TEKNOLOGISK
INSTITUT

CPENT... No other Pen Test Course like it!

Advanced Windows Attacks

This zone contains a complete forest that you first have to gain access to and then use PowerShell and any other means to execute Silver and Gold Ticket and Kerberoasting. The machines will be configured with defenses in place meaning you to have to use PowerShell bypass techniques and other advanced methods to score points within the zone.

Attacking IOT Systems

CPENT is the first certification that requires you to locate IOT devices and then gain access to the network. Once on the network, you must identify the firmware of the IOT device, extract it, and then reverse engineer it.

Writing Exploits: Advanced Binary Exploitation

Finding flawed code is a skill competent pen testers need. In this zone you will be required to find the flawed binaries then reverse engineer them to write exploits to take control of the program execution. The task is complicated by the requirement of penetrating from the perimeter to gain access then discover the binaries. Once that is done you have to reverse engineer the code. Unlike other certifications, CPENT includes 32 and 64 bit code challenges and some of the code will be compiled with basic protections of non-executable stacks. You must be able to write a driver program to exploit these binaries, then discover a method to escalate privileges. This will require advanced skills in binary exploitation to include the latest debugging concepts and egg hunting techniques. You are required to craft input code to first take control of program execution and second, map an area in memory to get your shell code to work and bypass system protections.

Bypassing a Filtered Network

The CPENT certification provides web zone challenges that exist within a segmentation architecture, so you have to identify the filtering of the architecture then leverage this knowledge to gain access to web applications. The next challenge is to compromise and then extract the required data from the web apps to achieve points.

Pentesting Operational Technology (OT)

The CPENT range contains a zone that is dedicated to ICS SCADA networks that the candidate will have to penetrate from the IT network side and gain access to the OT network. Once there, you will have to identify the Programmable Logic Controller (PLC) and then modify the data to impact the OT network. You must be able to intercept the Mod Bus Communication protocol and communication between the PLC and other nodes.

TEKNOLOGISK
INSTITUT

Access Hidden Networks with Pivoting

Based on our beta testing, pen testers struggle to identify the rules that are in place when they encounter a layered network. Therefore, in this zone you will have to identify the filtering rules then penetrate the direct network. From there, candidates have to attempt pivots into hidden networks using single pivoting methods, but through a filter. Most certifications do not have a true pivot across disparate networks and few (if any) have the requirement into and out of a filtering device.

Double Pivoting

Once you have braved and mastered the challenges of the pivot, the next challenge is the double pivot. This is not something that you can use a tool for; in most cases the pivot has to be set up manually. CPENT is the first certification in the world that requires you to access hidden networks using double pivoting.

Privilege Escalation

In this challenge, the latest methods of privilege escalation reverse engineering code to take control of execution then break out of the limited shell are required to gain root/admin.

Evading Defense Mechanisms

The range requires your exploits be tested by different defenses you are likely to see in the wild. Candidates are required to get their exploits past the defenses by weaponizing them.

Attack Automation with Scripts

Prepare for advanced penetration testing techniques and scripting with seven self-study appendices: Penetration testing with Ruby, Python, PowerShell, Perl, BASH, Fuzzing, and Metasploit.

Weaponize Your Exploits

Customize your own tools and build your armory with your coding expertise to hack the challenges presented to you as you would in real life.

Write Professional Reports

Experience how a pen tester can mitigate risks and validate the report presented to the client to really make an impact. Great pen testing doesn't mean much to clients without a clearly written report!

TEKNOLOGISK
INSTITUT