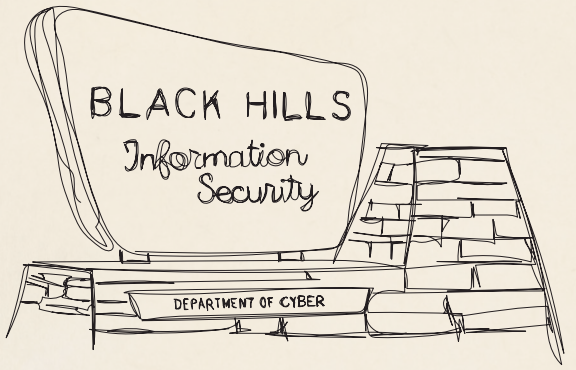
BLACK HILLS
INFORMATION SECURITY

THE INFOSEC SURVIVAL GUIDE

GREEN BOOK

Table of Contents



Brought to you by:

BLACK HILLS | Information Security

ANTISYPHON TRAINING — antisyphontraining.com

wildwesthackinfest.com

activecountermeasures.com

rekcahcomics.com

PROMPT# — promptzine.com

bhis.co

CREDITS

Made by and for the community!

and our team at BHIS

Writers

Kevin Klingbile
Kip Boyle
Graham Helton
Dieter Smith ------ @smithereens
Wade Wells ------ @WadingThruLogs
Blake Regan ------ @zer0cool
Matthew Thomas ------ @slegna
Alan Watson ------ @SenorWatsonSan
Leonardo Núñez ------ @LeonVQZ
Sean Reilly ------ @lokihakanin
John Hammond ------ @_JohnHammond
Serena DiPenti ------ @shenetworks
Glen Sorenson ------ @glen4108
Ashley Knowles ------ @jrpentester
Andrew Heishman ------ @WumpusTheBrave

Technical Editors

Kaitlyn Wimberley
Executive Head Co-Assistant Junior Pentester

Ashley Knowles
Junior Assistant Chief Senior Pentest Intern

Tim Fowler
Head Assistant Co-Executive Junior Pentester

Alyssa Snow
Chief Assistant to the Junior Pentest Executives

Dale Hobbs
Senior II Executive Head Assistant Junior Pentester

Brian King
Just Really Tall

I think they're trying to be funny?
they're all just pentesters.

PROMPT# Crew

idk who this is — John Strand ------ Did Not Stop Us
Deb Wigley ------ Found Problems *(copy editor, and some other stuff)*
wants to be called "excitement co-creator" which we have taken to HR — Jason Blanchard ------Kinda Looked At It
Kassie Kimball ------ Found Even More Problems *(editor)*
Caitlin Cash ------ Created Problems *(curator and professional doodler)*
Shelby Perry ------ Helped Solve Some Problems *(production coordinator)*
Dani Diem ------ Saved The Day *(graphic designer and hero on the side)*
Zach Hill ------ Professional Employee *(antisyphon ambassador)*

Look for all of us at cons and meetups!

How and Why This Book Was Made

Our last guide, **The Infosec Survival Guide: Yellow Book**, was an *experiment.* We had hoped to collaborate with you, to create something helpful for everyone in the community and beyond. And you did. With your help, we created a guide that covered more than twenty different topics to help readers as fresh as high school or as advanced as a C-O executive. Since our first printing, we've sent out over 20,000 copies to schools, companies, conferences, and one *very confused* kindergarten class (that was a hilarious misunderstanding).

You helped all those readers learn more about how to succeed in infosec (or if they even want to), decide what career path is right for them, land jobs, gain insight into their teammates' specialties, and protect themselves from all sorts of security threats (including one Twitch streamer who wanted to make sure The Great Robux Scandal of 2024 wouldn't happen again). By working together, the team behind **The Infosec Survival Guide: Yellow Book** accomplished amazing things. None of which could have been achieved without *you.*

With big wins like that, it's hard to walk away... but it's even harder to capture lightning in a bottle another time, right? Well, we tried anyway! Once again, we reached out to our community leaders on Discord and asked for people to claim the articles included in this guide. We gave them a style guide, a bit of a prompt, and... realized the topics this time were a bit more challenging. On top of that, this year just seemed pretty chaotic for everyone: job changes, hospital visits, you name it, we went through it. Despite all the twists and turns, **we maintained our belief that together we could create another helpful resource.** We share this insight in hopes that you, the reader, can carry that belief and hope in your own journey - **no matter how tough things get, you can still achieve your dreams.**

Just as before, this book is missing many topics that are important and vital to many in this community. We see you, we hear you, and we want your help to include your specialty. If you'd like to write your own article, or just submit some helpful nuggets, we may feature it in future REKCAH publications. Check out page 37 for details and submit your article to **info@promptzine.com**. We're excited to see what you write! Until then, we hope you find some nugget in this version that helps.

Thank you for sticking with us. Thank you for choosing to help others. Thank you for allowing us to build cool stuff like this. We couldn't do this without you.

PROMPT#

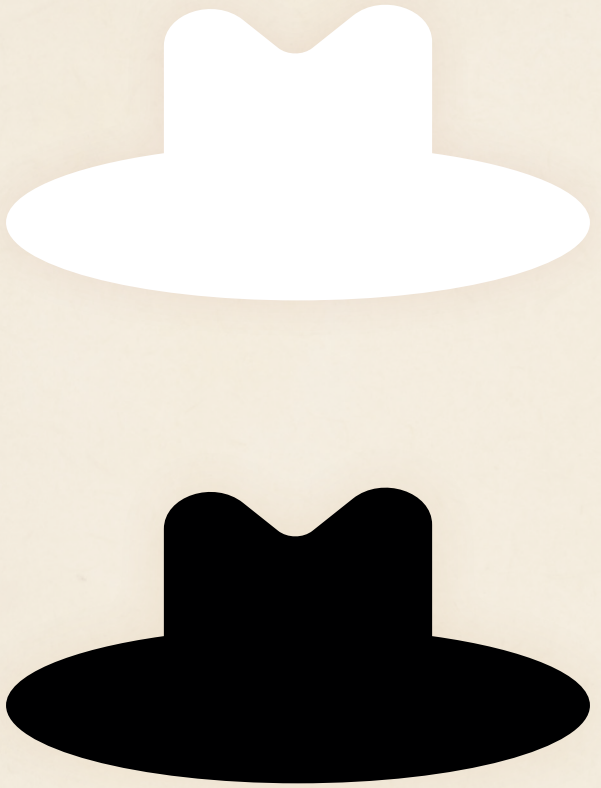
CHOOSE WISELY

Knowledge is power...

The world of information security is all about controlling access to information. The smallest things can have the biggest consequences... like your kid's name and that text you just sent saying you'll be late to pick them up from school. As you dive into the world of infosec, you'll learn all the tools, techniques, and tricks that both sides use to control and secure information. It will be solely up to you what you choose to do with those skills and the information you'll access.

...and with great power comes great responsibility.

We can't make you choose any specific route, but we can explain why we choose the white hats. Firstly, we don't like prison. It's not a fun place, and they don't let you leave. But more importantly, we love helping others, even if it doesn't make us rich. We proudly suck at capitalism, and just want to make the world a better place. We hope you do, too.



CHOOSE WISELY

COMMON CYBER THREATS

Threats That Are Common to Cyber Things

written by Dieter Smith, Wade Wells, Blake Regan, Matthew Thomas

In today's interconnected digital world, information security has become a critical concern for individuals, businesses, and governments alike. Cyber threats, which encompass a wide range of malicious activities targeting information systems, pose significant risks to the confidentiality, integrity, and availability of data. Understanding these threats is essential for developing effective strategies to protect sensitive information and maintain cybersecurity.

Malware

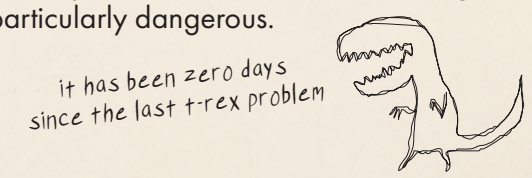
Malware, or **mal**icious soft**ware**, is a broad category of cyber threats that includes **viruses, worms, Trojans, ransomware, spyware, and adware.** These programs are designed to infiltrate, damage, or gain unauthorized access to computer systems.

- **Viruses** attach themselves to legitimate programs and spread when these programs are executed. They can corrupt or delete data, slow down system performance, and disrupt operations.
- **Worms** are self-replicating programs that spread without user intervention, often exploiting vulnerabilities in network protocols.
- **Trojans** disguise themselves as benign software but carry malicious payloads, such as creating backdoors for remote access.
- **Ransomware** encrypts a victim's data and demands a ransom for the decryption key, causing financial and operational disruptions.
- **Spyware** secretly monitors user activity, collecting sensitive information like login credentials and financial data.
- **Adware** displays unwanted advertisements and can track user behavior for marketing purposes.

gotta turn off those cookie preferences

Zero-Day Exploits

A **zero-day exploit** targets a vulnerability in software or hardware that is unknown to the vendor and has not yet been patched. Attackers exploit these vulnerabilities before developers can release a fix, making them particularly dangerous.



Insider Threats

SPIES!!! or just disgruntled employees

Insider threats involve malicious or negligent actions by individuals within an organization, such as employees, contractors, or partners. These threats can result from intentional misconduct, such as data theft or sabotage, or unintentional actions, like falling for phishing scams or accidentally mishandling sensitive information.

Advanced Persistent Threats (APTs)

APTs are sophisticated, long-term cyber attacks often orchestrated by well-funded and skilled threat actors, including nation-states. These attacks aim to infiltrate and maintain access to networks to steal sensitive information or disrupt operations.

Social Engineering

Social engineering manipulates individuals into revealing confidential information or performing actions that compromise security. It exploits human psychology through tactics like impersonation and urgency. Social engineering targets trust and fear, emphasizing the need for awareness and education to counteract these deceptive strategies.

Phishing Attacks

Phishing is a social engineering attack where attackers deceive individuals into revealing sensitive information, such as usernames, passwords, and credit card numbers. This is typically done through fraudulent emails, messages, or websites that appear legitimate.

- **Spear Phishing** targets specific individuals or organizations by personalizing the deceptive communication, increasing the likelihood of success.
- **Whaling** is a form of spear phishing aimed at high-profile targets like executives or wealthy individuals.
- **Vishing** is voice solicitation where attackers mask their phone number to pose as a legitimate service to compromise credentials, credit card numbers, and identity information.
- **Smishing** is performed by sending fraudulent text messages (SMS) to trick recipients into providing personal information or clicking on malicious links.

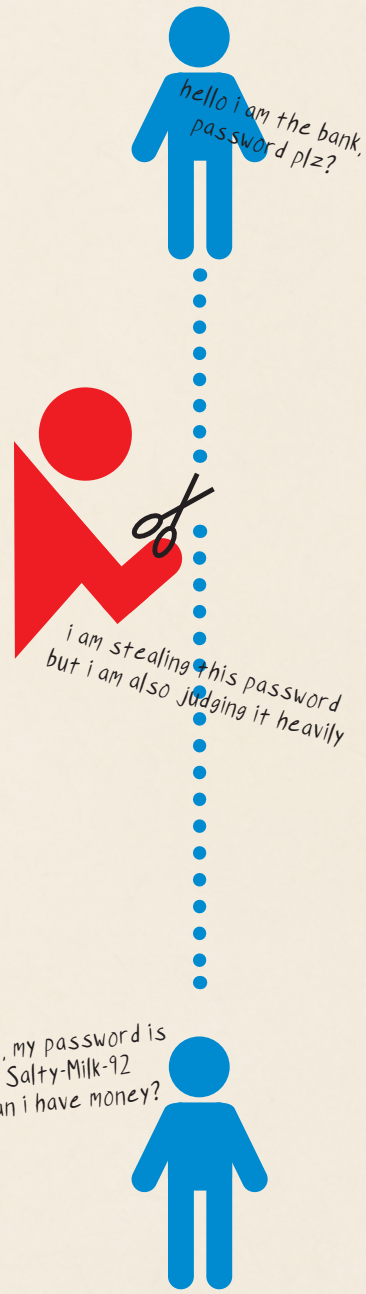
Denial of Service (DoS) & Distributed Denial of Service (DDoS) Attacks

this is what happened in Mr. Robot! among many other things....

