BISHOPFOX

EBOOK

GREATEST HITS

A Compilation of Our Favorite Offensive Testing Tools

Table of Contents

Introduction

What's better than a Top 10 List? An ultimate guide of all our favorite lists – from red team and cloud penetration tools TO our favorite music to hack to and the best reads for your offensive security journey.

At Bishop Fox, not only do we love hacking all the things, but sharing that knowledge with our peers is just as fun! We've got you covered to level up your pen testing game with this comprehensive cheat sheet of hacking goodies. Whether you know pen testing like the back of your hand or are just getting your feet wet, this guide will offer you something to expand your knowledge base for conducting the most comprehensive, optimum, in-depth security engagements.

If you've been considering 'making it official' with pen testing as a profession, we included a Training and Certifications section to guide you on your education journey. If the non-cert route is more your style, check out our helpful tips to map out your own customized pen testing career adventures to make you equally competitive on the job market.

MUSIC TO HACK TO

Perhaps even more impactful than the legacy of the movie "Hackers" was the three-volume soundtrack the movie produced. That sprawling soundtrack highlighted '90s electronic musical pioneers like Orbital and The Prodigy and even some more unlikely cuts featuring David Bowie and Squeeze.

To this day, many Bishop Fox security consultants rely on various hacking music playlists to help them stay in the zone during engagements. Here are a few of our recommendations; for a comprehensive list, check out 'Music To Hack To'.

Mnq026
by Survive

Night Light
by The Cancel

III
by BadBadNotGood

Trance 2022
by Planet Punk Music

And hacking in silence is no fun, so check out our music playlists for some acoustic accompaniment!

TOOLS YOU'LL WANT TO USE

TOP TOOLS
FOR PEN TESTING

With so many hacking tools to choose from, we find it handy to keep a running list of our must-have tools that all pen testers should know about and why they are so useful. We hope our list of favorites helps you wherever you may be on your hacking journey.

01 FEROXBUSTER

Creator: Ben 'epi' Risher (@epi052)

"A fast, simple, recursive content discovery tool written in Rust."

WHY WE LIKE IT:

We've written about GoBuster before, and this forced browsing tool is similar (forced browsing is a type of an attack where you seek out resources that the targeted web application does not display or reference). But unlike GoBuster, this tool uses Rust instead of Go, which makes it a bit different. And unlike GoBuster, Feroxbuster is a recursive tool. Lastly, Feroxbuster is super simple to install and use, and those features alone make it an invaluable asset.

02 EYEBALLER 2.0

Creator: Dan Petro (@2600AltF4) and Gavin Stroy (both of Bishop Fox)

"An AI-powered, open-source tool designed to help penetration testers assess large-scale external perimeters."

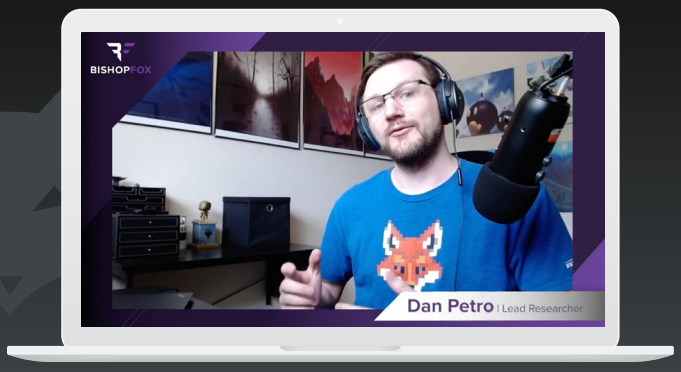
WHY WE LIKE IT:

If you want to cut down on time on your security engagements spent scrolling through screenshots for something promising that could yield a vulnerability or two, then check out Eyeballer. We just released an updated version of this award-winning tool with a cleaner, easier-to-use web interface, so there's no time like the present to give it a shot.

PAUSE MUSIC

Bishop Fox Lead Researcher Dan Petro shares how it works in this explainer video.

WATCH VIDEO >



03 NUCLEI

Creator: ProjectDiscovery

"Fast and customizable vulnerability scanner based on simple YAML based DSL."

WHY WE LIKE IT:

Nuclei is one of our favorite tools to run more speedy, efficient, customized, AND accurate multi-protocol vulnerability scanning. As our customers' security architecture inevitably changes over time and attack surfaces broaden, Nuclei templates provide a single source of truth to help reduce the noise and focus on the vulnerabilities at hand.

PAUSE MUSIC

ProjectDIscovery and Bishop Fox come together in this webcast to take a dive into Nuclei.

WATCH WEBCAST >

04 AUTOVNET

Creator: autovtools

"Provides simple, performant, intuitive, internet-scale IP network simulation empowering Cyber Range administrators and virtual Red Teamers to provide unprecedented realism in adversary emulation for "Red vs. Blue" cyber exercises and competitions."

WHY WE LIKE IT:

The description gives the gist, but here's a slightly more in-depth overview. Autovnet will help you to shore up your red team skills in a simulation environment. Use it to practice scenarios to build both red team and blue team techniques. As a bonus, if you're into CTFs, this tool is great for improving your skills on that front, too.

05 RIPGEN

Creator: resync

"Rust-based high performance domain permutation generator."

WHY WE LIKE IT:

Permutations are really good way to discover new subdomains that other tools miss, but you have to be careful of how much data you feed tools like Ripgen, since their output seems to grow almost exponentially. If you have a list of more than 1.000 subdomains, be prepared for this process to take a looooooong time.

PAUSE MUSIC

Justin Rhinehart, Senior Analyst & Joe Sechman, AVP of R&D at Bishop Fox walk you through why ripgen one of our favorite open-source tools.

