SANS The most trusted source for cybersecurity training, certifications, degrees, and research

GIAC CERTIFICATIONS

SEC550: Cyber Deception – Attack Detection, Disruption and Active Defense

6 Day Program	36 CPEs	Laptop Required

You Will Be Able To

- Know why cyber deception completely changes the information security game
- Use cyber deception to detect attackers on your network as much as 90% faster than traditional detection technologies
- Collect actionable threat intelligence and attack attribution information through the use of deception
- Create an environment where attackers need to be perfect to avoid detection, while you need to be right only once to catch them
- Actively engage attackers in real time
- Thwart attacks before attackers send a single packet towards your network
- Take back the advantage from attackers

Who Should Attend

- General security practitioners
- Deception planner
- Security decision makers
- Security program architects
- Incident responders
- Cyber defenders/blue team personnel
- Threat hunter
- Purple teamer
- Chief information security officer (CISO)
- Cybersecurity analyst/engineer

Traditional defensive controls are failing us. The time it takes for an attacker to go from initial compromise to lateral movement is rapidly decreasing while the time it takes to detect and effectively respond to breaches is measured in weeks or even months. Making the situation worse, studies such as the 2020 Ponemon Institute Cost of a Data Breach Report show a direct correlation between the time it takes to detect and respond to a breach and the cost of that breach to an organization; the longer it takes, the more a breach costs. To reduce risk, defenders need better ways to quickly detect adversary activity while also collecting information to facilitate faster and more effective response. Cyber deception is the solution for reducing this response time and minimizing cost.

The majority of detective controls in use today focus on looking for evil while attackers do a great job at appearing harmless or even invisible. Technologies such as anti-virus, application whitelisting, DLP, and firewalls can be circumvented with relative ease. A common solution is to change the detective strategy from looking for evil to looking for abnormal, however, attempting to normalize even fairly small computing environments can be both challenging and time consuming. Fortunately, there are alternatives.

Instead of attempting to normalize a production environment, what if we placed resources in that environment that have no production value or use? These resources could be user accounts, credentials, services, open ports, computers, or even complete networks. Because these resources are not part of normal production operations, normal can be defined as no interaction or no use. Because there is no reason for legitimate interaction with these deceptive resources, any interaction is abnormal and there are very few false positive alerts, creating a high fidelity, low noise detection solution. Furthermore, because the deceptive resources can be monitored and/or configured to generate logs, defenders can collect significant amounts of actionable threat intelligence and attack attribution information facilitating faster and more effective response. Better yet, this all occurs while the attacker is busy attempting to hack deceptive systems, distracting them from actual production resources.

SEC550 will give you an understanding of the core principles of cyber deception allowing you to plan and implement cyber deception campaigns to fit virtually any environment. During this hands-on class, you will not only learn deception theory and concepts, you will play an active role working with deception technology through over 15 hours of guided exercises. By the end of the class, you will not only understand the value of cyber deception, you will have practical experience you can immediately implement in your own computing environment.

Author Statement

"When I first started exploring the world of cyber deception I was confused, to say the least. I did not really understand what the fuss was all about. I viewed cyber deception to be something akin to a next-gen honeypot. Honeypots? Really? Then one day, it clicked. As I was looking at different ways honeypots could be deployed I had a thought. What if I was trying to conduct a penetration test against an environment using these techniques? What would that be like? My short answer was it would be terrible and with that realization, I finally understood. Unfortunately, that understanding generated more confusion for me. As I began to see how effective cyber deception could be I began to have doubts. It cannot be this good! There has to be something I am missing. After months of continued research, experimentation, and discussions with other deception practitioners I finally realized that I had found what has been missing from the security industry. I had finally found a way that defenders can finally take back the advantage! I have been passionate about the topic ever since. I also came to realize that each and every person that truly understood cyber deception was every bit as passionate as I was and that I needed to share this with everyone."
—Kevin Fiscus

Section Descriptions

SECTION 1: Understanding the Problem

During the first section of class, we will focus on understanding the core problems associated with attack detection and response and how deception technology can solve those problems. We will look at how common attacker tactics and techniques can evade traditional protective and detective controls. We will understand how even badly implemented deception provides benefits and what an ideal deception program looks like.

