Certified Penetration Testing Professional

Kód kurzu: CPENT

CPENT je najpokročilejší kurz etického hackingu vhodný pre všetkých budúcich penetračných testerov, bezpečnostných špecialistov a pre každého, kto chce mať istotu, že zvláda techniky etického hackingu prakticky a chce si svoje skúsenosti nechať potvrdiť v praktickej certifikácii. Po absolvovaní kurzu skladáte 24-hodinovú skúšku skutočného penetračného testovania, kde nie je len jedna plochá sieť, ale celá skupina sietí rovnako ako v enterprise prostredí a účastníci musia odhaliť schémy sietí, vykonávať hacking rôznych systémov a pomocou získaných informácií sa dostať do ďalších častí sietí, ktoré sú vo východiskovom stave neprístupné. Certifikácia CPENT je zameraná na efektívne vykonávanie penetračného testovania v enterprise prostredí. Nejde len o zoznámenie sa s technikami etického hackingu, ale absolventi sa naučia správne analyzovať, postupovať a vykonávať proces penetračného testovania. Jedinečnosť školení a certifikácie CPENT spočíva v jeho šírke – pokrýva nielen sieťové skenovanie a enumeráciu, penetračné testovanie Active Directory s hľadaním najčastejších chýb v konfigurácii enterprise systémov, Kerberoastingu a zneužívanie NTLM Relay, extrakciu dát a prestupovanie forestu pomocou Golden Ticketu, testovanie sieťovej infraštruktúry, webových aplikácií s reálnymi útokmi proti klientom a serverom, mobilných aplikácií, ale tento penetračný test taktiež zahŕňa IoT a OT hacking. CPENT je veľmi intenzívny kurz etického hackingu pre všetkých absolventov certifikácie CEH, ktorí si chcú prehĺbiť praktické znalosti a dôkladne sa pripraviť na dve najvyššie EC-Council certifikácie zároveň: CPENT – Certified Penetration Testing Professional a LPT – Licensed Penetration Tester. Účastníci, ktorí získajú certifikačné skóre nad 90 % získavajú najvyšší certifikačný titul LPT. Vzhľadom na zameranie a priebeh testu ide o ideálnu prípravu pre všetkých, ktorí chcú zložiť známu a uznávanú certifikačnú skúšku OSCP.Na CPENT školení sa naučíte reálne vykonávať testovanie vzdialene pomocou vhodne umiestnených headless zariadení, kedy reverzné tunely a overovanie pomocou kľúčov s minimálnou možnosťou detekcie bude samozrejmosťou – naučíte sa skenovať prostredie tak, aby ste neboli ihneď odhalení, ďalej sa naučíte správne pracovať s výstupmi skenovania a analyzovať ich tak, aby ste vedeli vytipovať vhodné ciele pre útok. Kurz zahŕňa aj praktické vykonávanie exploitácie, ktoré si na kurze vysvetlíme podrobne vrátane praktických cvičení. Samozrejmosťou je vykonávanie eskalácie privilégií, aby ste mohli dosiahnuť plného napadnutia cieľov, extrakcie všetkých dôležitých informácií a pomocou týchto informácií prestupovať ďalej sieťou pomocou lateral movementu a pomocou pivotingu prestupovať aj do sietí, ktoré sú pre Vás v počiatočnej fáze penetračného testu nedostupné. Pivoting vykonávate nielen pomocou metasploitu, ale tiež prostredníctvom proxy pivotingu, VPN pivotingu a naučíme sa pracovať s predávaním dát medzi viacerými spojeniami pomocou zanedbávaných komponentov v OS, aby ste mohli správne ovládať napadnuté systémy. Ďalej sa naučíte správne analyzovať webové aplikácie a praktickú exploitáciu ako web klientov, tak web serverov. V ďalšej fáze potom prakticky prechádzame chyby v bezpečnosti aplikácií a spôsobu ich exploitácie. Naučíme sa taktiež analyzovať IoT firmware tak, aby ste našli chybne zakomponované kľúče, chyby v komunikácii zariadení a informácie o fungovaní aplikácií tak, aby ste tieto zariadenia mohli ovládnuť. Zoznámite sa tiež s analýzou OT komunikácie.Vzhľadom na šírku záberu tém ide o veľmi intenzívne školenie, ktorým Vás bude prevádzať viacero lektorov pre maximálne zefektívnenie výučby a predávanie praktických skúseností a vysvetlenie najčastejších chýb v prevádzkovom prostredí a aplikáciách. Absolvovanie kurzu CEH a jeho všetkých požadovaných predošlých kurzov je preto nevyhnutné minimum. Vzhľadom na šírku a hĺbku tém silno odporúčame aj predošlé absolvovanie našich detailných hacking kurzov GOC32, GOC33, GOC54 (prípadne podrobnejších GOC541 a GOC542) a GOC56, kde účastníci získajú veľmi detailné praktické zvládnutie princípov a praktických techník penetračného testovania, a na CPENT kurze, vlastnej príprave a certifikácii sa mohli sústrediť predovšetkým na zvládnutie procesu penetračného testovania.Po absolvovaní kurzu si vyberáte medzi zložením certifikačnej skúšky v podobe jedného 24-hodinového testu alebo 2 testov v dĺžke 12 hodín a potom do týždňa odovzdávate reálny pentest report. V oboch prípadoch ide o praktický test pod dohľadom, bez rizika podvádzania a certifikácia dokladá, že ste schopní vykonávať penetračné testovanie prakticky. Po absolvovaní školenia, vlastnej intenzívnej príprave a certifikácii sa budete v HackTheBox, počas CTF a pri vykonávaní pentestingu cítiť ako doma.Tento kurz je náhradou za ukončený kurz EC-Council Certified Security Analyst [ECSA].