WATCH WEBCAST >

06 IAM VULNERABLE

Creator: Seth Art (@sethsec) of Bishop Fox

"An open-source tool designed to help penetration testers and security practitioners better understand how to identify and exploit common IAM misconfigurations that allow for privilege escalation."

WHY WE LIKE IT:

Besides being the product of Bishop Fox research, IAM Vulnerable is an excellent way to try out AWS privilege escalation techniques in a low-risk environment. Want to level up your cloud pen testing skills? Then this is a tool you must check out ASAP. Besides being the product of Bishop Fox research, IAM Vulnerable is an excellent way to try out AWS privilege escalation techniques in a low-risk environment. Want to level up your cloud pen testing skills? Then this is a tool you must check out ASAP.

07 BAD PODS

Creator: Seth Art (@sethsec) of Bishop Fox

"A collection of manifests that will create pods with elevated privileges."

WHY WE LIKE IT:

Bad Pods is the collection of Kubernetes privilege escalation manifests from Seth Art. Get a better sense of what can go wrong with common Kubernetes misconfigurations – something that can benefit both penetration testers and security administrators.

08 SUBFINDER

Creator: ProjectDiscovery (@pdiscoveryio)

"A subdomain discovery tool that discovers valid subdomains for websites."

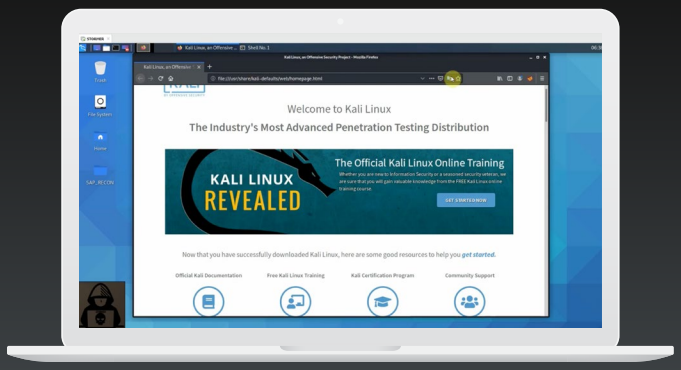
WHY WE LIKE IT:

ProjectDiscovery has some amazing tools – last year's pen testing tools blog included the vulnerability scanner Nuclei, which remains a great tool you should try if you haven't already. Subfinder comes in handy for quickly discovering additional attack surface, which is always a good thing when you're hunting for vulnerabilities.

PAUSE MUSIC

Watch how the latest versions of the Subfinder works in this short video.

WATCH VIDEO >



09 SEMGREP

Creator: r2c (@r2cdev)

A fast, open source, static analysis tool for finding bugs and enforcing code standards at editor, commit, and CI time."

WHY WE LIKE IT:

We chose this powerful yet lightweight tool because of its speed and flexibility. Spend more time exploiting impactful bugs and less time searching for them in the first place. Plus, Semgrep makes it easy to write custom rules to detect client-specific code patterns that could prove problematic. It might be easy to assume this tool is merely a glorified version of Grep. However, Semgrep understands the code it's examining so it's incredibly useful when you're searching for complicated patterns.

10 BONUS RESOURCE: PHONERATOR

Creator: Martin Vigo (@martin_vigo)

A fast, open source, static analysis tool for finding bugs and enforcing code standards at editor, commit, and CI time."

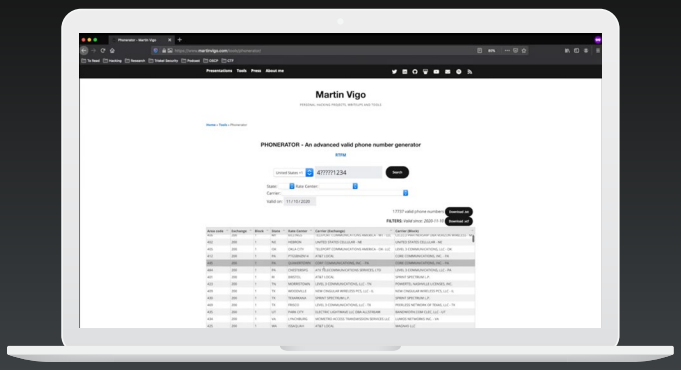
WHY WE LIKE IT:

Last month, we shared a list of OSINT tools on our blog. Martin Vigo was the creator of one of those tools and he directed our attention to Phonerator, which is another useful OSINT resource of his. We haven't played around with it too much, but it seems promising for a social engineering engagement or phishing campaign.

PAUSE MUSIC

Watch Martin Vigo himself walk you through the Phonerator in action.

WATCH VIDEO >



Now that we've got our general pen testing tools covered, let's move on to more specialized tools that help practitioners focus on reconnaissance, cloud pen testing, red teaming, and the pot of gold at the end of the rainbow – post exploitation!

TOP OSINT TOOLS FOR RECONNAISANCE

Looking to level up your open-source intelligence (OSINT) efforts for your next security engagement? There's no shortage of OSINT tools, techniques, and other resources – in fact, there's so much stuff, it's a little overwhelming to try and sort through it all. Writing a "best of" or otherwise "cumulative" list would be a futile endeavor, so instead, we compiled nine OSINT tools and other miscellaneous resources we find useful.

01 TRACE LABS OSINT VM VERSION 2

Creator: Trace Labs (@TraceLabs)

WHY WE LIKE IT:

Trace Labs is a nonprofit that has quite the name in the OSINT world – the mission of the organization is to help find missing people and reunite them with their families **(more on that here).** They have other available OSINT resources, but we wanted to focus on the OSINT Virtual Machine (v2). This VM is the go-to for all OSINT engagements. The VM comes with an incredibly expansive list of tools that allow you to quickly and easily get up and running in a dedicated environment.