DoS and DDoS attacks aim to make a service unavailable by overwhelming it with a flood of illegitimate requests that degrade the service. While a DoS attack originates from a single source, a DDoS attack uses multiple compromised devices to amplify the impact. These attacks can cause significant downtime, financial losses, and reputational damage.

Man-in-the-Middle (MitM) Attacks

Also known as **Machine-in-the-Middle** — In this attack, the attacker intercepts and potentially alters the communication between two parties without their knowledge. This can occur in various scenarios, such as unsecured Wi-Fi networks, compromised routers, or vulnerable communication protocols. MitM attacks can lead to data theft, unauthorized transactions, and the compromise of sensitive information.



Web-Based Threats

Web-based threats can vary in complexity and involve a user's interaction with a compromised website or service.

- **Cross-Site Scripting (XSS)** involves injecting malicious scripts into web pages to steal data or hijack sessions.
- **Drive-By Downloads** automatically install malware on users' devices through compromised websites or links.
- **Browser Hijacking** alters browser settings to redirect users to malicious sites or display unwanted content, often for ad revenue or phishing purposes.

SQL Injection

SQL injection is a code injection technique in which attackers insert malicious SQL queries into the input fields of a web application. If the client-side input is not validated, it may be possible to manipulate the database, gain unauthorized access to data, modify or delete records, and potentially take control of the server.

HOW TO SET SMART GOALS

That Actually Work For You

written by Graham Helton || grahamhelton.com/blog

Setting goals is a deceptively simple career skill we all know is important, but how do you set goals you're actually excited to work towards?

First Step

Identify what you're trying to set out to achieve. Is it landing a job? Learning a programming language? Learning how to exit vim? The traditional litmus test for if a goal is high quality is to identify if it is **S.M.A.R.T: Specific, Measurable, Achievable, Relevant, and Time-Bound.** This is a good starting place... but remember to tailor it to your circumstances! For example, I almost never make my goals "time-bound" because I generally have zero clue how long something new will take and I don't want to rush (or limit) my learning. It simply doesn't work for me, and that's ok. Where SMART goals can help is when trying to work towards an ambiguous goal such as "learning to code," which is probably too broad of a goal. When you sit down to work on it, where do you even begin?

i am very slow but i will get there

and i will leave my slime trail the whole way

I want to:	so my SMART goal is:
Learn to code	- Finish 3 tools using Python
Become a penetration tester	- Spend 1 hour a day learning skills that are listed on job postings for a penetration tester

Break It Down

Now that you've defined your main goal, break it down into smaller sub-goals that you can easily accomplish. If you have to do multiple things to accomplish a sub-goal, you probably need to break it down further.

My SMART goal is:	so the sub-goals are:
- Finish 3 tools using Python	- Find a resource for learning Python - Work through 1 chapter per day of *Automate the Boring Stuff with Python* by Al Sweigart - Write a tool that automates a simple task you do frequently (x3)
- Spend 1 hour a day learning skills that are listed on job postings for a penetration tester	- Find 10 job postings for penetration testers - Make a list of each skill or technology they want experience in - Find learning resources for each skill or technology - Spend 1 hour per day going through the learning resources

Helpful Tips

Now, for the fun part — working towards your goals. This is where 99% of the work comes in.

Can't find the time (or energy) to work towards your goal?

Work on them early in the day if you can. The later in the day you start working on your goals, the more likely you are to be too consumed by other important daily life tasks which makes it easy to say, "Oh, I'll get to it tomorrow." You're (probably) a human, though; some days you'll just want to watch Netflix, don't be too hard on yourself.

Keep a scratch pad.

If you're easily distracted like I am, try keeping a notebook next to you in which you can write down any random thoughts that come to your mind.

The second I attempt to start working towards my goals, my brain likes to flood me with reminders of other things I could be doing. Simply writing down those thoughts on a scratchpad allows me to get that thought out of my brain so that it doesn't keep resurfacing while I'm trying to focus.

and doodle in the margins of your books.

Find your own rhythm.

If you're having a blast working towards something, keep going! Goals should be the minimum target, not the maximum.

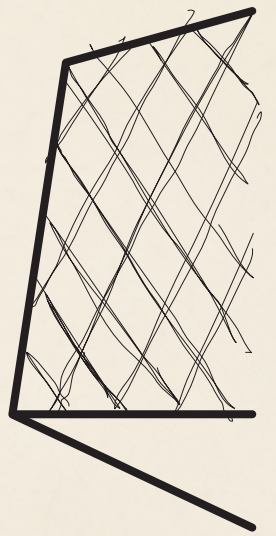
Having a blast studying a topic on your journey to become a penetration tester... but find yourself down a rabbit hole suddenly learning a different (cool) pentesting technique? As long as it's at least somewhat related to your end goal, keep going! You learn the best when you are having fun.

remember not to overdo it, either. my piano teacher would cut me off so it stayed fun and i would want to keep coming back for more.

Tell the world!

One of the best ways to keep things fun is to find people working on the same goals as you. The security community is vast and full of people working towards similar destinations. Connect and share your experiences; not only will it help others, but it will also help you stay accountable!

i actually kicked it this time!!



USE YOUR HOME LAB

What to Do with Your First Home Lab

written by Alan Watson || @SenorWatsonSan || senorwatsonsan.com

This article is a follow-up companion to the "Build a Home Lab" article from the Yellow Book. You can read that article here: https://www.blackhillsinfosec.com/build-a-home-lab-equipment-tools-and-tips/

Having assembled fundamental lab components, you now get to play! However, the ocean of potential projects can be intimidating. Where does one even start?

Make It Work!

The vulnerabilities infosec revolves around arise as unanticipated side effects of people just trying to get emails to send, documents to print, and cat pictures to load. Begin by making things work, because featuresets, functionality, misconfigurations, and misguided defaults ARE attack surfaces. So try building a miniature office network, and come to know these attack surfaces!

- **Build it**
- **Attack it**
- **Teach it**
- **Repeat!**

Teach and Learn

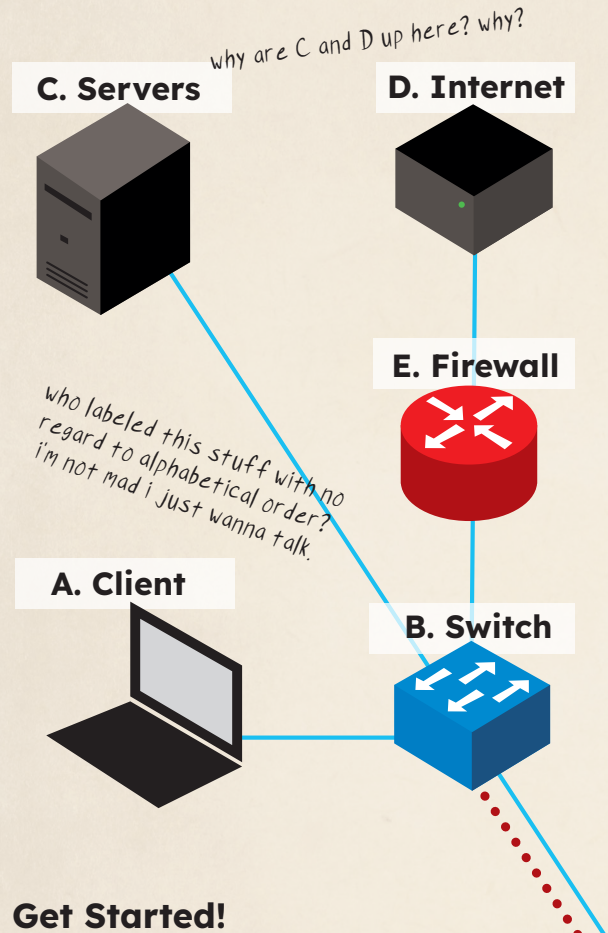
The act of explaining a thing (i.e. trying to teach it) is a powerful lifehack for helping you — yourself — absorb the thing. Look up "rubber duck programming." Maybe write a blog; Maybe create a YouTube channel; Maybe you just keep a private journal explaining to future-you what you did. Grok it!

make sure to smash that like button, and thanks again to today's sponsor, quackland's best. remember to use code GOBLIN24 at checkout for 24 free rubber ducks

Understanding how something *works* also means understanding how it can *break*.

Keep learning new things! Make LEDs go from happy-green to angry-red! **Progress is perfection. You'll never know it all, and that's ok.** If we were capable of knowing it all, there would be no need for conventions, collaboration, and shared shenanigans. Given the choice, I choose the latter.

i, however, will never be found in the corporeal form. you'll have to use your imagination as to what my beautiful goblin suit looks like IRL.



Your Mini Office*

A. Client	A laptop running virtual "user" workstations.
B. Switch	Mirroring network traffic to your Attack/Observation machine.
C. Servers	Virtual Windows Active Directory and a Linux server.
D. "Internet" Server	Something to represent a host on the internet (like a Raspberry Pi).
E. Firewall	Many options. pfSense is cheap. Great docs. Lots of features.
F. Attack & Observe	You, with two ethernet connections; the built-in port and a USB-to-ethernet adaptor (to listen to mirrored traffic). This is your battle station. Full Kali is fine, or maybe a Windows base + Kali in VMWare.

Get Started!

- Ping from (A) to (D).
- Ping from (D) to (A).
- Give (D) an FQDN and set up a DNS Server on the firewall (or maybe use Windows Active Directory).
- DHCP (go beyond basic DHCP and check out DHCP option 66 and 6).
- Set up Windows Active Directory on (C) and join (A) to it (note that this is a fantastic opportunity to create ridiculous usernames for your "users").
- Install Sysmon on your Windows machines and take a look at the logs.
- Webservers! Create one on your Linux server and IIS on your Windows server (both on (C)).
- Activate RDP on a Windows machine and try a password spray attack on it (then run DeepBlueCLI on that PC's .evtx logs and see how it can be detected).
- Use Responder from (F) to execute an LLMNR attack against (A).
- Use Wireshark to take PCAPs of interesting interactions and review them (both attacks and normal traffic).
- Follow the hardening procedures for different machines outlined by CIS (https://www.cisecurity.org/cis-benchmarks).

**For now, leave this environment disconnected from the internet and keep things as controlled as possible (with the exception of Wifi on your attack laptop so you can look things up and download things).*

OSINT

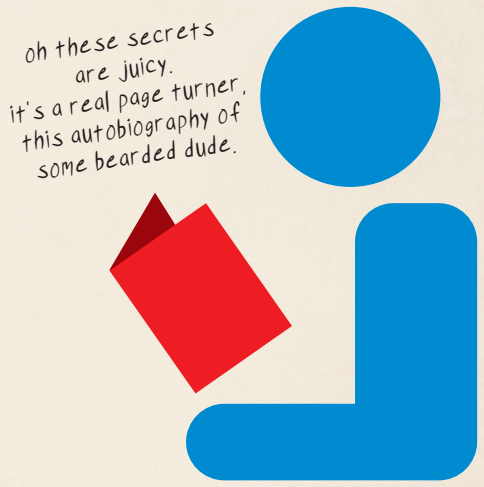
How to Find, Use, and Control Open-Source Intelligence

written by Leonardo Núñez || @LeonVQZ || whoami.leonvqz.com

Due to the wide-spread availability of OSINT, the information allowed to become OSINT should be handled with great care.

What Is OSINT?

OSINT stands for **open-source intelligence,** and it refers to all publicly available information on the open internet which has been obtained without any special requirements (paywalls, invitations, etc.). Information found on social media, in books, public reports, news articles, and press releases are good examples.



Best OSINT Practices

Keep it Legal: Ensure that all the activities performed comply with relevant data privacy and protection laws.

Stay Ethical: Ensure to respect the individuals' privacy rights.

Think about Risk: Conduct a risk assessment before undertaking investigations to identify potential legal, ethical, and operational risks.

Information Protection: Implement robust information security measures to protect collected data from unauthorized access or disclosure.

Transparency: Document methodology, sources, and findings to ensure reproducibility of your process on how to find the information.

Learn more about OSINT

Next Level OSINT
with Mishaal Khan
Available Live

16-hour Antisyphon course
antisyphontraining.com/course/next-level-osint-with-mishaal-khan/

What Are Some Tools?

Search Engines: One of the most basic and useful tools, search engines index almost everything possible.

