

Ready, Steady, Hack

1\2 day class

Basic Track

The routine, operational demands of a busy cybersecurity and IT department can often get in the way of good security strategy and leave you with little time to prepare for the decisions that really matter. If this sounds like your day-to-day, join this short, hands-on course. It's designed to take you temporarily out of the ring and put you into the mind of the adversaries targeting your organization so you can adopt a more calculated approach. Plus, you can get your hands dirty with our popular virtual labs and learn from experienced, practicing Penetration Testers with a legacy of training at Black Hat as you do it.

Who's it for?

- Security and IT decision makers (CISOs, Heads of, budget-holding managers, etc.)
- CTOs and development Team Leads
- Network Managers

(Note: this course is not suitable for technical practitioners, such as SOC analysts, Penetration Testers, and so on.)

Delegates must have the following to make the most of this course:

- Intermediate to advanced cybersecurity experience
- A good understanding of basic networking technologies
- Confidence using basic computer commands

Top 3 takeaways

- How to think like a real-world threat actor and plan your security tactics with the same offensive mindset
- Where to identify the “low hanging fruit” that’s creating high-risk vectors across your attack surface
- How single vulnerabilities can lead to a larger and more destructive attack chain

What you'll learn

This course uses a Defense by Offense methodology based on real world offensive research (not theory). That means everything we teach has been tried and tested on live environments and in our labs. By the end of the course, you'll understand how threat actors may:

- Gather information on your organization to identify exposures and prepare your tactics
- Exploit web application vulnerabilities to achieve Initial Access to your network
- Build attack paths to pivot across your environments
- Evade detection and maintain their foothold in your environments
- Pivot from system to system to gain access to your critical assets
- Harvest credentials and achieve root access

By stepping back to trace the behaviors displayed in many cyber attacks and learn more about the tools used, you can arm yourself and approach your security with the same combative mentality.

What you'll be doing

You'll be learning hands on:

- Spending over half the session (~55%) on lab-based exercises
- Using lab-based flows to explore and hack lifelike systems and environments
- Discussing the impact of the hacks and the security context around them with your course trainer

Why it's relevant

We created this course in response to a growing challenge facing many of our own customers. Across the board, CISOs and other security decision makers are finding that in being so caught up with day-to-day operational tasks, they're not performing the strategic work or providing the leadership needed to keep their organizations safe.

The best way to address the barriers getting in your way is to step back and refocus, which is what this course is designed to help you do. For half a day, drill into the mind of the threat actors you're up against so you can approach your defense with greater knowledge and deeper insight.

Unlike our technical courses, Ready, Steady, Hack isn't designed to blow your mind with complex, novel hacks that you'll never be able to replicate or apply context to in your organization. Instead, you'll be operating in a bespoke lab that uses commands to simulate many of the common behaviors of a real threat actor. We've identified some of the most popular techniques being used in the wild and modelled them so that you can see exactly why threat actors use them, how they're deployed against the types of systems you use, and how they would impact your organization.

What's in the syllabus

Note: our syllabuses are subject to change based on new vulnerabilities found and exploits released.

THE ENUMERATION PHASE

- Approaches to enumeration: opportunistic vs targeted
- IP and open port search engines
- Research-based Open-Source Intelligence Gathering (OSINT) techniques
- Vulnerability scanning
- Exercise: use OSINT to gather key information on your target

GETTING A FOOTHOLD

- Intro to Metasploit Framework (MSF)
- Search for auxiliary modules and exploits
- Exercise: use MSF to configure an exploit and get a reverse shell

ENUMERATING THE SYSTEM AND PIVOTING

- Find Privilege Escalation opportunities in Linux systems
- Enumerate internal network
- Pivot across internal systems

- Exercise: use shell to enumerate website host

TAKING A DIFFERENT APPROACH

- Server-Side Forgery (SSRF)
- Use AWS metadata API to obtain temporary credentials
- AWS CLI and list S3 buckets configuration
- Exercise: abuse SSRF vulnerability to access credentials

THE GREAT ESCAPE

- Cloud container risks
- Cloud orchestration risks
- How to abuse Docker socket
- Exercise: escape Docker container onto host OS

What you'll get

- Certificate of completion
- Learning pack: question & answer sheets, setup documents, and command cheat sheets

Course highlights

What delegates love:

- A mix of guided learning and hands on hacking: you'll be improving your knowledge from a wide range of sources.
- Individual access: you'll have your own environments to play with, enabling you to hack at your own speed.
- Real-world learning: where many of the leading cybersecurity training courses are based on theory, our scenario-led, research-based approach ensures you learn how real threat actors think and behave.
- Specialist-led training: you'll learn from highly skilled and experienced practicing penetration testers and red teamers.
- Up-to-date content: our syllabus remains so relevant and current, delegates come back year on year for more.
- Plenty of time for questions

Outcomes for delegates

This course is designed to refresh your understanding of how threat actors target your organization by simulating their techniques yourself. This will help you:

- Refresh your knowledge of threat actors, potential attack paths and vectors, and MITRE ATT&CK
- Identify potential gaps in your organization's risk posture
- Communicate a stronger case for securing your organization's on-premise and cloud practices
- Build a closer relationship with your technical team
- Understand the methodologies and techniques used by Penetration Testers your infrastructure
- Improve your understanding of the organisation's risk posture based on the frequency and severity of vulnerabilities identified
- Create a stronger case for securing your organisation's network admin and architecture practices