Praktična primjena tehnika napada na računalne sustave

Trajanje treninga: 2 dana (08h-16h or 09h-17h) – 6h30min + pauze
(pauza za ručak– 1 sat, pauze za kavu– 15 min x 2)

Potrebno predznanje: Trening „Pogled na sigurnost računalnih sustava s „tamne“ strane“.

Na treningu se, kroz dva dana, obrađuje sljedeće:

Korištenje alata i napadi na windows/Linux okruženje –Nije dovoljno samo razumjeti kako rade i kako se mogu provesti određeni napadi na mrežu i aplikcije, već je potrebno razumjeti i ovladati tehnikama i korištenjem alate kako bi mogli samostalno iskorištavati propuste. Ovaj trening je direktan nastavak na trening Pogled na sigurnost računalnih sustava s „tamne strane“, a fokus je stavjen na napredno korištenje alata, kao što su nmap, nc, cryptcat, metasploit framework, izrada reverse shell-ova pomoću msfvenom alata isl. Isto tako obrađuje se na praktičnim primjerima kako se lateralno kretati po mreži nakon što je kompromitirano jedno računalo u njoj i kako koristiti tehnike port forwarding-a u istu tu svrhu. Mete napada u ovom 80% praktičnom treningu su windows i linux OS-ovi i aplikacije koje se pokreću na njima.

Sadržaj treninga:

1. Korištenje alata (VJEŽBE/DEMO)
   - Nc, ncat, cryptcat
   - Nmap, identifikacija servisa, skeniranje ranjivosti
   - Metasploit framework,
   - Msfvenom izrada custom reverse shell-a
   - Pivoting pomoću msf-a, ssh i kroz windows kljentsko računalo
2. Windows napadi (VJEŽBE/DEMO)
   - Osnovni alati koje treba razumjeti
   - AD 101
   - Enumeracija korisnika i grupa
   - Razbijanje Windows lozinki (jtr, hashca, cain&abel)
   - PtH
   - EoP
   - Što nakon inicijalnog kompromitiranja windows računala – dodatne tehnike enumeracije
3. Linux napadi (VJEŽBE/DEMO)
   - Osnove bash-a
   - Osnovni alati koje treba razumjeti
   - Linux prava pristupa – osnove
   - Enumeracija korisnika na linux sustavima
   - NFS
   - R* servisi
   - X11
   - SSH