Social Media Platforms: Contain vast amounts of user-generated content.

Metadata Analysis Tools: Tools like ExifTool allow you to look at the metadata embedded in files.

TraceLabs' OSINT VM: A virtual machine with numerous pre-installed tools useful for OSINT, but the main benefit is a separate system you can delete once you're done with the investigation.
tracelabs.org/initiatives/osint-vm

The OSINT Framework: Framework containing a comprehensive mind map of tools needed to discover different types of information such as usernames, email addresses, public records, and more. *osintframework.com*

Tips & Tricks to Perform Effective OSINT

Define Goals: Clearly define your objectives and the type of information you seek before starting, that way you won't stray off from the information you're seeking.

Use Multiple Sources: Finding information from multiple sources to verify its accuracy and reliability will keep it truthful.

Be Creative: Employ creative search strategies and utilize lesser-known sources to uncover hidden information. Exploring seemingly unrelated sources or using unconventional methods might be the key to finding that missing piece of information.

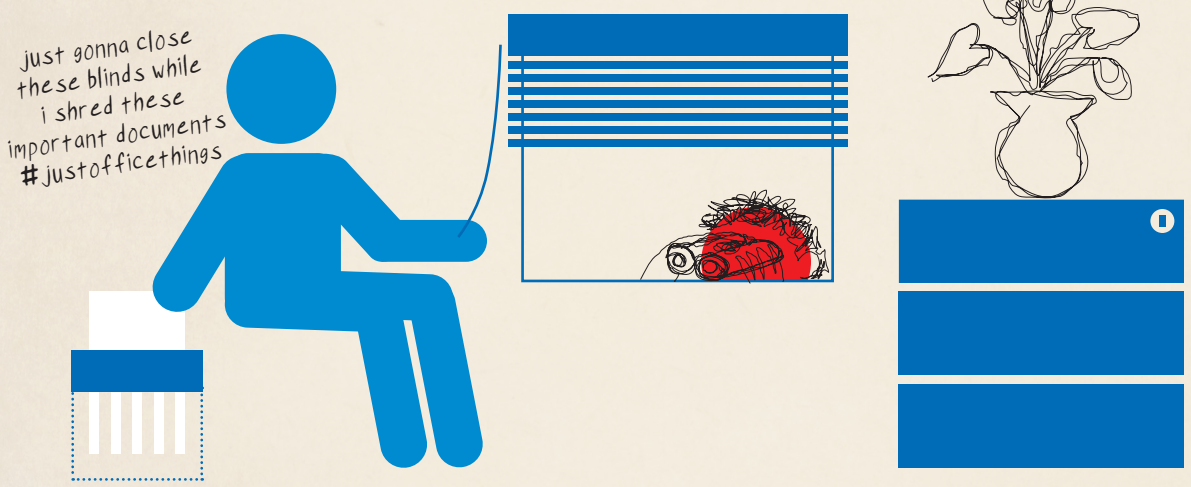
they're not just for watching "videos"

Protect Your Identity: Use VPNs and anonymous browsing tools to protect your identity while conducting OSINT investigations. Also, use sock puppets (*sans.org/blog/what-are-sock-puppets-in-osint/*) to search through social media.

Keep Records: Maintain detailed records of your findings — including timestamps, sources, and screenshots — to ensure accountability and reproducibility.

Collaborate: Engage with other OSINT practitioners and analysts to leverage collective expertise and resources.

Keep Learning: Make sure to stay up to date with novel techniques on how to find information. My OSINT Training, OSINT Combine, and TCM Security provide excellent courses which you can use to start, as well as improve upon, your existing OSINT skills.



How to Protect Against OSINT

Check Privacy Settings: Review the privacy settings of the OSINT sources you're using, especially social media platforms, which tend to track as much personal information as possible.

it's hilarious how irrelevant your ads get when you use a VPN to change location, and never give out real info

Careful Sharing: Be careful of what and when you are sharing on the internet, and consider the possible consequences of oversharing.

Monitor Online Presence: Use monitoring tools to track your online presence and make sure that no sensitive information is available online.

be the cryptid you wish to see in the woods

Limit Your Public Information: Minimize the information shared on public platforms.

Protect Your Data: Employ secure passwords and MFA to safeguard against unauthorized access to sensitive data.

UNDERSTANDING GRC

How to Navigate Risks and Compliance Standards

written by Sean Reilly || @lokihakanin || techsecuritybytes.blog

"GRC" isn't all witchcraft and administrative nonsense — it's the core that drives security initiatives, connects security spend to business outcomes, and powers a well-functioning security team.

GRC in a Nutshell

- Stands for **Governance, Risk Management, and Compliance.**
- Translates business risk appetite into a target risk profile, creates policies and mandates controls to achieve that risk, measures compliance, and gets business agreement on residual risk.
- Helps businesses understand security's activities, justifies spend, and enables risk-informed decisions.
- The goal is to manage risk, not eliminate it completely.

Measuring Risk – Numbers or Opinions?

There are 2 core approaches to assessing risk:

- Quantitative Assessment: Measuring risk in actual $$ values or similar quantifiable measures. Challenging, requiring a mature business and security program.
- Qualitative Assessment: Rating risk on a scale (e.g., 1-5) through expert opinions and measurable tests. Easier — therefore, more common.

Most frameworks consider impact and likelihood, often including assets (determining impact), vulnerabilities (determining likelihood), and threats. GRC considers a broad range of risks, including tech flaws, insider threats, natural disasters, and external market conditions.

Managing Risk

Risk management is what GRC is all about. GRC defines policies and controls based on business risk tolerance, assesses implementation, and identifies residual risk.

When risk is outside tolerance, we typically either:

- Remediate the source of the risk – Address the cause or vulnerability, often with temporary risk acceptance during the fix.
- Accept the risk as an exception – Document and accept isolated exposures.
- Adjust the target risk profile – Reevaluate and adjust overall tolerance.

Decisions are based on both impact and current or potential mitigations. Risks over agreed thresholds will be directly communicated to or signed off by business stakeholders.

Interested in Getting Into GRC?

Become the driving force behind security and a key interface between business and security leaders.

Educational Background

A bachelor's degree is generally required. Focus on analytical, technical, or risk-oriented fields like engineering, computer science, or business administration. Combine business acumen with technical skills.

Early Career & Company Selection

Good initial roles include:

- Junior Auditor / Analyst
- IT Helpdesk or Systems Support: Though not "GRC," these roles build analytical thinking and communication abilities while sharpening tech skills.

Look for employers in regulated industries like finance and healthcare, who need regular compliance assessments. Also, consider consulting firms (e.g., the "Big 4" - Deloitte, KPMG, PwC, and EY), who employ small armies of auditors and have career tracks from junior analyst to team lead.

Certifications

Certifications can help, but experience trumps all. Here are some helpful ones that won't break the bank:

- CompTIA Security+
- ISACA CISA

As you gain experience, consider:

- ISACA CRISC
- ISC2's CISSP or ISACA's CISM – both are management focused
- Pursue other niche certs only if you want to focus in a specific area

Helpful GRC Resources

NIST

- *nist.gov/cyberframework*
- *csrc.nist.gov/pubs/sp/800/53/r5/upd1/final*
- *csrc.nist.gov/projects/risk-management*
- *sans.org/reading%255Froom/*

ISO27001

- *iso.org/standard/27001*
- *cybrary.it/course/iso-27001-2022-information-security-management-systems*
- *itgovernance.co.uk/blog/category/iso27001*
- *iso27001security.com/html/toolkit.html*
- *udemy.com/course/isoiec-27001-information-security-management-system/*
- *udemy.com/course/iso-27001-cybersecurity-manager-guidelines/*

PCI-DSS

- *pcisecuritystandards.org*

HIPAA

- *hhs.gov/hipaa/for-professionals/index.html*
- *hhs.gov/hipaa/for-professionals/training/index.html*
- *healthit.gov/topic/privacy-security-and-hipaa*

ITIL & COBIT

- *axelos.com/certifications/itil-service-management*
- *isaca.org/resources/cobit*
- *axelos.com/resource-hub*
- *the-axelos-best-practice-podcast.simplecast.com/*
- *isaca.org/resources/cobit*

MALWARE ANALYSIS

How to Analyze and Understand Malware

written by John Hammond || youtube.com/@_JohnHammond

Malware analysis is an amazing field that can be interesting, fun, and useful for your cybersecurity career. If you're wondering WHY anyone would want to dig into malware, it's all for a better understanding of cybersecurity! Whether you are on "the blue team" and wanting to track what real threat actors are up to, or on "the red team" and wanting to emulate adversaries and know how their payloads work... malware analysis is an incredibly valuable skill. There are many who want to get started but aren't quite sure how. We've compiled a quick list of tools, tips, and advice to help you begin your journey!

Step 1: Set Up an Analysis Machine

You'll need a safe environment to analyze malware, as you don't want to accidentally infect your real system. Luckily, it's super easy to set up an analysis machine for free.

Here are some starting recommendations for beginners:

- Virtualization Software (VirtualBox or VMware Workstation)
- A Windows ISO File (you can download these from Microsoft's website)
- The FLARE VM Installation Script (which downloads all the analysis tools for you!)
- A REMnux OVA, the reverse engineering malware Linux distribution

Download VirtualBox or VMware Workstation, create a new virtual machine with your Windows ISO, and take a snapshot. I know it sounds crazy, because you haven't done anything yet, but **the best advice is to snapshot frequently** so you can always roll back to a known good state. Fresh install? Take a snapshot.

Run the FLARE install Powershell script on your Windows VM (and take a snapshot), and then be sure to lock down your VM settings by disabling networking and host access before starting to work with malware.

Step 2: Get Familiar With the Tools

The number of free analysis tools out there is amazing but also overwhelming. Luckily, you only need a few tools to get started. Here's a short list of tools that are free, beginner-friendly, and well documented in the form of public content.

PeStudio

PeStudio is the ultimate tool for inspecting binary files. It tells you everything prior to the files' execution, including strings, imported functions, entropy, and more. PeStudio is your best friend to begin analysis and inspect a suspicious binary file.

Process Hacker 2

Process Hacker 2 is like Task Manager on steroids. This tool allows you to easily view running processes, commands, strings, and memory regions.

Procmon

procmonster... no wait.... procodile

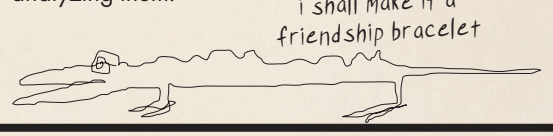
Procmon lets you see different operations that a program might do during execution. Procmon can see everything from executed commands, registry changes, and new files that were created during a program's runtime.

CyberChef

CyberChef is the Swiss Army Knife of script analysis and deobfuscation. It's a giant toolset of every operation and action that you might ever need to deobfuscate data.

DnSpy

DnSpy is for debugging and decompiling .NET malware. DnSpy can take a binary file and instantly provide the original source code for you to analyze. Many infostealers and RATs are written in .NET, so this is the perfect tool for analyzing them.



Honorable Mentions

These tools are super useful to know but can get a bit advanced for beginners. Keep these in mind, but don't get caught up on them early on: x64dbg, windbg, Ghidra, IDA, or Binary Ninja.

Step 3: Find Some Malware

To begin doing malware analysis, you'll need some actual malware to analyze. Here are some great resources for finding samples:

- Malware Bazaar
- Malshare

This can be a little overwhelming because it is a big data dump and feed of malware just being archived and cataloged... but honestly, just search for either a "type of malware" or a strain or variant that sounds interesting to you, or follow along with some other writeups and reports online!

Step 4: Learning Resources

Analyzing malware without any helpful resources can make you feel completely lost. Here are some great resources to get started and give some inspiration as to what to do when:

- Practical Malware Analysis (Book)
- Practical Malware Analysis & Triage (PMAT) Course
- John Hammond (YouTube)
- Jai Minton (YouTube, Website)

Step 5: Practice, Practice, Practice!

Sharpening malware analysis skills takes time and dedication... you may find you'll need to practice for days, weeks, months, or even years to stockpile your strengths and build confidence.

Keep learning, keep practicing, and don't give up! If you stay active in the community (on Twitter, Discord, Reddit, blogs, etc.) and engage with other learners and researchers, you all improve together.

Many others have been on this same journey and are often happy to help and answer questions. Never be afraid to ask for help and offer help to others!