TOPICS: Understanding the Problem; Describing the Solution; Offensive Techniques and Controls Evasion; Obvious Deception; Deception Done Right

SECTION 2: Deception Foundations

TOPICS:

Know Yourself

- Developing an IT asset inventory to facilitate deception planning
- Data classification and business impact analysis to identify deception priorities
- Identifying and locating sensitive data using regular expressions
- Vulnerability identification
- Creating a user and group inventory
- Identifying technology usage patterns

Know Your Enemy

- Discover methods to understand attacker tactics and techniques
- How training in offensive tactics can improve your deception planning
- Using incident response and forensic skills to create better deception
- Using the Lockheed Martin Intrusion Kill Chain, the Unified Kill Chain and MITRE ATT&CK to learn about attacker activities

Deception Goals and Components

- Understanding common deception goals
- Using MITRE Shield to clarify deception and active defense objectives
- Preview deception components/elements

Deception and Virtualization

- Understand how virtualization can be used in deceptive environments
- Differences between full and container virtualization solutions

SECTION 3: Deception Techniques and Technologies, Part I

TOPICS:

DNS Deception

- The importance of DNS
- Attacks involving DNS
- DNS deception tactics and techniques

Web Deception

- Web deception tactics and techniques
- Web deception tools and honeypots

Port and Service Deception

- Differences between high interaction and low interaction honeypots
- Port and service deception tools, utilities and honeypots
- Port and service deception advantages and disadvantages

High Interaction Honeypots

- High interaction honeypot overview
- Configuration and instrumentation of high interaction honeypots
- Honeypot monitoring solutions

File and Folder Deception

- File and folder deception overview
- File system instrumentation and alerting
- How to generate credible deceptive data

SECTION 4: Deception Techniques and Technologies, Part II

In this section we will continue looking at deception program components. You will learn how to design, implement and use:

- Deceptive accounts and credentials
- Wireless and network deception
- Email and IoT deception
- Honeynets and honeypot distribution

TOPICS:

Deceptive Accounts and Credentials

- Understanding attacks against accounts and credentials
- Deceptive countermeasures to credential attacks
- Deceptive persona creation, management, and use

Wireless Deception

- Understanding wireless attacks
- Wireless infrastructure deception
- Wireless client deception
- Wireless deception tools and utilities

Network Deception

- Generating and using deceptive network traffic
- Deceptive network devices

Email Deception

- Attacks involving email; phishing, spear phishing, and SPAM
- Anti-phishing deception strategies
- Anti-spam deception strategies

IoT/OT/ICS Deception

- IoT/OT/ICS Deception tools and utilities

Honeynets

- Honeynet overview
- Honeynet advantages and disadvantages
- Honeynet control and instrumentation

Honeypot Distributions

- Honeydrive
- Active Defense Harbinger Distribution (ADHD)
- Honeeepi
- BlackArch Linux

SECTION 5: Deception Concepts, Planning and Evaluation

In this section of the class, you will learn fundamental concepts of deception with a focus on how to create a deception story that effectively influences attacker behavior. You will learn deception maxims, core concepts, and foundational ideas. You will then use everything learned throughout the class to develop a comprehensive deception plan. Next, you will learn methods to evaluate the effectiveness of your deception program. Lastly, you will gain an understanding of the legality of deception, how incident response differs in deceptive environments, along with a brief overview of commercial deception solutions.

SECTION 6: Capstone Exercise

In this final course section, students will put the knowledge and skills learned throughout the class to practical use. Students will divide into teams and presented with a new computing environment within which they will operate. Students will be presented with a series of challenges designed to test their ability to understand their own environment as well as attacker tools, techniques and tactics. Students will be challenged to identify their deception goals based on provided information. Students will then be presented with specific cyber deception objectives. Answering profided questions and successfully achieving stated deception goals will result in scoring points. The team with the most points at the end of the day will be declared winner.

TOPICS: Know Your Self; Know Your Enemy and Your Goals; Deception Implementation