SEC562

CyberCity Hands-on Kinetic Cyber Range Exercise

Six-Day Program
36 CPEs
Laptop Required

Who Should Attend

- Red & Blue team members
- Cyber warriors
- Incident handlers
- Penetration testers
- Ethical hackers
- Other security personnel who are first responders when systems come under attack.

You Will Be Able To

- Scan for and discover the details associated computer, network, and ICS assets.
- Analyze and manipulate commonly used, very powerful, but often less-well-understood protocols such as Profinet, DNP3, Modbus, and more.
- Work as part of a team analyzing attacker actions and preventing kinetic impacts against industrial control systems.
- Look for vulnerabilities in systems associated with electrical power distribution, water systems, traffic systems, and other infrastructures.
- Use a variety of hands-on tools for analyzing and interacting with target systems, including Wireshark, tcpdump, Nmap, Metasploit, and much more.
- Control various Human Machine Interfaces and Operator Interface Terminals widely used by SCADA and other Industrial Control Systems (ICSs)
- Prevent attackers from wreaking havoc by manipulating computers that control physical infrastructures

SANS

SEC562 Training Formats
(subject to change)

Private Training
www.sans.org/onsite

Computers, networks, and programmable logic controllers operate most of the physical infrastructure of our modern world, ranging from electrical power grids, water systems, and traffic systems all the way down to HVAC systems and industrial automation. Increasingly, security professionals need the skills to assess and defend these important infrastructures. In this innovative and cutting-edge course based on the SANS CyberCity kinetic range, you will learn how to analyze and assess the security of control systems and related infrastructures, finding vulnerabilities that could result in significant kinetic impact.

You Will Learn:

- **How to analyze cyber infrastructures that control and impact kinetic infrastructures.**
- **How to manipulate a variety of key industrial protocols, including Modbus, CIP, DNP3, Profinet, and other SCADA-related protocols.**
- **How to rapidly prototype computer attack tools against specific vulnerabilities**
- **How to discover security flaws in a variety of SCADA and Industrial Control Systems (ICSs) and thwart attacks against them.**
- **How to conduct penetration tests and assessments associated with kinetic infrastructures.**

Course Day Descriptions

562.1 HANDS ON: Team Building, Visualizing the Battlespace, Recon, and HMIs

Mission 1: Camera mission: Visualizing the battlespace.
Mission 2: Team-building mission: Recon, social networking, intel gathering, and controlling billboards.
Mission 3: Water Reservoir mission: Ensure the water reservoir Human Machine Interface and data historian properly reflect water records to prevent contamination.
Mission 4: Train Derailment mission: Interact with SCADA-controlled train switching junctions to prevent a disaster.

562.2 HANDS ON: Protocol Manipulation, Data Integrity, and Operator Interface Terminals

Mission 5: Street light mission: Restore streetlights through manipulating an Operator Interface Terminal.
Mission 6: Bank alarm mission: Control a bank alarm system using intel gained from assets across the city.
Mission 7: Traffic light mission: Manipulating and injecting Modbus for system control.

562.3 HANDS ON: Malware Analysis, Privilege Escalation, Incident Response, Passwords Guessing, and Networking Equipment

Mission 8: Radar tower mission: Malware analysis and escaping restricting environments.
Mission 9: City-wide power grid mission: Gain control of SCADA systems to restore power on a city-wide basis.
Mission 10: Landing strip mission: Neutralize a cyber attack to restore lighting to an airfield landing strip.
Mission 11: Rocket launcher mission: Retake control of a rocket launcher and discharge its weapons safely.

562.4 HANDS ON: Cryptography and ICS Protocols

Mission 12: Gas pipeline mission: Crack crypto weaknesses to restore pressure in the gas pipeline to prevent catastrophe.
Mission 13: Residential power grid mission: Regain control of power grid systems to restore the residential infrastructure after a blackout.

562.5 HANDS ON: Power Grid, Weapons Systems, and Network Manipulation

Mission 14: Retailer HVAC mission: Prevent attackers from destroying a retailer who hacked via a contractor and left a time bomb.
Mission 15: ISP Infiltration: Perform a pen test on the ISP.

562.6 HANDS ON: Force-On-Force Attack and Defend

During the final day of SEC562, you'll apply the knowledge and skills you've built all week in SANS first ever course with a red-team/blue-team face off, all inside of CyberCity. Your team will defend your CyberCity turf against attackers while vying to expand your control over various portions of the city. The CyberCity power grid will light up to indicate your level of control over city assets and your progress through a variety of bonus missions as you adapt your skills to achieve even more.

SANS
www.sans.org/SEC562