02 OSINT FRAMEWORK

Creator: Justin Nordine (@jnordine)

WHY WE LIKE IT:

No OSINT tool list would be complete without the OSINT Framework. The OSINT Framework contains resources for finding information about targets via social networking, instant messaging, metadata, and more. From these categories, you can narrow your search further and even further. No matter what kind of information you're seeking, the OSINT Framework more than likely has a resource for you.

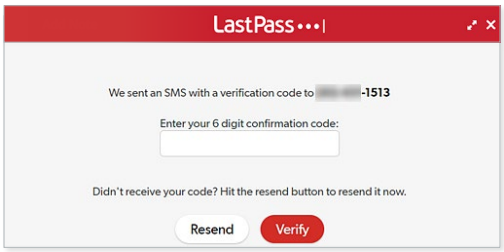
03 EMAIL2PHONENUMBER

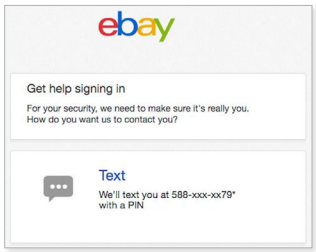
Creator: Martin Vigo (@martin_vigo)

WHY WE LIKE IT:

The name of the tool says it all; you just need a target's email address, and with that information alone, it's possible to retrieve their phone number. The tool works several different ways. It scrapes websites for phone number digits (initiating password resets via the email address), generates phone numbers based on the country's Phone Numbering Plan, and brute-forces by iterating over a list of numbers and initiating password resets to obtain associated email addresses.

Like the other OSINT tools on this list, it depends on publicly available data. For more information on how email2phonenumber works, BSides Las Vegas 2019 presentation.





04 SPIDERFOOT

Creator: SpiderFoot (@SpiderFoot)

WHY WE LIKE IT:

Automation can be an invaluable asset in security (as this blog post from Zach Zeitlin illustrates). SpiderFoot applies automation to OSINT. It can make your OSINT efforts much faster and much more powerful; it even works while you sleep! Introduced to the world in 2005, SpiderFoot has kept foot (pun intended) with the times, as today's attack surface is significantly vaster than the attack surface of nearly 20 years ago. There are two ways to use SpiderFoot; you can get the open-source version or the HX version.

05 PHONEBOOK.CZ

Creator: Intelligence X (@_IntelligenceX)

WHY WE LIKE IT:

With Phonebook.cz, you enter a website domain or subdomain – and voila! It returns a list of related email addresses. This is certainly a useful OSINT tool to have in your back pocket, especially if you're on an engagement that requires social engineering prowess. Intelligence X, the security company behind Phonebook, is also responsible for several other OSINT tools that are worth your time.

06 SUBLIST3R

Creator: Ahmed Aboul-Ela

WHY WE LIKE IT:
Have you ever needed to find the subdomains of a target domain? If so, this is the tool for the job. sublist3r is a Python-based tool that quickly enumerates subdomains. This tool is designed for security engineers and developers to identify assets that are otherwise unknown. sublist3r leverages search engines such as Google, Yahoo, and Bing to find subdomains that have been mapped on other websites. This tool also has the option to brute-force subdomains via a wordlist, which comes in handy for finding otherwise hidden subdomains!

07 THEHARVESTER

Creator: Christian Martorella

WHY WE LIKE IT:
There are few OSINT tools – or pen testing tools in general – as well regarded in the security community as theHarvester. And with good reason; when provided a domain or company name, this tool proceeds to gather email addresses, names, subdomains, IPs, and URLs. All the information it grabs can be found on an organization's external footprint.

08 GITGOT

Creator: Jake Miller (@TheBumbleSec)

WHY WE LIKE IT:
Former Bishop Fox Researcher Jake Miller created several popular tools in his tenure here (such as GadgetProbe and RMIScout), and GitGot was his contribution to the world of OSINT. GitGot is a semi-automated, feedback-driven tool designed to scour public GitHub data for sensitive secrets. This tool can significantly reduce time spent searching for promising leads while testing, bringing you the information you need to get the most impact.

09 KARMA_V2

Creator: Dheerajmadhukar (@Dheerajmadhukar)

WHY WE LIKE IT:
Karma touts that it offers pen testers and other security researchers the ability to comb through "deep information, more assets, WAF/CDN bypassed IPs, internal/external infra[structure], publicly exposed leaks" for info about a particular target. Leaks it searches in include WordPress, CloudFront, Jenkins, and Kubernetes. One caveat about Karma_v2 is that it requires premium Shodan access to use (which is helpful to have anyway if you can spend the money).

OTHER OSINT RESOURCES TO EXPLORE

Aside from these aforementioned tools, there are many other resources available to help enhance your OSINT skills. If you're just starting out, give the CIA guide **"Sailing the Sea of OSINT in the Information Age"** a read. Also, be sure to read **"Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise"** by the Rand Corporation.

Finally, it's worth iterating that OSINT is a discipline. There are plenty of techniques for finding people, assets, and information on the internet. The OSINT community is expansive, and used among security researchers, IT personnel, and **even law enforcement.** In fact, as alluded to earlier, OSINT is often used to help **find missing people** – making it an extremely beneficial discipline to add to your repertoire.

TOP TOOLS FOR SUCCESSFUL RED TEAMING

Have you ever wondered how Red Teams are able to emulate the world's most formidable cyber adversaries? Look no further than this comprehensive list of top tools supporting successful red team offensive security engagements. If you need to exploit vulnerabilities to magnify even the smallest hairline fractures in a customer's infrastructure, this list should be handy.