CLOUD SECURITY

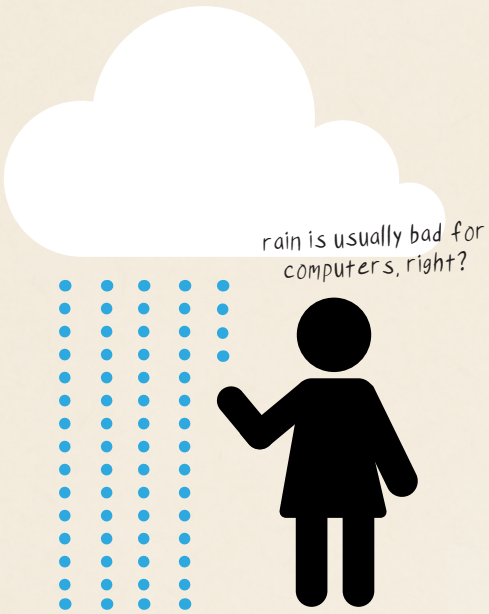
Security for the Cloud

written by Kevin Klingbile

Cloud Security is a combination of policies, controls, and technologies that an organization uses to protect cloud-based infrastructure, applications, and data.

Primary Providers

There are three primary cloud providers: Microsoft Azure, Amazon Web Services (AWS), and Google Cloud Provider (GCP). Security in these environments is managed through a shared responsibility model. This means that some aspects of security will be managed by you while others will be managed by your selected cloud provider. An organization's responsibility within the shared model will depend on the service types that are used.



Shared Responsibility Models:

Microsoft:
https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility

Amazon:
https://aws.amazon.com/compliance/shared-responsibility-model/

Google:
https://cloud.google.com/architecture/framework/security/shared-responsibility-shared-fate

Responsibility

On-Premises

You are responsible for everything from the physical security to the applications hosted.

Infrastructure as a Service (IaaS)

You don't worry about the physical things or even the virtualization, but you are responsible for the operating system and everything else.

Platform as a Service (PaaS)

Split responsibility between you and the cloud provider. You could be responsible for the security of deployed resources such as databases, accounts, and/or the authentication method. There are usually checkboxes for you to manage the security and limited options within the management interface.

Software as a Service (SaaS)

There is no direct control and often few security options available for you to manage. (Although, you are always responsible for your data no matter where it goes.) You may have control over the vendors you choose and verify what security is offered.

Working Together

Overall, effective cloud security involves people working together to protect cloud-based assets from potential threats and vulnerabilities. This role requires a blend of technical expertise, strategic thinking, and proactive risk management to address the unique challenges posed by cloud computing. Technical expertise can include securing operating systems, networks, applications, Identity and Access Management (IAM), devices (mobile and PC), and data.

Tips

- Always require multi-factor authentication (MFA)
- Stay up to date, cloud changes often
- Misconfigurations can easily lead to a compromise
- Always consider standard security principles including least privilege and need-to-know
- Review the provider's security recommendations at a minimum
- Use third-party resources to secure beyond the cloud provider's recommendations
- Review all menus and checkboxes for available security options
- Disable unused "features"
- Always look for a new attack surface after changes or new deployments

trust no one. constant vigilance.

Resources

General

Use the ATT&CK® Cloud Matrix to be aware of tactics and techniques that apply to cloud-based technologies.
https://attack.mitre.org/matrices/enterprise/cloud/

Use Center for Internet Security (CIS) cloud benchmarks to compare against your cloud configuration.
https://www.cisecurity.org/cis-benchmarks

Comprehensive security guidance for cloud environments.
https://cloudsecurityalliance.org/artifacts/security-guidance-v5

Tools for Defense

Cloud Auditing Tool – works on all major cloud platforms. Quickly gathers configuration settings and highlights areas of risk.
github.com/nccgroup/ScoutSuite

Post-Exploitation toolset using the Microsoft Graph API. Recon, persistence, and data theft.
github.com/dafthack/GraphRunner

Find gaps within Azure MFA requirements.
github.com/absolomb/FindMeAccess

BloodHound data collector, Microsoft Azure.
github.com/BloodHoundAD/AzureHound

Azure AD hacking and admin toolkit.
github.com/Gerenios/AADInternals

Cloud Security Courses
antisyphontraining.com/course-catalog/

LEAD EFFECTIVE TABLETOPS

How to Learn More by Having Fun

written by Glen Sorenson || @glen4108 || linkedin.com/in/glen-sorensen/

Imagine herding your team of proverbial cats for what they expect to be another eye-rolling "preparedness exercise." But instead of the standard fare, you introduce a tabletop exercise (TTX) that's less about enduring another meeting and more about engaging in a collaborative challenge. It's like suddenly finding yourselves as the key players in a thrilling plot to outsmart security incidents, bad actors, and other such diabolical disasters.

Tabletop exercises have long been a staple of security and BCDR activities, designed to simulate real-world scenarios for team training and preparedness. These exercises typically unfold boringly — in a meeting-style setting where participants discuss sterile scenarios. With some will and some skill, these monotonous exercises can be made much more engaging and even... **gasp** **fun.**

not when i'm there

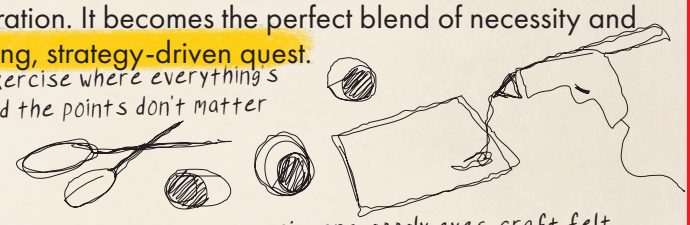
nothing will top the raccoon incident

People do learn effectively *(and arguably* ***better)*** **when they're having a good time.**

Make It a Game

You can build engaging TTXs by adding elements of gamification. This doesn't have to be an all-or-nothing prospect. The benefits of a fun tabletop exercise are manyfold: identifying gaps in plans, improving team cohesion, and enhancing decision-making skills, all while making the dreaded drill a source of laughter and inspiration. It becomes the perfect blend of necessity and engagement, turning a chore into an intriguing, strategy-driven quest.

an improv exercise where everything's made up and the points don't matter



scissors, googly eyes, craft felt, and an unhealthy amount of hot glue

But How?

How do we craft and run a fun and effective TTX experience?

Know Your Audience.

Is your TTX for a group of highly technical IT and security folks or do you have a mix of IT and non-technical business leaders?

Understand Your Objective.

Are you training your technical IR team or are you raising awareness with business leaders?

Play with Assumptions.

Don't be afraid to make assumptions about the scenario and challenge assumptions made by the team. Yes, your EDR can be bypassed. No, your web app is not invulnerable behind a WAF. Yes, people will click links and cough up credentials and MFA codes.

Keep it Believeable.

or the laws of physics

Don't feel bound by reality. You can invent a fictitious company and environment. It should be grounded in reality, but it doesn't have to be real.

When there's more fiction **involved,**
egos and attachments to outcomes **often become *less involved.***
This is a good thing.

Give players a character with a role that may be different than their normal daily self. Have someone play the company CFO bent on numbers, a Communications Manager more focused on their book deal, or the crazy Linux guy that has to use Microsoft technology against his will. Seriously, exaggerate and have fun with it. In doing so, you can greatly broaden worldviews.

Don't Lose Sight of Reality.

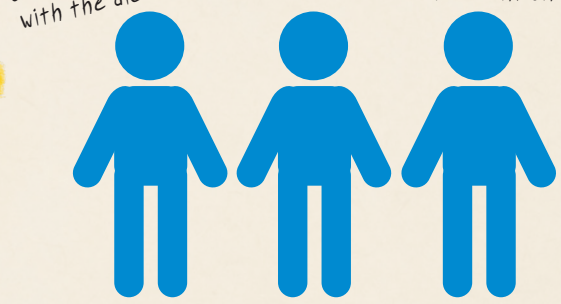
Bring in some realistic elements. Do a little homework. A good source of inspiration is MITRE ATT&CK Framework and MITRE's Cyber Threat Intelligence, which has a great deal of information about real-world campaigns, threat actors, and tooling. You should know the chain of events behind the scenes, but you don't always have to get extremely technical about it.

Adapt and Be Flexible.

You can shoot yourself in the foot if you plan too rigidly and the participants/players take it a direction you didn't think of. like i always do

oh no, cheryl's at it with the dice again

time for another intervention



i'm not even playing anything, i just like tossing these

Randomize It.

Roll dice. When someone wants to take an action, determine a difficulty level (a simple high, medium, or low will suffice) and make them roll dice to determine success or failure based on that difficulty. How many times in a real investigation have you wanted to examine logs for something specific, only to find you weren't logging what you thought you were? Or the flip side; by some sheer miracle, an employee recognized unusual behavior, shut down their computer, and called the security team?

Different IR roles (and characters if you're using them) may have different strengths and weaknesses. Your legal counsel is probably not going to sift through logs and your crazy Linux guy may not be the best person to craft messages to customers. Modify dice rolls appropriately.

Bring pizza. Have fun. Learn. Grow!

For help structuring a gamified incident response, check out:

HackBack Gaming: *hackbackgaming.com*

Backdoors & Breaches: *backdoorsandbreaches.com*

--ahem-- speaking of Backdoors + Breaches, check this out...

BACKDOORS & BREACHES

How to Play and Where to Get Started

an Incident Response card game created by BHIS

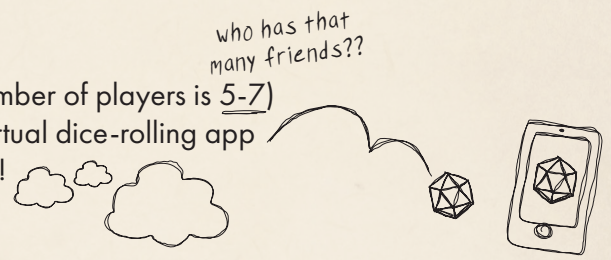
Backdoors & Breaches is a cooperative, cybersecurity threat emulation game in which "Defenders" will work together to uncover the attack pathways used to hack into their environment. Taking the concept of traditional tabletop exercises, Backdoors & Breaches combines the structure of a card game with the flair of classic role-playing games to help organizations and individuals learn about the tactics, methods, and tools used in cyber attacks and defense.

Contents

Among the 52 unique playing cards in your Backdoors & Breaches: Core Deck, you will find:

You Will Also Need

- A crew of 2 or more (ideal number of players is 5-7)
- A d20 (20-sided die) OR a virtual dice-rolling app
- A healthy dose of imagination!



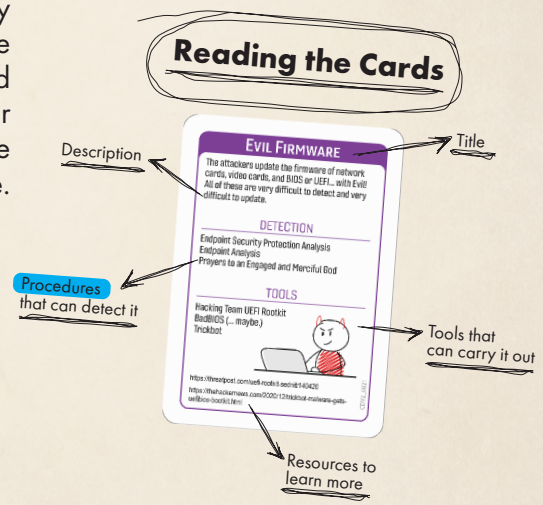
Getting Started

Overview

Using a secret array of 4 Attack cards, the "Incident Captain" will craft an imagined security breach and guide the "Defenders" through the scenario. Equipped with critical thinking, dice, and PROCEDURES, the Defenders will attempt to discover what the attackers are doing before it's too late! The gameplay of Backdoors & Breaches is cooperative. You either win as a team, or you lose as a team.

Objective

To win, the Defenders must reveal all 4 Attack cards before 10 turns have passed. Otherwise, they have failed to uncover the various avenues of the attack, and they lose.

