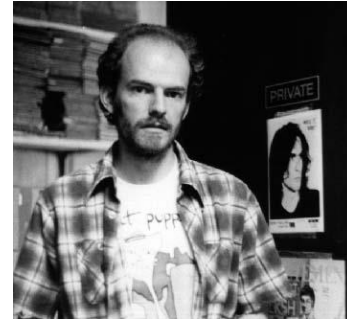


# GitHub

**Microsoft®**  
**PowerShell**



# And... Henry Rollins...





# Year Three



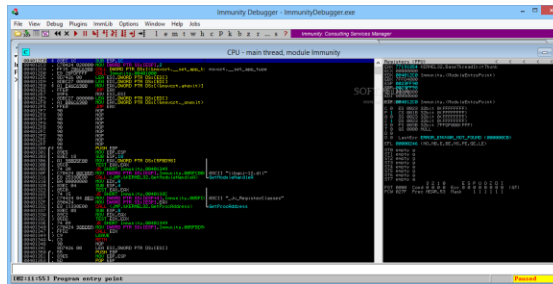
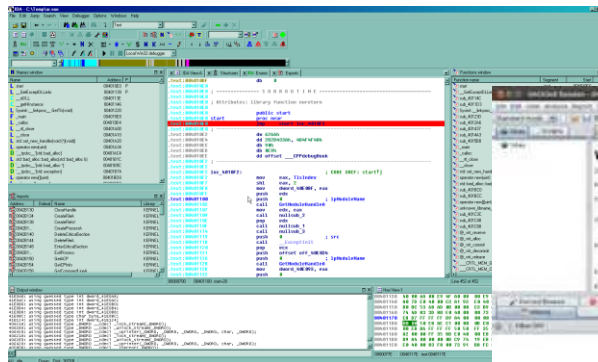
- The year of web apps
- Start with PHP and ASP.NET
  - Don't get distracted with other crap just yet
- Feel free to branch out to networked iOS and Android Apps
- But develop something
- Learn to code badly
  - Trust me.. You will suck.



# 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



# Five Years



- 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 going after epic Pokémon
  - Binge watch shows on Netflix
  - Use Bing for anything...
  - Just barely learn Metasploit to impress women/men/pets
  - Spend more time on the hacker "look" than learning
  - Get angry
  - Blame others



# Come Play With Us!



- Most of these things are what good firms do



© Black Hills Information Security | @BHInfoSecurity

# Reporting

- Always Screenshot
- Never just copy text
  - Both is better
- Screenshot tool configurations
- Methodology is key – Tell a story
- **NEVER, EVER, F\*INGK COPY AND PASTE FROM ANOTHER REPORT!!!!**

## Penetration Testers Code of Ethics

- I will never copy and paste automated results
- I will never completely trust scan results
- I will strive to get caught (after being awesome)
- I will go beyond the scan results
- I will be a hacker in the original sense of the word
- I will always stay in scope
- My reports will rock



# BB Does it Better

← ↻ 🔒 [https://www.youtube.com/watch?v=c\\_LBWqNDY0M](https://www.youtube.com/watch?v=c_LBWqNDY0M)

☰ YouTube 🔍 🎤


## WILD WEST HACKIN' FEST 2018


**BBKing**



Brian B. King @BBhackKing  
Tester with Black Hills Infosec

Infosec.

Artist.

 © Black Hills Information Security | @BHInfoSecurity





▶ ⏮ 🔊 0:19 / 51:36 ⏸ ⌂ ⚙ 📺 🖥 🗖

© Black Hills Information Security | @BHInfoSecurity



# More Mr. The King



← ↻ 🔒 <https://www.youtube.com/watch?v=bJ4gJVXPAS0>

☰ YouTube 🔍 🔊

Search

Hack for Show  
Report for Dough  
Part II

You do want to get paid for this, right?

▶ ⏮ ⏭ 🔊 19:37 / 1:59:14 • PreShow Banter > ⏸ ⌂ ⌵ ⌶



© Black Hills Information Security | @BHInfoSecurity



# No Red Ink



**noredink** Curriculum Premium Careers About ▾ Help & Info

## Assignment Library

Search all content 🔍

Choose an activity, or browse by your standards.

### Practice

Targeted exercises to help students master writing and grammar skills

### Writing

Scaffolded writing and revising activities for a range of genres and purposes

### Assessment

Diagnostics and quizzes to assess your students' skills

### Standards & Tests

Activities that align to your standards and standardized tests

**noredink**

Product

- Premium
- Case Studies
- Curriculum

About Us

- Our Values
- Team
- Careers
- Press
- Tech Blog

Help

- Help Center
- Resources
- Contact

Site Usage


- Privacy Policy
- California Privacy Notice
- Terms of Service
- Accessibility

Copyright 2022 © NoRedInk Corp.

© Black Hills Information Security | @BHInfoSecurity

# Reporting: Frameworks



[Platform](#)[Solutions](#)[Resources](#)[Company](#)[Pricing](#)[BOOK A DEMO](#)

## Improving efficiency and effectiveness

ROI reported from PlexTrac users

**5X**  
ROI in one  
Year


**30%**  
increase in  
efficiency

**65%**  
shorter  
reporting cycle

**20%**  
time saved on  
engagements

[LEARN MORE](#)


## Providing solutions for



### Red Teams

Streamline all steps of the pentest and assessment reporting process and export to your custom template with a click or give stakeholders direct access with the client portal feature.