01 CURSEDCHROME

Creator: @IAmMandatory

ITS USE:
Just like it sounds, this tool is a riff on the Google Chrome browser – essentially, it allows you to turn a victim's browser into a proxy for testing.

WHY WE LIKE IT:
CursedChrome makes it easy to emulate a malicious browser extension during a red teaming engagement. Use it to hijack Chrome browsers, bypass most 2FA or other security protections that might be in place, and ride cookies to reach any web-based targets.

02 UNIVERSAL LOADER

Creator: @symbolcrash1

ITS USE:
Universal Loader is a Golang library you can use across multiple platforms (Linux, Windows, and OSX) to load shared libraries from memory and without CGO.

WHY WE LIKE IT:
Universal Loader's ability to jump across popular platforms is certainly appealing, but it's not the only reason we like using it. It even can be used on the new Apple M1 chip. Also, worth calling out is that this Golang library does not use memfd, which makes it the first Golang Linux loader to do so. For those two reasons alone, Universal Loader is a fairly impressive red team tool.

03 OVERLORD

Creator: QSecure Labs

ITS USE:
Overlord is a Python-based console command-line interface for automating red teaming infrastructure.

WHY WE LIKE IT:
It's important to be able to quickly spin up secure infrastructure as needed during red team engagements, and Overlord is without a doubt an amazing asset to have in your back pocket for such instances. This tool will save you a lot of time, which you can then put toward doing some actual hacking – you know, the fun stuff.

04 SLIVER

Creator: @LittleJoeTables and @rkervell

ITS USE:
Sliver is a cross-platform general purpose implant framework written in Golang.

WHY WE LIKE IT:
This tool is the brainchild of two Bishop Fox researchers, so our bias may be showing. And it is like the popular commercial tool Cobalt Strike (which is a terrific pen testing tool in its own right). What makes Sliver noteworthy is features like dynamic code generation with per-binary obfuscation, multiple and extensible egress protocols, and support for numerous operators simultaneously controlling implants. Plus, it's easy to use and it works fast.

05 GITHOUND

Creator: @tillson

ITS USE:
Use Githound to locate exposed API keys and other sensitive information floating around GitHub. The tool works via pattern matching, commit history searching, and "a unique result scoring system."

WHY WE LIKE IT:
Secret snatching tools like Githound aren't exactly uncommon, but that doesn't make this tool (or others like it) any less valuable. Some possible use cases for Githound include detecting exposed customer API keys as well as employee API tokens. If you do bug bounties at all, this tool is useful to have bookmarked – some people have reported earning thousands of dollars in bounties thanks to it.

06 ACTIVE DIRECTORY LAB SETUP TOOL

Creator: @browninfosecguy

ITS USE:
This tool's title says everything – this tool allows you to easily set up a lab for Microsoft Active Directory in PowerShell.

WHY WE LIKE IT:
It's quick, and it works well. You can use this tool to make sure any exploits you're using against Active Directory are perfected before introducing them to a client's environment. It's also great for pen testers who simply want to become more comfortable testing Active Directory.

07 STORMSPOTTER

Creator: Microsoft Azure Red Team

ITS USE:
You can better visualize an Azure attack surface with Stormspotter; this tool helps you graph Azure and Azure Active Directory objects.

WHY WE LIKE IT:
If you're at all familiar with the popular pen testing tool BloodHound, then you'll love Stormspotter. Stormspotter's concept is similar, except this tool is designed for Azure environments. And who better to trust for comprehensive Azure hacking tools than the team behind the cloud platform themselves (or, more specifically, their red team?)

08 ECG

Creator: @Void_Sec

ITS USE:
Unlike the majority of the tools on this list, ECG is actually a commercial tool. This tool is a "Static Source Code Scanner able to analyze & detect real and complex security vulnerabilities in TCL/ADP source-code."

WHY WE LIKE IT:
ECG is one powerful tool that fills a surprisingly vacant niche. As VoidSec notes on their official write-up, TCL code is fairly pervasive; so being able to thoroughly analyze it for vulnerabilities can be incredibly helpful. There aren't many other tools out there that fit this unique need, commercial or otherwise.

09 DUMPSTERFIRE

Creator: @TryCatchHCF

ITS USE:
Described as a "Security incident in a box!," you can use DumpsterFire to build "time-triggered, distributed" security events to test both red team offenses and blue team defenses.

WHY WE LIKE IT:
Not only does DumpsterFire take your traditional tabletop exercises to the next level, it uses automation to help you effectively multitask during engagements (and sidestep some of the more tedious stuff). And the degree of customization that DumpsterFire permits is impressive; you can truly tailor a simulated security incident to meet one-of-a-kind circumstances.

The above list consists of only nine of the red teaming tools we've found useful while conducting our engagements. There are countless other tools to explore, but hopefully these can give you a running start – and something of an edge on your next red team engagement.

TOP TOOLS TO SHOWCASE

POST-EXPLOITATION EFFORTS

After exploiting a vulnerability and getting inside a network on an engagement, we often want to show what trophies we can collect as a way of demonstrating impact to the client. To tackle these post-exploitation efforts, we regularly leverage various tools to improve our efficiency.

01 GHOSTPACK

Creator: SpecterOps (@SpecterOps)

ITS USE:
With the powerful post-exploitation toolset GhostPack, you can do all kinds of things; you can attack KeePass 2.X databases, copy locked files, tamper with Active Directory certificates, and more.