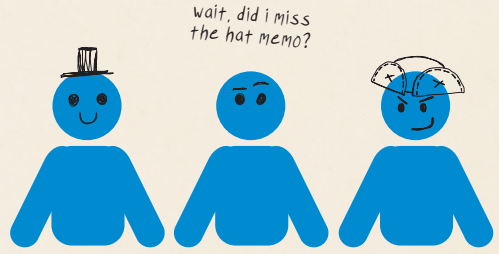


Determining Roles

Before you start, you must determine roles for each player: Incident Captain or Defender.

Choose 1 person to serve as the Incident Captain. This person will be responsible for crafting the starting scenario, answering questions, improvising situations, and is overall in charge of guiding the game process. Whoever you choose should have a wide breadth of cybersecurity knowledge and be a quick thinker. All other players will serve as Defenders. They form the team responding to the incident at hand.

INCIDENT CAPTAIN
1 CREATIVE LEADER



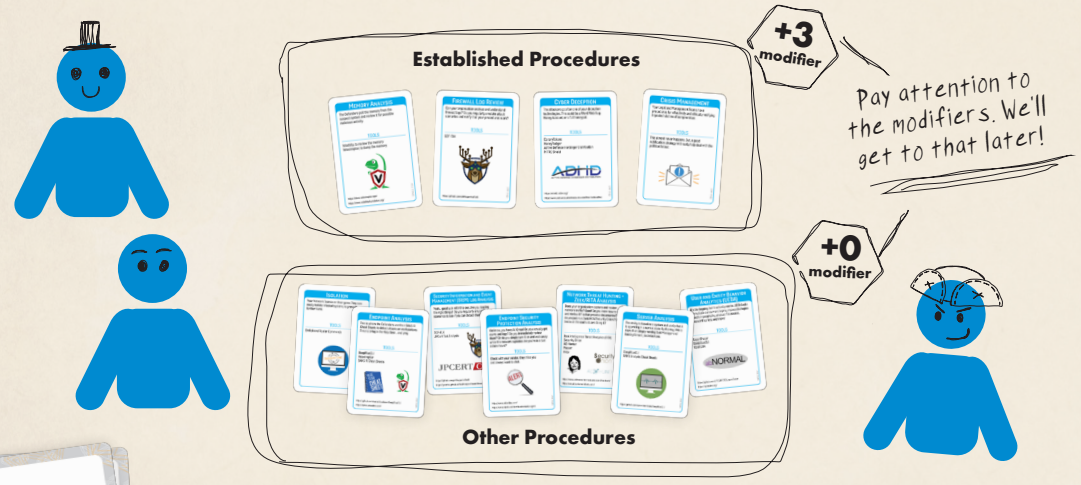
DEFENDERS
2+ ENTHUSIASTIC PLAYERS

Incident Captain Setup — Attacks

The Incident Captain chooses 1 card from each Attack card pile (INITIAL COMPROMISE, PIVOT and ESCALATE, C2 and EXFIL, PERSISTENCE) and keeps those cards hidden from the Defenders! Once the Incident Captain has all 4 Attack cards, you will not need the rest of the Attack card piles for the remainder of the game.

Defenders Setup - Procedures

You will now deal the PROCEDURE cards into 2 rows: Established Procedures and Other Procedures. For Established Procedures, deal 4 random cards face up. For Other Procedures, place all remaining PROCEDURE cards face up in a row beneath.



Injects Setup

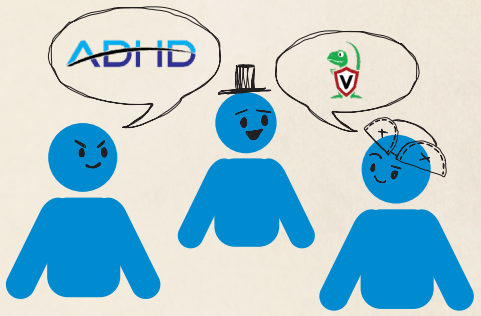
Place the INJECTS pile to the side of your play area, face down.

Playing The Game

To begin, the Incident Captain must set the stage by crafting a breach scenario based on the 4 Attack cards. This should be detailed enough to give the Defenders a place to start, without giving away the specifics of any Attack cards.

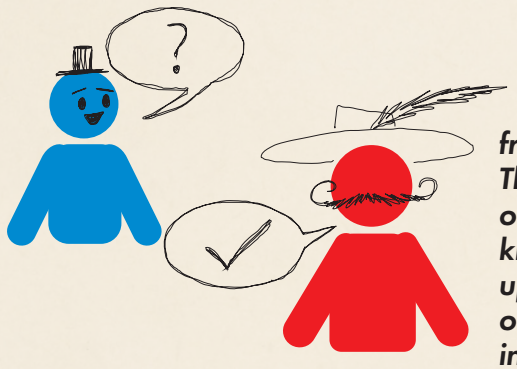
[Incident Captain Tip: It is usually easiest to build the scenario from the INITIAL COMPROMISE card.]

Sequence of Play



1. Discussion

The Defenders should discuss the current situation amongst themselves and decide which of the PROCEDURES they should attempt to use.



[Defenders Tip: The Defenders can seek clarity from the Incident Captain during this phase. They may ask the Incident Captain to expand on details that would make sense for them to know. This does not require any dice rolls. It is up to the Incident Captain to decide whether or not the Defenders would have access to the information they are seeking clarity on.]

2. Decision

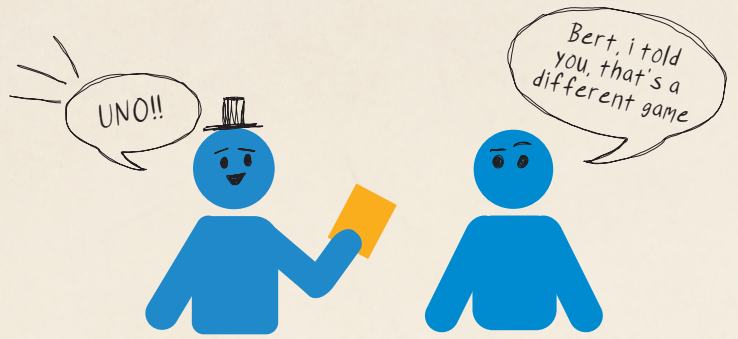
Once the Defenders have reached a consensus, they declare which PROCEDURE they will be attempting, and roll the d20. You may only play 1 PROCEDURE per turn. Established Procedures (top row) add a **+3 modifier** to the dice roll when they are played. These have an advantage as they indicate procedures that your team is very experienced with. Other Procedures (bottom row) **do not receive any modifiers.**

3. Rolling

When the Defenders wish to play a PROCEDURE card, they must roll the die to determine if the PROCEDURE is successful or if it fails to detect an attack.

Failure	**1-10**
Success	**11-20**

Remember to add any relevant modifiers to the roll! A roll of either a natural 1 or natural 20 (indicating the number on the die face before anymodifiers are added) or 3 failures in a row will trigger an INJECT!



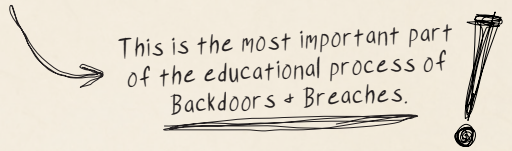
If an INJECT is triggered: Draw 1 card from the top of the INJECT pile and reveal it to all players. Follow any instructions that may be on the card, and have the Defenders discuss how (or if) this INJECT will affect their investigation.

INJECTS simulate the random events that can happen during a security incident. They add a bit of chaos to the scenario and spur important conversations. Some might not affect the game at all... or might end it. Either way, they're always unexpected.

4. Outcome

On a failure, nothing new is learned and the turn ends. On a success, the Incident Captain checks if the PROCEDURE played is listed under "Detection" on any of the Attack cards. If it is, they reveal that card to the Defenders. If the PROCEDURE could detect multiple Attack cards, it is up to the Incident Captain to choose only one card to reveal. (As in real life, when doing incident response, you find one thing at a time, not everything all at once.) After a PROCEDURE has been played, regardless of outcome, that card will have a 3-turn cooldown period during which it cannot be used again.

[Incident Captain Tip: If a PROCEDURE is unsuccessful, ask the Defenders for a reason—whether financial, political, personnel-wise, or technological — why the PROCEDURE would not be successful at that time.]



Ending The Game

The turn cycle repeats until whichever comes first:

The Defenders have revealed all 4 Attack cards
OR
10 turns have passed

Ready to Start Playing?

Play Online: *https://play.backdoorsandbreaches.com/*
Order Physical Decks: *backdoorsandbreaches.com*

NETWORK ENGINEERING

How to Engineer Networks

written by Serena DiPenti || @shenetworks

The computer networking field is broad, encompassing many focus areas similar to cybersecurity. If you're new to the field or just interested in networking, knowing where to start can be challenging.

Searching for a network engineer position on any job listing site will yield thousands of results, and no two job descriptions will be the same. However, there are some similarities. Below are three common roles associated with networking positions and brief descriptions:

- **Network Analyst:**
  - » Focuses on network maintenance and support.
- **Network Engineer:**
  - » Handles network implementation and complex troubleshooting.
- **Network Architect:**
  - » Focuses on long-term strategic planning and design.

Role Differentiation

While these descriptions help understand some differences between these roles, they often blend together. For example, a network engineer at a company with tens of thousands of employees may have different responsibilities than a network engineer supporting small businesses. Typically, as companies and networks grow larger, the jobs become more specialized. A network engineer in a small township might need to know a bit about everything the city uses, whereas a network engineer at a massive international company may only support one small network area and be expected to know it in depth.

Key Areas Within Networking

Network Operations Center (NOC):

A team responsible for monitoring and maintaining network performance and availability while proactively identifying potential issues to ensure minimal downtime.

Enterprise Networking:

Supports the daily operations of a large organization by providing connectivity for employees, devices, and business units.

Data Center Networking:

Manages data center infrastructure, such as virtual computing, storage systems, data processing, and large-scale applications. High performance and low latency are crucial.

Cellular Networking:

Supports wireless and mobile networking over large geographical areas, focusing on voice and data services and maintaining good coverage.

Internet Service Provider (ISP):

ISPs service wide-area networks (WANs) and facilitate global communication from large businesses to residential neighborhoods worldwide.

Additional Areas Include:

Network security, network automation, and cloud networking. This list is not exhaustive but offers a great starting point for investigating which area you might be interested in.

Career Opportunities

One day, you could be racking and stacking servers at Meta's 4.6 million square foot data farm or helping to expand 5G and supporting the Internet of Things (IoT). Maybe you'll be in charge of securing a classified network. There's even the possibility of designing an underwater data center, like Google's Project Natick, which deployed a shipping container-sized data center 117 feet deep into the ocean.

Standards

The good news is that the fundamentals remain largely the same no matter what you choose. Vendors may use their own names and terminology, but ultimately, everything runs on standardized protocols. Standardization is necessary for interoperability, ensuring that no matter the vendor or manufacturer, land or sea, Canada or China, toaster to rocket ship, they'll all be speaking the same language.

