Hacking v praxi II

Kód kurzu: GOC32

V tomto jedinečnom a veľmi detailnom hacking kurze prinášame prehľad útokov, ktoré sú pre väčšinu podnikových sietí najrizikovejšie. Kurz vhodne rozširuje dlhodobo najobľúbenejšiu časť školenia CEH a do väčších detailov preberá časť útokov pomocou malware a systémových útokov.Vysvetlíme si, ako často dochádza k otváraniu podnikovej siete na diaľku pomocou malware a trójskych koní v a ako možno takýto útok zneužiť pre kompletné ovládnutie siete bez fyzického prístupu. V následnej časti systémových útokov si preukážeme, že staré zvyky správcov a chyby v správe, na ktorých stále funguje väčšina podnikov, vedú ku kompletnej kompromitácii bez potreby akokoľvek prelamovať prihlasovacie údaje a ako obrovsky uľahčia prístup údaje získané z pamäte a profilov užívateľov. Pre vykonanie útokov použijeme aj falošné USB zariadenia, ktoré sa naučíte vytvárať za behu a pomocou ktorých môžete ovládnuť cudzí počítač na diaľku a bez vedomia používateľov aj správcov ich počítače pripojiť do svojej siete a odcudziť prevádzku, s ktorou môžete aj manipulovať. V záverečnej časti kurzu sa pozrieme aj do úvodu hackingu mobilných platforiem, ktoré možno použiť ako platformu pre vykonanie útoku, ale zacielime aj na útoky proti mobilným klientom, ktoré vedú k zneužitiu našich mobilných zariadení a dát v nich uložených.

Pre koho je kurz určený

Kurz je určený pre správcov sietí, administrátorov bezpečnosti IT, audítorom bezpečnosti a budúcim penetračným testerom, ktorí sú už oboznámení s obsahom základného kurzu GOC3 a chcú si prakticky vyskúšať pokročilejšie hacking techniky a spoznať reálne, na ktorých princípoch funguje napádanie a ovládanie firemných systémov vzdialene, bez nutnosti priameho zásahu do sieťového prostredia, porozumieť kľúčovým problémom bezpečnosti počítačových sietí ako je sledovanie našich aktivít na počítači, spôsoby ovládania počítačov na diaľku a ich dôsledky pre bezpečnosť firemných dát a celého prostredia. Kurz Vám umožní tiež pochopiť princípy útokov pomocou USB zariadení a prakticky sa ich naučiť využívať pre získanie kontroly nad vzdialeným počítačom. Kurz je vhodný pre každého, kto chce do detailu nielen pochopiť, ale aj prakticky vyskúšať pokročilejšie metódy útokov, ktoré zneužívajú najbolestivejšie chyby, ktorých sa dopúšťa väčšina dnešných IT administrátorov aj používateľov.

Čo vás na kurze naučíme

Tento ojedinelý kurz Vás naučí odhaľovať a na účely penetračného testovania využívať najzávažnejšie chyby, kvôli ktorým možno ovládať firemné prostredia a ktoré reálne ohrozujú bezpečnosť väčšiny firiem. Naučíme sa zneužívať chyby, ktorých sa dopúšťa väčšina pracovníkov IT na najrôznejších pozíciách a prečo môžu ľahko viesť k strate kontroly nad firemnou infraštruktúrou počas systémových útokov. V ďalšej časti sa naučíme ako sa vytvára malware pre vzdialené prevzatie kontroly nad počítačmi, sledovanie aktivít používateľov, získavanie uložených tajomstiev, skrývanie komunikácie pri ovládaní obetí a spoznáme, že bežní používatelia IT prakticky nemajú príliš možnosť rozpoznať, že sa stali obeťou útoku spustenia škodlivého kódu v spustiteľných súboroch, makrách alebo priestrelnej klientskej aplikácie a nemôžu správne rozpoznať závažnosť vplyvov útoku. V ďalšej časti kurzu sa naučíme útoky vykonávať pomocou USB zariadenia, ktoré možno zneužiť na priame napadnutie systémov a uvidíme, že to ani zďaleka nie je o USB flash diskoch, na ktorých by mal byť malware a naučíme sa priame ovládanie komunikácie našich USB zariadení. V ďalšej časti kurzu sa naučíte vytvárať kód pre ovládanie aj na mobilných zariadeniach a možnosť kontroly dát na nich. V záverečnej časti sa potom venujeme tiež problémom DOS útokov, ktoré sú jedným z dôsledkov napádania našej infraštruktúry rovnako tak ako cestou k odstaveniu kľúčovej infraštruktúry.