WHY WE LIKE IT:
GhostPack is sort of a "one-stop shop" for your hacking needs. Among the 13 tools it contains are the enormously useful Rubeus, Seatbelt, and SharpUp. Rubeus is a C# toolset that interacts directly with the Kerberos protocol in Active Directory environments, allowing you to directly communicate with Kerberos attributes like tickets and general authentication that you can then leverage to move around a network. Seatbelt is a C# project you can use for security-oriented host "safety checks," and SharpUp is a C# tool that identifies local privilege escalation paths. These tools are used by countless red teamers and network pen testers. If you're not using them already, there's no time like the present to start!

02 MIMIKATZ

Creator: Benjamin Delpy (@gentilkiwi)

ITS USE:
Mimikatz can help you extract passwords and other credentials from Windows environments. It is an extremely popular pen testing tool, having existed for over a decade. But Mimikatz is regularly maintained and updated, ensuring that it remains a cutting-edge asset.

WHY WE LIKE IT:
Think of Mimikatz as a Swiss Army knife for network pen testing. It comes with several built-in tools and is useful for Kerberoasting, password dumping, you name it, Mimikatz can probably do it. And Mimikatz isn't just for the offensive security professionals out there – defensive security teams can benefit from it, too (which also bodes well if you find yourself in a purple team scenario).

03 METASPLOIT

Creator: The Metasploit Project (@metasploit), operated by Rapid7 as a collaboration with the open-source community.

ITS USE:
Metasploit is arguably the world's leading penetration testing framework, created by H.D. Moore in 2003. Metasploit includes modules for just about every phase of a pen test, which helps with its popularity. It includes ~250 post-exploitation modules that can be used for capturing keystrokes, gathering information on your network, displaying operating system environment variables, and so on.

WHY WE LIKE IT:
Metasploit's post-exploitation modules are vast, but one module sticks out above them all – the Meterpreter payload. Meterpreter allows you to explore the targeted system, and execute code, and since it works via in-memory DLL injection, you don't risk leaving behind any evidence of your actions. Metasploit's post-exploitation capabilities are also extremely versatile, with modules for Windows, Linux, and OS X.

04 POWERHUB

Creator: Adrian Vollmer (@mr_mitm)

ITS USE:
This post-exploitation tool is intended to help you bypass endpoint detection and application blocklisting.

WHY WE LIKE IT:
You can use PowerHub to transfer files without alerting any security protections in your testing environment, which will make your next pen test smoother and easier. Stay a step ahead of Windows Defender with this tool.

05 LOLBAS AND LLOLBAS

Creator: The LOLBAS Project and the Arizona Security Engineering and Research Group

ITS USE:
LOLBAS is a dictionary for finding possible privilege escalation paths using binaries on Windows machines. LLOLBAS is the ingestor that works in conjunction with LOLBAS. The ingestor finds all the binaries on the LOLBAS list that are on the Windows machine so you're not guessing or sorting through the list trying to find them (which can be tedious).

WHY WE LIKE IT:
The LOLBAS Project helps you to search for possible privilege escalation paths on your machine whereas LLOLBAS allows you to tailor those paths to the specific machine. With these two tools combined, you are (almost) unstoppable on an engagement. And as an added benefit, it's convenient to have offline tools available if a situation arises that demands them.

06 PHPSPLOIT

Creator: @nil0×42

ITS USE:
PHPSploit acts as a full-featured C2 framework, silently persisting on web servers via a single-line PHP backdoor.

WHY WE LIKE IT:
PHPSploit is a terrific asset to have on hand for your next offsec engagement – it's efficient, it's user-friendly, and it works quietly. As its GitHub description states, PHPSploit is designed "by paranoids, for paranoids."

07 SWAP_DIGGER

Creator: Sevagas

ITS USE:
You can use swap_digger for automating Linux swap analysis during post-exploitation or forensics.

WHY WE LIKE IT:
All kinds of good stuff can be found in Linux swap spaces – everything from passwords and email addresses to GPG private keys. Swap_digger can help you comb through these swap spaces and find high-impact trophies that will make your assessment more successful.

08 BASHARK

Creator: RedCode Labs

ITS USE:
Bashark is a post-exploitation toolkit that – as the name implies – is written in the programming language Bash. It's a simple script that can yield big results.

WHY WE LIKE IT:
Bashark works quickly and stealthily, allows you to add new commands by creating Bash functions, and cleans up any traces that might be left behind after using the script in your target environment – so it's like you were never there.

09 BEROOT PROJECT

Creator: AlessandroZ

ITS USE:
Use the BeRoot Project to find common misconfigurations that can be leveraged for privilege escalation in Windows, Linux, and OS X environments.

WHY WE LIKE IT:
Identifying common misconfigurations is one of the most surefire ways to get a foothold into the network, so the faster you can find these misconfigurations the better. And the BeRoot Project helps immensely on that front.

It supports the major cloud computing providers: AWS, Azure, Google Cloud, Alibaba Cloud, and Oracle Cloud. That means this is one extremely versatile tool. Plus, ScoutSuite was designed to make assessing cloud environments much easier, providing the user "a clear view of the attack surface automatically," saving significant time.

PEN TESTING TOOLS FOR THE CLOUD

You spoke, and we listened! A list that focused on the cloud was the clear crowd favorite when we polled our social followers. So that being said, we collected nine of our favorite tools for cloud pen tests.

01 WEIRDAAL: AN AWS ATTACK LIBRARY

Creator: Chris Gates (@carnal0wnage)

WHY WE LIKE IT:
One thing I love about infosec is the names people come up with for tools and talks, this being an example. That aside, Gates describes one of WeirdAAL's two overarching goals to be a repo of useful defensive and offensive security functions for AWS, making it a resource you'll want to bookmark. And if you find yourself in a more black box testing scenario, WeirdAAL is a perfect choice.