Pre koho je kurz určený

Tento najpokročilejší kurz etického hackingu je vhodný pre budúcich penetračných testerov, ktorí pomocou skutočne uznávaných certifikácií dokladajú zákazníkom, že zvládajú proces penetračného testovania prakticky. CPENT je určený tiež pre IT bezpečnostných špecialistov, ktorí chcú prakticky poznať problematiku hackingu z širšej perspektívy, spôsob práce útočníka v napadnutom firemnom prostredí. CPENT je tiež kurz vhodný pre všetkých, ktorí sa zaujímajú o počítačovú bezpečnosť a hacking a súčasne si trúfnu na praktickú hacking challenge.

GOPAS Praha
Kodaňská 1441/46
101 00 Praha 10
Tel.: +420 234 064 900-3
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 542 422 111
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 248 282 701-2
info@gopas.sk

Certified Penetration Testing Professional

Tento kurz je náhradou za ukončený kurz EC-Council Certified Security Analyst [ECSA].

Čo Vás naučíme

Reálne vykonávať penetračné testovanie firemnej infraštruktúry a webových aplikácií na úrovní certifikačných skúšok

CPENT, LPT a OSCP

Požadované vstupné znalosti

Pre absolvovanie kurzu je úplne nevyhnutné zvládnutie techník z kurzu CEH – Certified Ethical Hacker verze 9+

Vrelo odporúčame taktiež predchádzajúce absolvovanie kurzov:

GOC32 – Hacking v Praxi II

GOC33 – Hacking v Praxi III

GOC54 – Zranitelnosť webových aplikácií (prípadne podrobnejších a novších GOC541 a GOC542)

Študijné materiály

Originálna príručka firmy EC-Council v podobe e-Courseware

Osnova kurzu

Prieskum cieľa

- OSINT
- Fyzický prieskum a vytipovanie slabých miest vo fyzickom zabezpečení
- Hardware útoky
- Headless device deployment a management

Skenovanie a enumerácia

- Efektívne využívanie nmapu, ale aj komponentov v OS
- DNS extraction
- Prieskum prostredia pomocou pasívnej analýzy okolitej a vlastnej prevádzky v sieti
- Zisťovanie topológie siete a cieľových segmentov

Malware deployment

- Social engineering
- USB útoky
- Obfuscation
- Covert channel

Pentesting Active Directory

- Kerberos hacking
- Kerberoasting
- NTLM Relay
- Golden Ticket
- Secret data extraction
- Lateral movement

Pivoting

- Identifikácia filtrovania komunikácie
- Základný pivoting
- Double pivoting
- Manuálny postup

Exploitácia

GOPAS Praha
Kodaňská 1441/46
101 00 Praha 10
Tel.: +420 234 064 900-3
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 542 422 111
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 248 282 701-2
info@gopas.sk

- Reverse engineering
- Fuzzing
- Buffer overflow
- Payload execution

Privilege escalation
- Analýza konfigurácie systémov
- Identifikácia aplikácií a chýb v konfigurácii
- Zneužívanie nájdených chýb

Web Pentesting
- Enumerácia web serveru
- Mapovanie aplikácie
- Exploitácia vstupu pomocou injektáže - SQL Injection, Function injection, Object injection
- Local file inclusion
- Remote file inclusion
- Local session poisoning
- Session management
- Remote Code Execution
- Command Execution
- CSRF
- XSS

IoT Hacking
- Firmware extraction
- Key extraction
- Analýza komunikácie

OT Hacking
- Prestup z IT do OT
- Analýza komunikácie
- PLC, Mod Bus

GOPAS Praha
Kodaňská 1441/46
101 00 Praha 10
Tel.: +420 234 064 900-3
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 542 422 111
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 248 282 701-2
info@gopas.sk