Helpful Resources

Cisco Networking Academy:

Offers a range of courses, including CCNA (Cisco Certified Network Associate), which is a foundational certification in networking

https://www.netacad.com/

Packet Tracer:

A network simulation tool provided by Cisco that allows you to create network topologies and simulate network traffic.

https://www.netacad.com/courses/packet-tracer

GNS3:

An open-source network simulator that allows you to run a virtual network.

https://www.gns3.com/

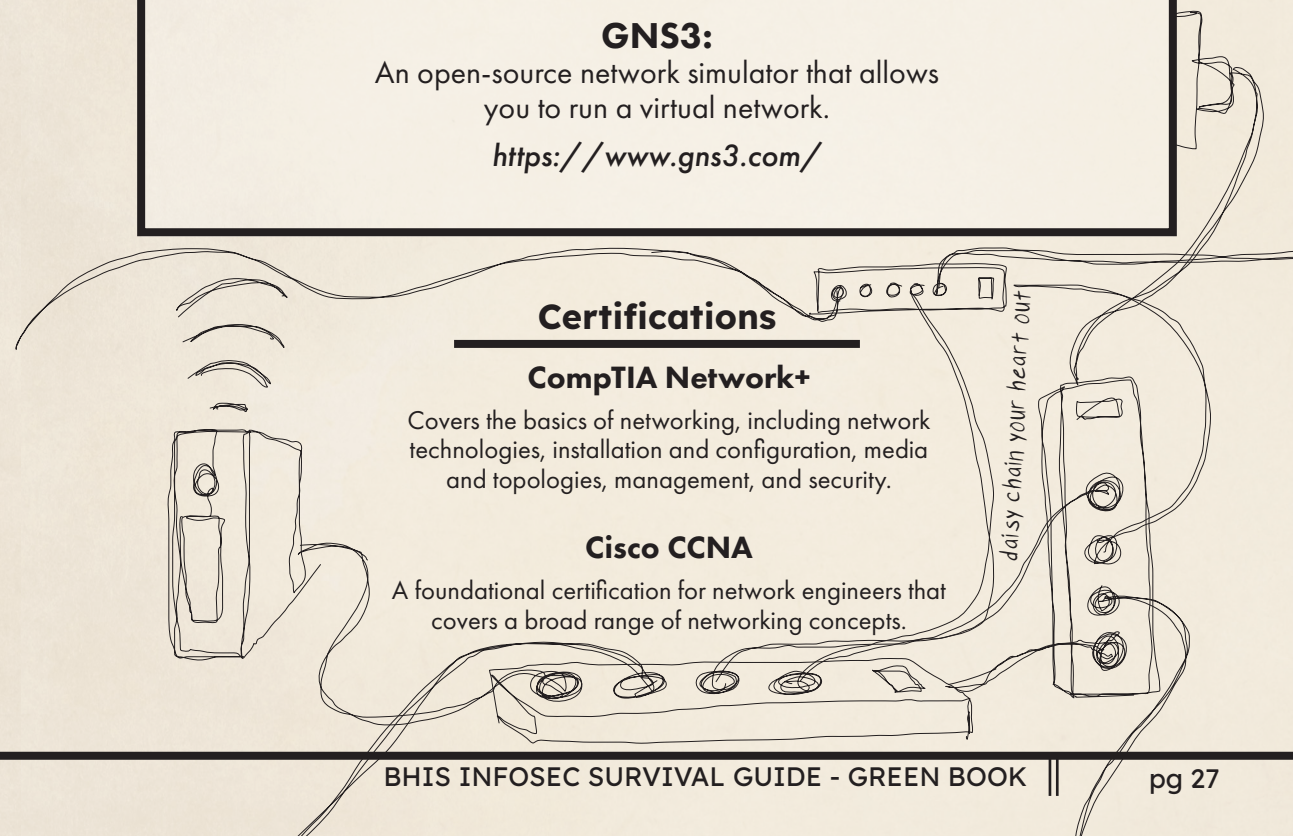
Certifications

CompTIA Network+

Covers the basics of networking, including network technologies, installation and configuration, media and topologies, management, and security.

Cisco CCNA

A foundational certification for network engineers that covers a broad range of networking concepts.



IT HELP DESK

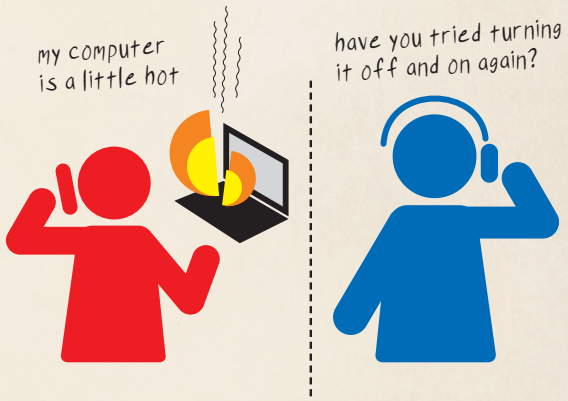
How to Succeed and Grow

written by Sean Reilly || @lokihakanin || techsecuritybytes.blog

Looking to work in security? Start your career in "Tech" — where helpdesk roles are an excellent place to get going. These roles build foundational skills that transfer well into functions like SOC, GRC analysts, and more.

Helpdesk - What Is It?

- Frontline support focusing on end-user needs. Often, these are internal customers; you work at "company A" and help other "company A" employees.
- A blend of issue resolution (*"My laptop / MS Office / Slack is not working..."*) and service requests (*"I'm looking to get a new device / application / etc."*)



How Do You Get In?

Helpdesk is foundational to IT, and therefore, easier to get into than other roles. Many organizations hire people with limited experience. Here are a few tips to land that first gig:

- **Showcase customer service experience:** Whether it's retail or restaurant work, emphasize your people skills on your resume.
- **Highlight your tech affinity:** Technical hobbies or skills — from PC building to coding to CTFs — are all a plus.
- **Target larger organizations or educational institutions for your first role:** They have established helpdesks and the capacity to train.

Stand Out on the Job

The key to using a helpdesk as a stepping stone is to make the most of it.

Learn Continuously:
When escalating to experienced engineers, don't "tune out" — ask questions, take notes, shadow them to gain insights.

Don't blindly follow procedures:
Grasp the why behind them, and research if you don't understand.

Innovate and automate:
Seek ways to streamline processes. Build or update documentation, or learn scripting to automate common tasks.

Embrace "on-call," especially off-hours:
The skills to handle issues "on-demand" at odd times, remotely, etc., are as applicable to troubleshooting user issues as they are to dealing with SOC alerts at 3 am.

Don't overdo it:
Equally important in a 24x7 SOC is self-managing and knowing when to tap out. Make sure to keep a healthy work-life balance.

Invest in training: *make them pay for you to learn*
Make use of any company-provided training to upskill without bearing the cost. Even if studying outside the office, it's basically free money.

Solicit feedback:
"98% surveyed satisfaction" says a lot about your quality of problem solving to a future employer. *it says that two percent didn't like you*

Helpful Resources

Google's IT Support Professional Certificate
A cost-effective "crash course."
https://grow.google/certificates/it-support/

CompTIA A+ and Network+
Ideal for those ready to deepen their knowledge post-first gig or for ambitious newcomers.
https://www.comptia.org/certifications/a
https://www.comptia.org/certifications/network

How Do I Leverage Helpdesk for Bigger Things?

Helpdesk can be a fantastic launchpad for careers in tech and security. Depending on your goals and preferences, there are many tracks to follow. Here are some examples:

Help Desk > **Back-end/Cloud Support > SOC Analyst**
Help Desk > **GRC Auditor or Analyst**
Help Desk > **Developer (and/or backend support) > Pentester**

Helpdesk can teach many transferable skills, including working in shifts, developing shared procedures and knowledge bases, basic automation and scripting, basic networking, and OS configuration and diagnostics.

You'll also develop communications & customer service skills. Both are helpful in other roles — connecting with diverse people is a key skill in a GRC assessor or auditor, concise communication to management is an asset for any SOC analyst, and pentesters must clearly and effectively summarize complex vulnerabilities.

Broaden your tool belt by springing into back-end (e.g. server-side and cloud-based) app support. This will round out your operating system experience and teach you valuable skills about system monitoring (foundational to SIEMs used in security).

If scripting scratched an itch for you, target a move into software dev, which can help get you into SOC, pentesting, and other disciplines.

If you're looking to get into security, particularly with limited tech, a helpdesk can be an incredible jumping off point. Roles are accessible, opportunities to learn are common, and benefits are solid. Consider starting your security journey in IT helpdesk.

HIRE THE RIGHT PERSON

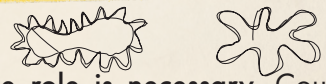
Hire Like a Hacker

written by Kip Boyle

This decision will shape the future of your team and your legacy as their manager. Instead of covering what questions to ask, let's focus on the pre-search process — an often overlooked foundation for success.

This process deserves time and attention.

A hasty hiring can lead to setbacks and waste political capital. It's not just about filling a position; it's about finding someone who will contribute to your team's growth and culture. but not like in a petri dish way



Before jumping into the hiring process, **ask if the role is necessary.** Could the tasks be automated, delegated, or outsourced? If you decide that hiring is essential, **commit to putting the right amount of care and attention into the decision.**

Working with HR

or whatever weirdo is serving as your HR department because your company is too small. (am i right, CJ?)

When creating a job posting, it's important to work closely with your human resources (HR) department to make sure they understand the role's requirements and the type of candidate you're looking for.

If there's a disconnect between your vision and HR's approach, it's time to understand why. Some HR departments focus on filling positions quickly rather than finding candidates who align with the company's values and culture. If you find yourself in this situation, spend some time understanding your working relationship with your HR department. In other words: if it's bad, why is it bad?

> Often, **a bad working relationship** with HR can be explained by a **mismatch in values.**

If HR really does see people as the company's greatest asset, they'll search for people who possess critical, unteachable skills that cannot be trained on the job — like curiosity, humbleness, and resilience.

In contrast, if they prioritize putting "butts in seats," they'll hire as quickly and cheaply as possible. Their pre-employment screening will focus on hard skills and pedigrees. Ask yourself which approach you value and which one they value. If you both match and the relationship is still not productive, then you've really got some work to do. But it could be as simple as educating your HR team on your hiring philosophy.

Learn more with the **HR Tool Kit**
https://b.link/hr-partner

Cybersecurity Hiring Manager Handbook:
This podcast offers additional insights and strategies for making informed hiring decisions:
https://cr-map.com/podcast/102/

Finding Candidates

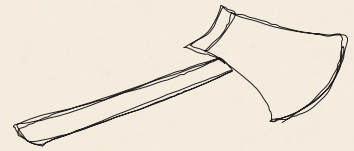
Remember that candidates often view job descriptions as strict requirements. If the description lists many non-negotiable skills or qualifications, you might intimidate people who could have been a great fit. (Most hiring managers want someone with so many skills and capabilities that you might as well search for a unicorn!) Instead, focus on essential qualities and skills. Lower the bar as much as you dare.

Your network is a powerful tool. Share the job description with contacts and ask for candidate recommendations. Or consider internal candidates who want to grow in the organization.

If you're interested in hiring for character, looking for traits like humility, soft skills, and an appetite for growth is essential for building a cohesive and effective team.

> **Ideal candidates are humble, hungry for growth, and people smart.**
>
> - Patrick Lencioni in "**The Ideal Team Player**"

Be Selective



so you don't accidentally hire an axe murderer.... again.

During screening and interviewing, look for reasons to say "no" rather than "yes." While this may seem counterintuitive, being selective helps you move forward with candidates who truly meet your criteria, thus reducing your risk of a mis-hire.

There aren't any special questions you need to ask to find reasons to say "no." Simply set a high bar as you evaluate the answers you're getting back from the candidates. Are there any "red flags" in the answer you just heard? If so, move on.

Regarding what questions to ask, be sure to give equal attention to both hard skills and the skills you want but cannot teach. What do I mean? In my experience, I can teach most people hard skills as long as they have some aptitude. However, it's extremely difficult, if not impossible, to teach someone curiosity, perseverance, or how to create and nurture healthy working relationships. because that's just therapy, not workplace skill training

Remember, the consequences of a hiring decision will affect your team and company for a long time. Being thorough and deliberate in this process is crucial. Don't give in to "decision fatigue" so you can "get back to work." Hiring this person is your work.

Hiring Handbook:
How to Build an InfoSec Team that Gets Stuff Done
with Kip Boyle

Available On-Demand
16-hour Antisyphon course
https://www.antisyphontraining.com/course/hiring-handbook-how-to-build-an-infosec-team-that-gets-stuff-done-with-kip-boyle/

SECURE SMALL BUSINESS

Advice for Small IT Teams

written by Ashley Knowles || @jrpentester

Small businesses typically don't have the budget or manpower needed to reach reasonable security. Employees in the IT role often wear many hats and may not know what to do or have the budget to complete the necessary steps to secure their infrastructure. This quick start guide should help any-size business secure their company.

We'll be exploring the NIST Cybersecurity Framework v2.0 *(https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf)*. NIST also released a quick start guide for small-to-medium business owners, including those that have little-to-no cybersecurity plans in place *(https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1300.pdf)*.

Check out the CIS Reasonable Cybersecurity Guide for an expanded definition on reasonable security:

https://www.cisecurity.org/insights/white-papers/reasonable-cybersecurity-guide

Identify

When assessing your security posture, it's important to start with an inventory of physical and software assets. Include things like any servers deployed, workstations like laptops, VoIP phones, printers, fax machines, any IoT devices, what operating systems are in use, etc. These lists should be readily available for easy updates.