02 SCOUTSUITE: A MULTI-CLOUD SECURITY-AUDITING TOOL

Creator: NCC Group (@NCCGroupplc)

WHY WE LIKE IT:
It supports the major cloud computing providers: AWS, Azure, Google Cloud, Alibaba Cloud, and Oracle Cloud. That means this is one extremely versatile tool. Plus, ScoutSuite was designed to make assessing cloud environments much easier, providing the user "a clear view of the attack surface automatically," saving significant time.

03 GITOOPS: ALL PATHS LEAD TO CLOUDS

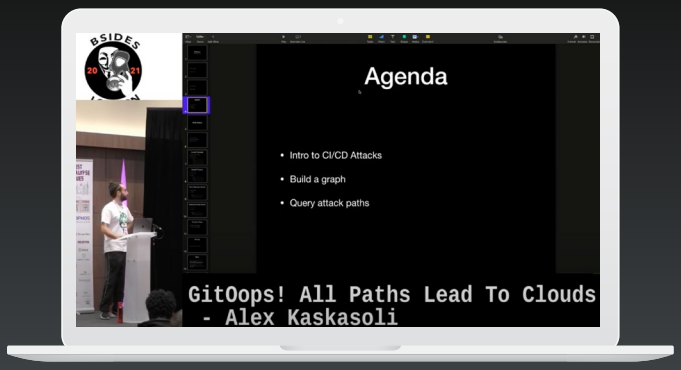
Creator: OvoTechnology

WHY WE LIKE IT:
As teams scale, it becomes more difficult for security departments to monitor GitHub repos. This is where GitOops comes in, as the tool leverages the literal GitHub "oops." Another well-named tool, you can use GitOops to find privilege escalation paths as well as for lateral movement in GitHub.

PAUSE MUSIC

Watch Alex Kaskasoli explore lateral movement and privilege escalation in a GitHub organization.

WATCH VIDEO >



04 S3SCANNER: SCAN FOR OPEN AWS S3 BUCKETS

Creator: Dan Salmon (@bltjetpack)

WHY WE LIKE IT:
You can use this tool during a black-box assessment to dump AWS S3 buckets, which are bound to contain valuable information. S3Scanner allows the user to automate the search for public resources available in different clouds and dump the information, not just in AWS but in other cloud services like DigitalOcean, too.

P.S. If you want to learn more about testing Azure environments, we recommend his book "Penetration Testing Azure for Ethical Hackers."

05 MICROBURST: ASSORTED SCRIPTS FOR AZURE SECURITY

Creator: NetSPI (@NetSPI)

WHY WE LIKE IT:
This is your one-stop shop for everything Azure related. You can use it for Azure services discovery, configuration auditing, and post-exploitation. This handy toolkit was created by Karl Fosaaen, an expert in cloud pen testing and an excellent resource when it comes to testing Azure environments.

06 SKYARK: DISCOVER THE MOST PRIVILEGED CLOUD USERS

Creator: CyberArk (@CyberArk)

WHY WE LIKE IT:

Available for Azure and AWS, this is a useful tool for identifying additional attack surface. Specifically, the tool is designed to detect the presence of cloud shadow admins, a very real threat to cloud environments (making it worthwhile for defenders to keep around, too.)

07 ROADTOOLS: FRAMEWORK FOR INTERACTING WITH AZURE ACTIVE DIRECTORY (AD)

Creator: Dirk-jan (@_dirkjan)

WHY WE LIKE IT:

This entry is both a library and an exploitation tool. The library is meant to authenticate with AD; alternatively, you can use it to build tools that integrate with a database containing ROADrecon data. The tool meanwhile is for deeper exploration of AD; there's a lot of data to sift through in AD, and ROADTools can help you make sense of it.

Other similar tools you can check out are PMapper, which is designed for AWS environments, and this Google Cloud privilege escalation toolkit by Rhino Security Labs.

PAUSE MUSIC

Watch Dirk-jan Mollema presenting the Roadtools framework. Additional details in his blog.

WATCH VIDEO >

08 POWERZURE: POWERSHELL FRAMEWORK FOR AZURE SECURITY

Creator: Ryan Hausknecht (@Haus3c)

WHY WE LIKE IT:

It's multifaceted: It can be used for reconnaissance and post-exploitation. So, you can use it to kick off an engagement and bring things to a close. Couple this with AzureHound and your testing should go seamlessly!

ADDITIONAL RESOURCES FOR ENHANCING YOUR CLOUD PEN TESTING SKILLS

These aren't pen testing tools per se, but they are incredibly useful and robust resources. The shared purpose of all three of these interfaces is to act as a "mission control" for their specific cloud platform, providing all kinds of tools for interacting with the platform.

AWS Command Line Interface
AWS CLI is a unified tool that provides a consistent interface for interacting with all parts of Amazon Web Services. AWS CLI commands for different services are covered in the accompanying user guide, including descriptions, syntax, and usage examples.

GO TO RESOURCE >

Azure Command-Line Interface
The Azure CLI is a set of commands used to create and manage Azure resources. The Azure CLI is available across Azure services and is designed to get you working quickly with Azure, with an emphasis on automation.

GO TO RESOURCE >

Cloud SDK & gcloud CLI
Libraries and tools for interacting with Google Cloud products and services. Learn how Google Cloud's tools can help you accomplish tasks effectively, and establish powerful workflows across whichever OS you use.

GO TO RESOURCE >

If you're interested in upping your cloud game, here are some additional resources to take a crack at and build your skillset.

Hacking the Cloud
This is a volunteer-run encyclopedia for helping security professionals learn various cloud security attacks, techniques, and tactics.