[LEARN MORE](#)



### Blue Teams

Aggregate security findings from all sources so you can analyze, prioritize, assign, and track remediation all in one interface – gaining a real-time view of security posture.


[LEARN MORE](#)



### Purple Teams

Plan, execute, collaborate, and report on adversarial emulation activities using procedures or supported test plans and frameworks like MITRE Engenuity, SCYTHE or BlindSPOT.

[LEARN MORE](#)



### Security Leaders

Be more proactive and strategic and demonstrate progress over time, while also improving team efficiency and effectiveness across all workflows in the cybersecurity lifecycle.

[LEARN MORE](#)

© Black Hills

# Debrief Meeting



- Multiple Audiences
- Plan upfront in pricing
- Why the BHIS Methodology kicks ass
- Start with the Exe summary and work through
- Open Ended
  - "Please feel free to contact us with any questions anytime"



# Worst Customer Experiences



- We will be sharing.... A Lot of stories.....
- I have been burned a lot
- 15+ years... Thousands of tests
- Possibly, 5 really bad things have happened...
- Dozens of little annoyances
- Thousands of things that make me smile



Kelly Clarkson told me  
"What doesn't kill you  
makes you stronger!"



© Black Hills Information Security | @BHInfoSecurity

# Why Do We Test?

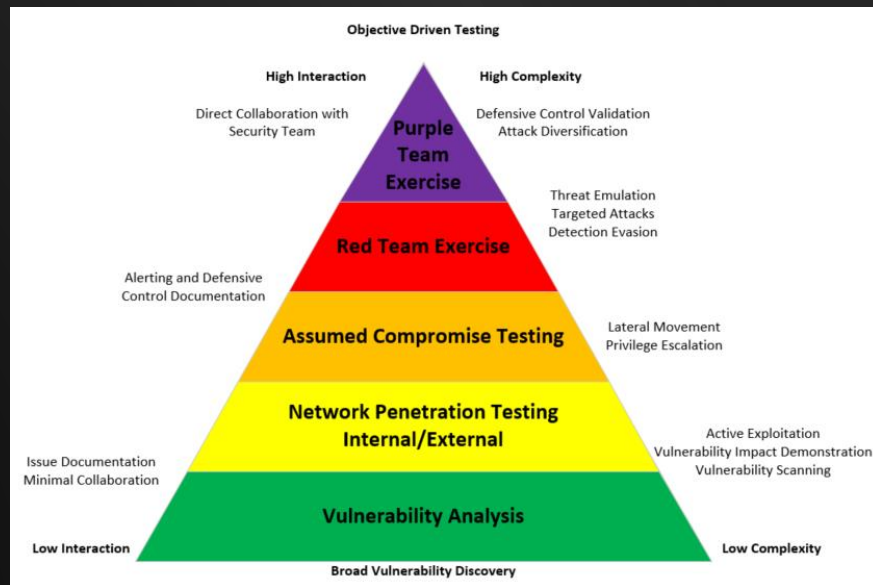
- Compliance
- To Get Better... Yea... Right.
- A note on architecture



# Types of Tests



- Sometimes the customer does not know what they want
  - Sometimes...
- It is key to find out with they really what/need
- Saves time down the line
- Communication is key <- You will hear this a lot



# Vulnerability Scans



- Usually just a scan
- There is value in this
- Do not rip on it
- Think of steps
  - Do not Jump to a Red Team
- Scanning and some validation
- **\*\*NO EXPLOITATION\*\***
- This is not stealthy!!!!
- Low isn't always a low
  - High isn't always a High





# Pentest



- Just one step up from a scan
- Exploitation is on the table
- The goal is not just vulnerabilities
- The goal is identifying risk
- ***This is still not stealthy!!!!***



Dental hygiene.  
All the time.  
Every time.



# External/Internal Objectives/Targets



- Provide a profile of the organization and threat modeling available to potential attackers
- Identify systems and key assets exposed to attackers
- Enumeration of vulnerabilities present on systems
- **Learn to love your target**



Knowing you have a problem is a good first step



# External/Internal Objectives/Targets 2



- Provide recommendations for protecting key company assets
- Identify areas where sensitive information is exposed
- *Provide evidence of the effectiveness of current defensive mechanisms and attack detection methodologies!*



# External/Internal Objectives/Targets 3



- Provide an in-depth understanding of discovered vulnerabilities and repercussions, via exploit attempts, where applicable
- Provide recommendations for remediation of the identified practices and/or exposures based on the above testing



**ADULTING**

OVERRATED. OVERPRICED.  
WOULD NOT RECOMMEND.



# External Network Pen Test



- Reconnaissance
  - Open Source
  - Goal is to identify what might be useful
- Vulnerability Scanning
  - Against in scope hosts/IPs only
  - ID Potential Vulnerabilities
  - Identified Conditions are Validated
  - Exploitation attempted
  - Post scan



# External Network Pen Test 2



- Content Discovery
  - Dictionary based
  - Against Web Service discovered during scanning
- Password Spraying
  - Against login portals
  - Lockout!
    - Frequency approved by customer
    - And fellow testers on engagement
- Social Engineering involved?
  - Not likely
- ***Does NOT include authenticated Web App Testing***



"Yep... Someone did a web test without checking..."