Some questions you can ask to help guide yourself through the identification process:

Who has a business-issued laptop?
What systems are online in the office that help with day-to-day operations?
What data is stored on those systems?
What software is being used to ensure the business operates?
Where can we store the inventory of hardware, software, and data so it is easily accessible?

Protect

Once you've identified your hardware, software, and data in your network, the next step is to protect those assets. The following is not an exhaustive list but a good starting point of things that can be done to secure and protect the network.

Data protection: Many operating systems offer disk encryption, consider also encrypting any sensitive data.

Data backups: Consider backing up important data and key systems regularly to multiple locations.

Hot Onsite: Maintains a constant backup of live data on premises.

Hot Offsite: Constant backups that are slightly behind hot onsite save states.

Cold Offsite: Takes more time, is used to generate a stable state with some data loss.

Secure Configuration of Assets: Conduct research into the assets on the network and their security features. Create a baseline of what the configuration should look like and ensure policies and procedures are updated so that any new systems deployed to the network are upheld to these standards.

Account and Asset Control Management: Consider implementing a "business need-to-know" policy of least privilege. If someone doesn't need access to something, don't give it to them. Implement separate administrative accounts from user accounts for technology admin tasks; admins should not be checking their email from a privileged account.

Network Infrastructure Management: Implement a protected list of systems and consider including an easy way to conduct regular health checks on those systems.

Security Awareness and Skills Training: One of the easiest ways to gain access to an internal network is through social engineering. Help employees learn to detect and respond to social engineering attempts.

Amazon's Cybersecurity Awareness training:
https://learnsecurity.amazon.com/en/index.html

Social Engineering Survival Guide Article:
https://www.blackhillsinfosec.com/how-to-perform-and-combat-social-engineering

Detect

Detecting possible attacks and compromises is paramount. Continuous vulnerability management can help ensure systems and software are patched and that attackers are not provided an opportunity to gain a foothold in the environment.

Make sure systems are properly recording and sending logs by auditing them regularly. Check that alert generation is working; for example, if a server goes down overnight, how will alerts be generated and sent? A good frequency is quarterly, better frequency would be monthly, best would be weekly.

See that all possible protections are put in place for email and web browsers, including ad blockers. Implement content filtering in boundary devices. Install malware and anti-virus protection as well as ensuring that it cannot be disabled easily. Consider utilizing both workstation and network firewalls.

If possible, get a penetration test done once the above steps have been taken.

Respond

The next step is creating policies and procedures on how to respond to a potential attack, ensuring they're easily accessible and known to all parties necessary. Conducting dry-run tabletops like Backdoors & Breaches is a great way to test that they're working appropriately.

Recover

If an attack does occur and systems need to be recovered, this step makes sure that is possible. This should also include operational recovery, which refers to specific parts of IT infrastructure in case of an IT failure or a small incident.

Lastly, make sure that a plan is put in place, such as a business continuity plan and/or a disaster recovery plan. These plans should outline how your company will prevent, respond, and recover from potential threats and include contact information for key personnel.

AI FOR GOOD

It's Not All Bad (but, yeah, some of it is)

written by The PROMPT# team and Andrew Heishman || @WumpusTheBrave

It's easy to feel frustrated by the over-abundance of AI in places where AI just ain't as good. We've made it our mission to track down some reasons to be hopeful about the future of AI and where it can be used to aid incredible human accomplishments.

Areas of Concern

We've outlined three major areas of concern: **soft skills, authority, and creativity.** It's no mistake that these are also very human skills. AI can help in many ways, but there's no replacing humans full of heart. We love. We care. We don't want that replaced by a cold algorithm.

What if we reframe the conversation? Instead of replacing humans, we use AI as a tool to enhance our efforts. After all, AI isn't out to take down humanity. It's just a tool, and, like any tool, it can be used to hurt or to help.

Enhance Your Soft Skills

Empathy affects efficacy. When folks struggle with soft skills, it's challenging for everyone involved.

Tools like Grammarly are built to analyze your input and rate it on how friendly or professional it sounds. Using ChatGPT to help practice conversations (like job interviews) can make therapeutic role-playing exercises accessible to anyone with a computer. Depending on your career, improving your soft skills may help you earn a promotion or even save a life.

AI can be used to help train soft skills and track their impact. Discover more: *https://hbr.org/2022/01/can-ai-teach-us-how-to-become-more-emotionally-intelligent*

Understand Authority & Protection

Not a Lawyer but Played One in a Video Game

AI can help translate complex knowledge into something more accessible, helping to speed up research processes, summarize lengthy findings, and translate jargon into everyday language.

But it's not a replacement for human review. AI doesn't verify; it can present false "facts" known as "AI hallucination." To prevent getting caught in an AI hallucination, try googling the key pieces of info, like names and places. Or try asking AI for links *(and actually click them)*. If you can't verify, it's an AI hallucination.

i wanna try whatever AI's been taking

AI hallucination has already been demonstrated and rejected in court: *https://www.forbes.com/sites/mollybohannon/2023/06/08/lawyer-used-chatgpt-in-court-and-cited-fake-cases-a-judge-is-considering-sanctions/amp/*

Ace Detective on the Case

the word you're looking for is "automated" lots of stuff labeled "AI" is actually just an automated process.

AI tools can help sift through mountains of data, speeding up detective processes and providing small teams with big help. This helps all sorts of guardians, from cybersecurity to murder investigations, forensics, and more by enhancing their efforts, not replacing them.

Learn more about a wide range of inspiring crime-fighting AI help: *https://www.bbc.com/future/article/20190228-how-ai-is-helping-to-fight-crime*

Boost Your Creativity

Embrace traditional strategies in a modern way.

Brainstorming

keep creativity human and support your local/favorite artists

Artists have always looked to references for guidance and inspiration. AI can help "photobash" some ideas together for a good brainstorm reference. It provides a quick way to find unique or impossible reference images, and you can still apply the same rules of ethics typically applied to traditional references. This is not the same as sketching with AI. Use AI as inspiration, to boost your own creativity, not a replacement for your own skills and brain. don't even sketch with AI. create a mood board, sure, but remember to practice your own sketching to build that skill and always grow as an artist.

AI may be used to help conservators repair damaged masterpieces, watch this: *https://youtu.be/rDVcgpSwnyg*

Stock Images

Going far back to ye olde printing days, there's always been reused, recycled "clip art" or "stock" graphics. Learn more about that history from graphic designer Linus Boman: *https://youtu.be/XfLlpxE6AYM*. Humans use these stock assets in low-impact ways. You were never going to hire a designer to make your PowerPoint meme. So go ahead and ask AI to draw you that muscular cat rescuing a kitten-sized firefighter from a tree.

i support shenanigans

Learn more about working with designers, ways to use AI art, and why we should care: *https://youtu.be/12foW5hVa4c*

Computer Solutions to Computer Problems

QR codes aren't aesthetically pleasing because they aren't made by or for human eyes. So, what if we toss this problem back to the computers? There are AI art engines trained to create beautiful QR codes that remain readable.

https://stable-diffusion-art.com/qr-code/
https://antfu.me/posts/ai-qrcode-101

Save Humans and the World

"It's not about replacing the expertise, it's helping and [...] empowering physicians to do what they're good at."

https://cbs12.com/amp/news/local/boca-raton-regional-hospital-uses-artificial-intelligence-to-detect-breast-cancer-earlier-baptist-health-ai-mammogram-scan-lynn-cancer-institute

Medical Solutions

AI can help doctors diagnose medical conditions ranging from breast cancer to childhood ear infections more quickly and accurately. These earlier diagnoses are already saving lives.

https://www.cbsnews.com/pittsburgh/news/ai-smartphone-app-diagnose-ear-infections-pittsburgh/

Protecting the Rainforest

By sifting through thousands of hours of monitoring footage assessing the wildlife population or scanning the local geography in search of illegal deforestation, AI can help empower protectors of the earth by providing a helping hand with data. Utilizing these tools, humans have helped repopulate formerly endangered species and are allowing forests to recover by stopping illegal activities in protected areas.

https://abcnews.go.com/US/researchers-ai-save-rainforest-species-puerto-rico-exclusive/story

AI for United Nation's Sustainable Development Goals:

https://aiforgood.itu.int/

Your Choice

AI is not inherently evil. It's a frustrating buzzword, but there is still plenty of hope if we look deeper. It's a powerful tool in our arsenal to help tackle challenges, big and small.

We get to choose whether it replaces our dream jobs or helps us save the world.

We, as humans, still get to make that choice.

choose wisely

UMM, ACTUALLY...

This book is incomplete and already out of date

We know. And we still published this. We checked as best as we could, but this world is fast-paced. One of the biggest challenges in any job, tech or not, is keeping up with new apps, new tools, new knowledge, new everything. It's a daunting task, and when you choose to publish something in print, there's always a risk that between the print date and the time the reader receives their copy, a newer thing has already appeared.

If you're always worried about being the most up to date, the most complete, the most perfect, you'll be waiting forever. This book is full of useful knowledge, encouragement, and resources that can help people. One of the recurring notions throughout is: Just get started. Start small if you have to, just start somewhere. That's what we did with this book too.

When we first drafted the idea for this format of the Infosec Survival Guide, we came up with more than 100 different topics, and even more sub-topics within each category. Every time we talked to another person, more topics were added. Making a 300+ page book is a monumental task, so we're taking it in little chunks.

We're not done yet.

We need your help.

We asked our community for help on this Survival Guide, and they were a delightfully helpful bunch. But if we want to keep going and make more volumes, more inclusive of every topic, every specialty, and every helpful nugget we can squeeze in, we need even more help.

If there's a topic you're looking for - ask us for it!
If there's a tool you want to share - share it with us!
If you're an expert and want to contribute - reach out!

Thank you for taking the time to read what we've compiled and participating in this project. We really mean it when we say we couldn't do it without you.

Better together.

or send in pictures of your pets. they won't go in the guide, but it sure is nice to see floofs and fronds

Help us make this guide more complete

info@promptzine.com

We're looking for articles! Submit yours now!!

Articles should be 200-700 words, encompassing one subject. They can be expanding on subjects we've already covered or new ones we've yet to explore. We're really trying to focus on the technical skills of our ever-changing industry.

Who and How

You do NOT need to be an advanced professional to qualify for writing an article! We're not checking resumes (we might poke around and make sure you're not like... an axe murderer or something), we're just checking your article. So if you're a student and you're passionate about what you're currently learning, you should write in! Equally so, if you're a seasoned veteran and have wisdom to share with The Youths, we wanna hear from you too!

We've found it helpful to write as if you're giving a friend a refresher, rather than teaching someone from scratch. Keep it casual, encouraging, and short! Jam-pack as much knowledge as possible within the word count, but remember the reader may be at ANY level. Try to find a nice balance that allows readers who already know what you're talking about to learn more, and readers who are new to follow along. **We usually say try to include enough to get the reader googling in the right direction.**

Remember this is printed, so screenshots take up valuable real-estate. If you must include screenshots, remember you must reduce your word count too. Try to write without them, or provide links so the reader can see them large and in charge on a digital screen.

If all that sounds hard.... IT IS! Writing short and sweet but still including a lot of info is a huge challenge, and most of our writers have found it easier to write long reports than it is to write short. We believe in you, and we're happy to help cut the word count down if you're eager to contribute but struggling to write in this style. **We know it's a challenge, but YOU'VE GOT THIS!**

The Process & What To Expect

When we get your article, it'll pass through 3 rounds of edits - first is the content round, to see if the article is applicable to the Survival Guide and if there are any requests for changes in tone or content. If your word count is a little over, we help edit it down to fit, or help make the call that all those words are worth keeping! Writers usually aren't involved past this round of edits.

Once that's ready, we toss it to our tech checkers for the second round of edits, they make sure everything in there is accurate. We wanna make sure you look your best, so we help to make sure everything checks out!

The third round of edits is when the article goes to the design phase. Sometimes we have to cut or add words to make things fit and not leave orphan words dangling, or we find visual ways to condense longer concepts.

Once all that's done, you'll see your article in print!

WHO IS BHIS?

Established in 2008, Black Hills Information Security has created a network of companies in the infosec industry dedicated to providing affordable, outstanding products and services that cover all of your information security needs from pentesting to training.

Each company helps to support the infosec community in their own way—offering free educational content, open-source tools, or even donating to various projects.

