Hacking v Praxi III

Kód kurzu: GOC33

Počas pokročilého kurzu hackingu sa zaoberáme pokročilými sieťovými útokmi pre detailný prieskum sieťového prostredia. Naučíme sa zneužívať slabiny v chybnej implementácii zabezpečenia ethernetu aj WiFi sietí. Vyskúšame si prestup ochranou siete na úrovni L2 v podobe VLAN hoppingu aj L3 v podobe útokov na routery. Detailne sa zoznámime s možnosťami skenovania cieľov a to aj v situácii, keď nemáte možnosť skenovať ciele priamo. Zoznámime sa s princípmi najčastejších webových útokov, ktoré si vyskúšame prakticky proti klientom i serverom. Účastníci sa zoznámia so zneužívaním útokov XSS, Cross Site Request Forgery, SQL injection, blind SQL injection, command injection a ďalšími. Zoznámime sa aj s hackingom bezdrôtovej komunikácie pomocou Software Defined Radio a hackingu BluetoothLE. V ďalšej časti potom využijeme predošle získané znalosti na analýzu a útoky na IoT zariadenia, ovládanie kamery, žiarovky alebo embeded zariadenia, takže si ukážeme aj hacking HW.

Pre koho je kurz určený

Kurz je určený pre správcov sietí, pentesterov, bezpečnostných audítorov a architektov sieťovej bezpečnosti so znalosťami tém z kurzu GOC3, ktorí sa chcú do detailu zoznámiť s pokročilejšími útokmi na sieťovú infraštruktúru, prerazenie ochrany, rozdeľovanie sietí do VLAN a alternatívnymi možnosťami Man-in-the-Middle, Software Defined Radio. Kurz je určený aj pre všetkých, ktorí sa chcú prakticky zoznámiť s metódami webhacking útokov.

Čo vás naučíme

Na tomto praktickom kurze sa naučíme pokročilé techniky napádania sietí, obchádzať zabezpečenia segmentácie sietí do VLAN, prestreliť routery oddeľujúce naše sieťové segmenty. Naučíme sa tiež testovať bezpečnosť podnikových WiFi klientov a infraštruktúry. Ďalej sa zoznámime s princípmi SDR hackingu a s útokmi na BluetoothLE. Účastníci kurzu sa tiež prakticky zoznámia s najobľúbenejšími webhacking útokmi. Tieto nabité znalosti sa potom naučíme uplatňovať pri útokoch na kamery, IoT a embeded zariadenia.

Požadované vstupné vlastnosti

Absolvovanie kurzu GOC3

Osnova kurzu

Pokročilé sieťové útoky

- SPAN a RSPAN
- Vlan Hopping
- Útoky na 802.1x
- Man in the Middle aj bez APR
- Statické zásahy do cache
- Statické zásahy do routingu
- Podvrhnutie DHCP serveru
- DHCP Starvation attacks
- DNS spoofing a poisoning
- DNS typy záznamov a chyby v zabezpečení

Falošná AP a WPA-Enterprise útoky

- Prebúravanie identít pomocou falošných AP
- Zneužívanie falošných AP pre otrávenie klientov
- Zneužívanie Hosted Networks ako backdoor do podnikového prostredia

Prieskum sieťového prostredia

- Skenovanie živých cieľov aj bez nmapu
- Skenovanie cieľov, s ktorými nejde komunikovať
- Enumerácia alebo zaisťovanie detailov o napadnutom prostredí

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

- SNMP alebo Security Not My Problem a ako môže viesť až ku podrobeniu siete

Útoky na routery

- Sieťové útoky
- Inštalácia backdoorov do firmware
- Praktické otvorenie administrácie pomocou CSRF útokov
- Pretečenie pamäti

Web útoky

- Session Hijacking
- Cross Site Request Forgery
- Cross Site Scripting
- Error Based SQL Injection vs. blind SQL injection
- Command injection
- Click jacking
- Praktické vyskúšanie útokov k ovládaniu klientov, serverov aj celkovému otvoreniu siete

SDR - Software Defined Radio

- Princíp SDR útokov
- Praktické testovanie SDR
- Útoky na BLE

IoT hacking

- Statická analýza firmware
- Credential bruteforcing
- Napádanie sieťovej komunikácie
- Command injection

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