GO TO RESOURCE >

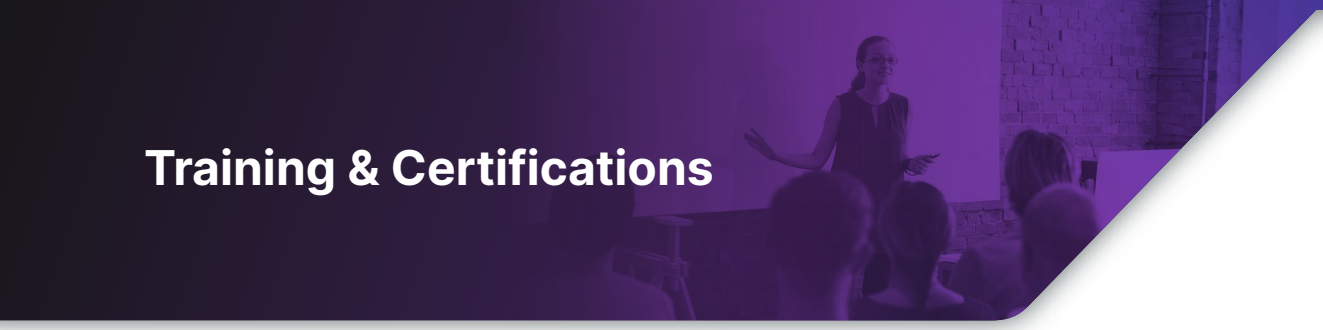
CloudSecDocs
Not only does this website contain a vast array of information (like cheat sheets) on cloud security technologies, but it's also solid for resources related to security culture and leadership.

GO TO RESOURCE >

Cloud Security Wiki
Finally, this site aims to be the place to go for all things cloud security. So, we couldn't do a proper cloud security blog without giving a shoutout!

GO TO RESOURCE >

Training & Certifications



Now, this is where this guide becomes a security cert "choose your own adventure." If you are still interested in getting a security cert, keep reading for a breakdown of some of the most popular and common certs. If you decide, certs aren't for you, we also dive into some alternatives (like finding a cybersecurity mentor) to earning a cert that can still help boost your skillset and make you more appealing to potential employers.

POPULAR AND COMMON SECURITY CERTS

C|EH™
CERTIFIED ETHICAL HACKER

The Certified Ethical Hacker (CEH) is issued by the EC-Council, a security training-centric organization. The CEH is a good "starter" cert, so it's a perfect option if you're just getting your feet wet in security. Once you have the CEH to your name, you can then move on to more advanced certs like the OSCP and SANS certs. You can attempt to earn a CEH with or without official training from the organization. If you choose to forgo the training, you'll need to pass an application process before taking the official CEH exam. You'll also need to show proof that you have two years of security experience. The proctored CEH exam is four hours long, and costs approximately $1200. Once you become a CEH, expect to renew your cert every three years for $80.

OFFENSIVE® security

The Offensive Security Certs: OSCP/OSWP/OSWE/OSED/OSEP (formerly OSCE). This group of certs is offered by the Offensive Security organization, which is responsible for popular security projects such as ExploitDB and Kali Linux.

- Easily the most well-known of the Offensive Security family of certs, the Offensive Security Certified Professional (OSCP) is highly sought-after. It costs anywhere from $1200 to $2148 depending on the package you pick. You'll need to complete a 24-hour proctored exam in a lab environment to obtain this cert. The OSCP exam is fairly difficult for anyone who is just starting out in security, but the good news about the OSCP is that it doesn't require renewal. You'll spend a significant amount of time preparing for the OSCP – anywhere from several weeks to several months.
- The OSWP (Offensive Security Wireless Professional) is less expensive than other certs, but more for folks interested in network pen testing or wireless security.
- The OSCE (Offensive Security Certified Expert) was the next step after the OSCP, but it's been retired as of 2020 (although the cert remains valid for anyone who previously earned it). The OSCE has since been broken into smaller certs: the OSED, the OSWE, and the OSEP. The OSED (Offensive Security Exploit Developer) is an "intermediate exploit development cert" that will cost you $1200 - $1500. The OSWE (Offensive Security Web Expert) consists of passing a 48-hour proctored exam and will run around the same price as the OSED. And the OSEP (Offensive Security Experienced Penetration Tester) is similarly priced to the OSWE/OSED and earned by passing a 48-hour proctored exam. Like the OSCP, none of the other Offensive Security certs require renewal, so once you are certified, you're set for life.

CISSP® | Certified Information Systems Security Professional

One of the older security certs available, the Certified Information Systems Security Professional (CISSP) is a cert you'll want to get if you aspire to be a security leader. This cert is intended to teach you how to "effectively design, implement, and manage a best-in-class cybersecurity program." So, if that sounds like something that aligns with your long-term career objectives, you'll want to pursue the CISSP. It's also worth noting that this is a cert more geared for those in the mid-level or senior stages of their security career, especially since you need five years of relevant experience in "two or more of the eight domains of the CISSP CBK" to even take the exam. Issued by the International Information System Security Certification Consortium or (ISC)², a CISSP will cost you a few thousand dollars in official training materials. The exam itself is priced at about $700 and lasts for six hours. As far as the overall time commitment, the CISSP seems to average people a few months of preparation. But once you earn the CISSP, you must pay dues to keep it ($85 per year). After three years, you'll either need to retake the exam to renew your CISSP or you'll need to invest in continuing education instead.