Osnova kurzu

Systémové útoky alebo desať najčastejších hriechov IT pracovníkov, kvôli ktorým prichádzame o firmu

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

- Zneužívanie najčastejších chýb v administrácii ku kompletnej kompromitácii siete
- Prečo nevinné presmerovanie lokálnych zdrojov v RDP môže viesť k ovládnutiu siete
- RDP MITM a session recording aneb vzdialený záznam klávesnice a obrazovky admina
- Chybné používanie identít pre administráciu, spustenie úloh a služieb
- Offline útoky pre ovládnutie domény
- Heslá a vykrádanie tajomstiev z počítačov
- Zneužívanie shadowcopy pre vykrádanie databáz, Active Directory a file serverov
- Zneužívanie lokálnych účtov v predvolenom nastavení
- Vykrádanie pamäte počítača
- Vykrádanie profilov a šifrovacích tajomstiev
- Pass The Hash alebo ako s údajmi z pamäte ovládnuť vzdialené systémy a prečo nie je potrebné lámať heslá
- NTLM Relay alebo ako položiť úplne vzdialené systémy, kam nikto nechcel pristupovať len počas útokov MITM
- Responder a podvrh legitímnych cieľov alebo ako ľahko nalákať obeť a zneužiť jej predvolené nastavenia
- Pass The Ticket alebo vykrádanie Kerberosu
- Kerb roasting alebo kompromitácia účtov služieb
- Golden Ticket prakticky - priestrel celého AD forestu pomocou jedinej domény
- DMA útoky alebo ako obísť ochranu BitLocker

Malware a všetko na čo ste sa báli opýtať alebo ako ovládnuť firmu na diaľku a prečo je väčšina firiem priestrelenou zvnútra

- Princíp komunikácie a prečo útoky zvnútra vedú
- Ako zneužiť najčastejšie cesty spustenia malwaru k infiltrácii prostredia
- Možnosti ovládania a sledovanie obetí
- Skrývanie malware - kam sa skryť, aby vás nikto nehľadal
- Wmi filtre
- Využívanie viac úrovní streamov
- Zanedbávané nastavenia office
- Skrývanie v registroch
- Šifrovanie
- Nezvyčajné metódy spúšťania kódu
- Využívanie skrytých kanálov a tunelingu v iných protokoloch
- Pivoting alebo ako prestúpiť z napadnutého počítača ďalej do neprístupného prostredia
- Automatizácia prestupu prostredím
- Infekcia obsahu pri MITM útokoch
- Fileless backdooring
- Asynchrónne komunikácie
- Skrývanie malwaru pomocou Application Compatibility Toolkit a tvorba Shima

USB Hid útoky alebo ako zneužiť čokoľvek v USB ku kompletnej kompromitácii systému

- Falošné USB flash disky dynamicky meniace svoj obsah pre ovládnutie siete
- Spôsob vytvárania objektov na HID zbernici
- Ovládanie počítačov pomocou HID injection
- Spôsoby odcudzenia sieťovej prevádzky a SSL inšpekcie
- Prihlásenie sa k systému bez fyzického prístupu
- Reverzný SSH tunel pre ovládnutie počítača
- Kali Nethunter ako penetračná platforma
- P4wnP1 a BashBunny ako prostriedok pre penetračné testovanie

MouseJacking a KeyJacking

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

- Zneužívanie zraniteľných klávesníc a myší pre ovládnutie vzdialených počítačov

Úvod do Android hackingu

- Generovanie malwaru pre mobilné prostredie
- Priestrel slabín na zastaralých systémoch
- Zneužívanie oprávnenia aplikácií
- Možnosti sledovania mobilných zariadení

DoS attacks

- Flooding cieľov
- Reflection attacks
- Amplification effect

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