We Offer

- Penetration Testing
- Red Teaming
- Active SOC
- Blue Team Services
- Purple Teaming
- Threat Hunting
- Incident Response
- Consulting
- Training
- IR Tabletop Demos
- Strategy, GRC (Governance, Risk, Compliance), and Privacy

"Our main goal is not to prove that we can hack into a company but to help the customer develop a series of on-point solutions and technologies that will improve the overall security of the company. Testing should never be adversarial, but collaborative."

– John Strand, Owner

We've worked with

- Credit Unions
- Banks
- Investment Firms
- Higher Education
- Health Care
- Medical Devices
- Insurance
- Law Firms
- Real Estate
- Retail
- Technology
- IT
- Software
- Utilities
- ICS/SCADA

From the smallest mom & pop shops to the biggest Fortune 5 companies, our top priority is helping you understand and achieve your security needs.

OFFENSIVE

Our team of 40+ pentesters conduct more than 1000 security assessments every year.

Knowledge transfer from our team to yours empowers you to mature and grow, so we take special care in our reporting. Our reports provide you with not only what was successful in an engagement, but also highlight your current strengths by showing what efforts failed.

Our experienced testers help you understand and fortify your own system.

- Penetration Tests
- Red Teams
- Internal
- External
- Pivots
- C2
- Web Apps/APIs
- Mobile
- Physical
- Wireless
- Cloud
- Embedded Device
- Active SOC

DEFENSIVE

To stop an adversary, we must think like one. Let our extensive years of red team experience inform and support your blue team needs.

- Purple Teaming
- Breach Assessment
- Atomic Controls Assessment
- Audit
- Network Operations Active Directory Consulting
- BHIS Expert Support Team
- Strategy, GRC (Governance, Risk, Compliance), and Privacy

ACTIVE SOC:

- Log Analysis & Active Directory Review
- Adversarial Simulation
- Cyber Deception
- Threat Hunting

INCIDENT RESPONSE

With experience as both red and blue teams, our IR team knows the ways to hunt down threats and analyze the evidence because we've been on both sides.

Whether you've already been breached, or you're looking to prevent it, we've got you covered.

- Training
- Collection and Analysis
- IR Retainer
- Monitoring
- Consulting
- IR Checklists and Playbooks
- IR Tabletop

BLACK HILLS | Information Security

ANTISYPHON TRAINING — antisyphontraining.com

wildwesthackinfest.com

activecountermeasures.com

REKCAH HACKER — rekcahcomics.com

PROMPT# — promptzine.com

bhis.co

ANTISYPHON TRAINING

Learn What's Bad; Do What's Good

you heard me

*We're here to **disrupt** the traditional training industry by providing **affordable education that doesn't suck.** Whether you're a total newbie or a seasoned pro, dive into interactive, hands-on sessions with certified instructors, and build real-world skills **while earning cool badges.** From pay-what-you-can to full price and everything in between, **we're all about making your learning journey effective, engaging, and ridiculously fun.***

Pay-What-You-Can Courses

L Live OD On-Demand ★ On-Site

- ☐ Active Defense & Cyber Deception L OD
  John Strand
- ☐ AI for Cybersecurity Professionals L
  Joff Thyer & Derek Banks
- ☐ Enterprise Security for All OD
  Rich Fifarek & Bob Hewitt
- ☐ Foundational Application Security Training (FAST) L
  Instructor: Secure Ideas
- ☐ Getting Started in Packet Decoding L OD
  Chris Brenton
- ☐ Getting Started in Security with BHIS and MITRE ATT&CK L OD
  John Strand
- ☐ MITRE ATT&CK Framework and Tools L
  Carrie Roberts
- ☐ Introduction to PCI – PCI 101 L
  Kathy Collins
- ☐ Introduction to AI for Cybersecurity Professionals L
  Instructor: Secure Ideas
- ☐ Professionally Evil API Testing: A Practical Course for Beginners L
  Instructor: Secure Ideas
- ☐ Professionally Evil API Testing: AAA and Keys are Not Just for Cars L
  Instructor: Secure Ideas
- ☐ Professionally Evil API Testing: GraphQL, SOAP, and REST Fundamentals and Techniques L
  Instructor: Secure Ideas
- ☐ Professionally Evil Application Security (PEAS): Mastering Application Reconnaissance and Mapping L
  Instructor: Secure Ideas
- ☐ Professionally Evil Application Security (PEAS): Mastering Client-Side Flaws and Exploitation L
  Instructor: Secure Ideas
- ☐ Professionally Evil Application Security (PEAS): Unveiling Server-Side Discovery and Exploitation L
  Instructor: Secure Ideas
- ☐ Professionally Evil CISSP Mentorship Program L
  Instructor: Secure Ideas
- ☐ Regular Expressions, Your New Lifestyle L OD
  Joff Thyer
- ☐ SOC Core Skills v3 L OD
  John Strand
- ☐ Zero to Linux L
  Hal Pomeranz

learn by doing for goodness sake!

Full Course Catalog

- ☐ Advanced Endpoint Investigations L OD
  Alissa Torres
- ☐ Advanced Network Threat Hunting L OD
  Chris Brenton
- ☐ Advanced Offensive Tooling L
  Chris Traynor
- ☐ Attack Emulation Tools: Atomic Red Team, CALDERA and More L OD
  Carrie Roberts
- ☐ Attack-Detect-Defend (ADD) L
  Kent Ickler & Jordan Drysdale
- ☐ Bash Scripting for Server Administration OD
  Bill Stearns
- ☐ Blue Team Foundations with Atomic Controls L OD
  Bryan Strand
- ☐ Breaching the Cloud L OD
  Beau Bullock ← allegedly the best beard in all infosec
- ☐ Cyber Security Incident Command L
  Gerard Johansen
- ☐ Cyber Threat Intelligence 101 L
  Wade Wells
- ☐ Defending the Enterprise L OD
  Kent Ickler & Jordan Drysdale
- ☐ Enterprise Attack: Initial Access ★
  Steve Borosh
- ☐ Enterprise Attacker Emulation and C2 Implant Development L OD
  Joff Thyer
- ☐ Enterprise Forensics and Response L OD
  Gerard Johansen
- ☐ Foundational Application Security Training (FAST) OD
  Kevin Johnson
- ☐ Foundational Data Protection Training (FDPT) L
  Bill McCauley
- ☐ HackerOps L OD
  Ralph May
- ☐ Hacking Active Directory: Fundamentals and Techniques L
  Dale Hobbs
- ☐ Hiring Handbook: How to Build an InfoSec Team that Gets Stuff Done OD
  Kip Boyle
- ☐ How to be Irresistible to Hiring Managers L
  Kip Boyle
- ☐ Incident Response Foundations L OD
  Derek Banks
- ☐ Intro to IoT Hacking L
  Rick Wisser & Dave Fletcher
- ☐ Intro to Offensive Tooling L OD
  Chris Traynor
- ☐ Introduction to Cybersecurity in Space Systems L
  Tim Fowler
- ☐ Introduction to Industrial Control Systems L OD
  Ashley Van Hoosen
- ☐ Introduction to Pentesting L OD
  John Strand the man, the myth, the legend (not the underwear model)
- ☐ Introduction to Python L OD
  Joff Thyer
- ☐ Linux Command Line For Analysts & Operators L OD
  Hal Pomeranz
- ☐ Linux Forensics L OD
  Hal Pomeranz
- ☐ Modern WebApp Pentesting L OD
  BB King
- ☐ MWAP 2: Webapp Internals L
  BB King
- ☐ Network Forensics and Incident Response L OD
  Troy Wojewoda
- ☐ Next Level OSINT L
  Mishaal Khan
- ☐ Offense for Defense L
  Jason Downey & Tim Medin
- ☐ OWASP Top 10 OD
  Jim Manico
- ☐ PECSEC Out of the Box: Strategies for Escaping from Containers OD
  Cory Sabol

rumor has it, these instructors are so good, even malware asks them for advice

- ☐ PowerShell for InfoSec: What You Need to Know OD
  Carrie Roberts
- ☐ Practical Physical Exploitation ★
  Ralph May & Travis Weathers
- ☐ Practical OWASP TOP 10 OD
  Kevin Johnson
- ☐ Practical Window Forensics OD
  Marcus Schober
- ☐ Professionally Evil Network Testing (PENT) L
  Instructor: Secure Ideas
- ☐ Ransomware Attack Simulation and Investigation for Blue Teamers L
  Markus Schober
- ☐ Red Team Fundamentals for Active Directory L
  Eric Kuehn
- ☐ Red Team: Initial Access L
  Michael Allen
- ☐ Reporting for Pentesters L OD
  BB King
- ☐ Securing the Cloud: Foundations L OD
  Andrew Krug
- ☐ Security Compliance and Leadership L OD
  Chris Brenton
- ☐ Security Defense and Detection TTX L
  Amanda Berlin & Jeremy Mio
- ☐ Security for MSPs OD
  John Strand
- ☐ SELinux L OD
  Hal Pomeranz
- ☐ Threat Hunting & Incident Response with Velociraptor L
  Eric Capuano & Whitney Champion

On-demand classes are being added regularly.
Please check the Antisyphon Training website for the most current information.

Level Up Your Team

- Customized training for any budget
- Subscribe to over 40 courses from our catalog
- Learn actionable new skills to secure your organization
- Live and virtual private training
- Track your team's progress with On-Demand courses
- Hands-on labs and Cyber Range access

Sign Up Today!

ANTISYPHON TRAINING
POWERED BY BHIS

Connect with the Antisyphon Community on Discord!

let's be friends, we're cool i promise

> Antisyphon has been a welcoming community to grow with. The instructors are experts in their fields. They take pride in their work and have a passion for teaching as many people as they can so the world can be a safer place overall. The discord server is a safe place to come as you are, fellow students are kind to one another, and though we all come from different backgrounds we find learning and cybersecurity to be our common ground upon which we help each other become better.
> **– *childofalliance***

just here for the fun handles (and memes)

> I appreciate being able to be a part of the Antisyphon community because it's absolutely welcoming and helps provide resources that are in dire need of accessibility for our future Security Professionals. I also appreciate the opportunity to give back and help others as a part of this amazing community!
> **– *SamunoskeX***

> The Antisyphon community embodies what it means to be a collaborative and helpful infosec group. Questions and requests for help result in healthy discussions without the edge of criticism and with the goal of ultimately providing an answer. To put it another way, the community has a general attitude of 'You got a problem, yo, I'll solve it.'
> **– *JOantom***

def didn't pay them to say nice things.

If Discord isn't your thing, here are some other ways you can keep up:

Get Hired: *linkedin.com/company/antisyphon-training*
Join the Discussion: *x.com/Antisy_Training*
Get Weekly Security Tips: *youtube.com/@AntisyphonTraining*
Read About What's Happening: facebook.com/antisyphontraining

Read past issues of PROMPT#
and Infosec Survival Guides!

Visit our online store for shirts, hoodies,
stickers, Backdoors & Breaches, comics,
zines, survival guides, hats, and more!

go ahead, scan it

BLACK HILLS
Information Security

890 Lazelle Street
Sturgis, SD 57785

Contact Us: 701-484-BHIS or info@promptzine.com

PRINTED IN CANADA. SECOND PRINTING.

Join the Community!

MADE BY AND FOR THE COMMUNITY

Learn More:

Everything You Need to Survive in Infosec (almost)

Ok, not quite... but still plenty of useful stuff. Check out our Yellow Book for additional topics, or submit your own article for the future PROMPT# zines and Infosec Survival Guides.

Articles Covering:

Soft Skills:

- Setting Smart Goals
- Leading Tabletops
- How to Play B&B
- Hiring

Technical Skills:

- Common Cyber Threats
- Use Your Home Lab
- OSINT
- Understanding GRC
- Malware Analysis
- Cloud Security
- Network Engineering
- IT Help Desk

...and more!

With Special Contributions:

IT Help Desk with **Sean Reilly**

Malware Analysis with **John Hammond**

Leading Effective Tabletops with **Glen Sorenson**

and MEEEE the scribble voice from the GREAT BEYOND

Brought to you by:

BLACK HILLS | Information Security

ANTISYPHON TRAINING — antisyphontraining.com

wildwesthackinfest.com

ACTIVE COUNTERMEASURES — activecountermeasures.com

REKCAH — rekcahcomics.com

PROMPT# — promptzine.com

bhis.co