SANS

SANS GIAC Certs is one of the most reputable names in security training, so it would make sense that their certs carry a lot of weight. Some of the most in-demand SANS certs are the GIAC Penetration Tester (GPEN), GIAC Web Application Penetration Tester (GWAPT), GIAC Security Essentials Certification (GSEC), and the GIAC Cloud Penetration Tester (GCPN). The GPEN, GWAPT, and GIAC's purposes are more self-evident: They're technical deep dives into penetration testing. The GSEC though is meant to cover an array of security areas, like cryptography. These certs tend to be a similar difficulty level to the OSCP. The GPEN is approximately $2500 and should take about four months to complete. The GSEC is the same price and roughly the same timeframe, as is the GCPN and the GWAPT. All these certs will require continued renewal.

These are only a handful of the numerous available security certs out there. Something to keep in mind as you research and consider certs – no matter what kind – is that earning a cert is more of a means to an end than an actual end. All of these were created to help security professionals stay relevant in a constantly changing industry and substantiate their expertise. Continuous learning, though, is not only limited to the realm of certs. There are many other ways you can add to your "security portfolio," and stay on the cutting edge of the latest developments in the industry.

THE NON-CERT TRACK

You can entirely bypass earning any certs and still have a satisfying security career – and attract the attention of prospective employers. Here are some alternatives for bolstering your pen testing skillset (no matter what career stage you're in) without devoting time and money to certs.

BECOME INTIMATELY FAMILIAR WITH THE OWASP TOP 10

If you want to become an expert pen tester, one of the best places to start is gaining a deep familiarity with the **OWASP Top 10 list of vulnerabilities.** This will give you the fundamentals you need for success, as it will help you understand the most prevalent issues encountered in the security space.

PARTICIPATE IN BUG BOUNTY PROGRAMS

Get involved with one of the various bug bounty platforms once you're more comfortable with your pen testing skills. There's no better teacher than experience, and one of the best ways to gain experience as a hacker is the wonderfully legal world of bug bounties.

EARN CVES

This goes hand in hand with bug bounties but having a few CVEs to call out on your résumé significantly substantiates claims of your pen testing abilities. And don't fret if you're not finding the most glamorous 0-days right out the gate; even accruing low and medium-risk bugs is still a useful way to get started.

AUTHOR BLOG POSTS

Having a few write-ups to your name will nicely illustrate both your passion for and understanding of security. Don't pressure yourself to focus on novel research or groundbreaking techniques – even a well-written piece about a common vulnerability has value.

SPEAK AT CONFERENCES

This might be out of your comfort zone but give some serious consideration to submitting to conferences. You can always recycle a blog post as a compelling presentation, and you don't need to focus on the DEFCONs and Black Hats – even speaking at smaller conferences and meet-ups can add some color to your security resumé.

ENGAGE IN THE SECURITY COMMUNITY

Nowadays, there are so many ways to connect with other security professionals. Social media is a great asset on this front; infosec Twitter is fairly active, and there are **countless security Discords**, **Slack channels**, and **subreddits** you can join to broaden your horizons and expand your network. (Of course, we'd be remiss not to mention our own: **/redsec** subreddit and the **redsec Discord server**).

DEVOUR RELEVANT RESOURCES AS YOU FIND THEM

Online security courses like those offered on **Udemy** and **Coursera**, CTF platforms such as **VulnHub** and **HackTheBox**, books on security topics (see next section!), and even talks from yesteryear's security conferences can all prove beneficial in further fine-tuning your skillset.

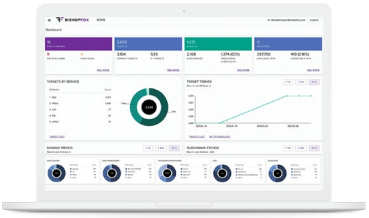
About Bishop Fox

Bishop Fox is recognized as the leading authority in offensive security, providing solutions ranging from continuous penetration testing, red teaming, and attack surface management to product, cloud, and application security assessments.

Over the past 16 years, we've worked with more than 25% of the Fortune 100, 8 of the top 10 global tech companies, and hundreds of other organizations to improve their security. Our award-winning Cosmos platform was named **Best Emerging Technology** in the 2021 SC Media Awards and our offerings are consistently ranked as "world class" in customer experience surveys.

Security isn't just a job to us. We do this because we love it — and because we're committed to the common good. In fact, we have authored 15 open-source tools, shared groundbreaking research, and published more than 50 security advisories in the last 5 years.

Cosmos



Cosmos proactively defends dynamic attack surfaces by combining advanced technology, automation, and expert-driven testing to continuously identify and remediate high-risk exposures before attackers even know they exist.

Leveraging a proprietary asset discovery and exposure reconnaissance engine, Cosmos continuously discovers and maps your ever-changing attack surface and identifies dangerous vulnerabilities targeted by attackers.

Acting as an extension of your security team, our operators provide deep insights into findings, deliver real-time answers to pressing questions, and conduct on-demand retesting to validate remediation procedures and accelerate the closure of attack windows.

Consulting Services

Network Security

Our experts simulate real-world attack scenarios, delivering deep insight into how skilled adversaries could establish network access and susceptible internal pathways that could put sensitive systems and data at risk.

Red Teaming

We utilize advanced offensive tools and tactics that mimic real-world adversaries to identify exploitable weaknesses in your organization while stress testing your incident responders and their playbooks for handling active, persistent attackers.

Cloud Security

Our service combines configuration review with objective-based penetration testing to identify vulnerabilities in public clouds, such as Amazon Web Services (AWS), Google Cloud Platform (GCP), and Microsoft Azure.

CONNECT WITH US

Get started today.

Are you ready to start "defending forward"? Get in touch with our offensive security experts today to explore solutions that meet your unique business needs.

Request a Meeting **Explore Cosmos**

22020601 © Bishop Fox. All rights reserved worldwide.

8240 S. Kyrene Rd. • Tempe, AZ 85284
480.621.8967
hello@bishopfox.com • bishopfox.com