HIC SALTA

Ravbarji&Žandarji seminar

METASPLOIT

14. junij 2016

Seminar Ravbarji & Žandarji – junij 2016

V seminarjih in delavnicah "Ravbarji in žandarji" se udeleženci seznanijo z novimi trendi na področju informcijske varnosti.

Sledenje in seznanjanje z vedno novimi triki in tehnikami napadalcev je zahtevna naloga za specialiste informacijske varnosti, a tudi upravljalci omrežij in sistemov pri svojem vsakodnevnem delu potrebujejo čim bolj ažurne informacije in znanja s tega področja, da lahko preprečijo vdore. Če pa do vdora kljub temu pride, ga morajo čim prej prepoznati in učinkovito ukrepati. Tokratna tema je orodje METASPLOIT – "švicarski nož" pen-testerjev, varnostnih strokovnjakov in administratorjev omrežij.

Vsebina:

- **Osnove orodja METASPLOIT**
  - Zgodovina, edicije (framework, Express, Pro): od brezplačne do komercialne edicije
  - Različni pristopi in oblike napadov
- **Osnovni gradniki orodja METASPLOIT**
  - Auxiliary
  - Exploit
  - Payload
  - Encoder
- **Namestitev in osnovna uporaba**
  - Win/Linux platforma, Kali distribucija
  - Konzola, Armitage GUI okolje
  - Priprava okolja za napad – listener modul
- **Izraba ranljivosti OS, aplikacij, programskih modulov**
  - Skeniranje sistemov, servisov in aplikacij
  - Moduli za odkrivanje servisov in njihovih nastavitev
  - Integracija z drugimi varnostnimi skenerji
  - Demo: Napad na Linux in Windows sistem
- **Uporabniška gesla**
  - Osnovna gesla, lista gesel, "brute force" napad
- **Izraba ranljivosti na strani uporabnikov**
  - Ranljivosti brskalniških tehnologij
  - Napadi preko MS office dokumentov
  - Izogibanje antivirusni detekciji
  - Demo: Primer napada preko MS Excel dokumenta
  - Demo: Napad na Android napravo
- **"Post-hack" koraki kot nadaljevanje napada na sistem in uporabnika**
  - Pridobivanje varnostno kritičnih informacij
  - "Pass-the-hash" modul
  - Powershell
  - Demo: Napad na Windows domenski kontroler
- **Programskam oprema Cobalt Strike**
  - Kopija lažnega spletnega strežnika
  - Napredne oblike napadov
- **Socialni inženirig in okolje METASPLOIT**

Predavatelj

BRANE VASILJEVIČ ima večletne izkušnje na področju informacijske varnosti. Večino svojega časa posveča izvajanju različnih oblik varnostnih testiranj in uvajanju tehničnih rešitev v podjetjih. Mnogi ga poznajo kot odličnega predavatelja o varnostnih problemih tako na NT in HEK konferencah , kot drugih srečanjih informatikov.

ČAS IN LOKACIJA

- 14. Junij 2016
- TRAJANJE: OD 9-15 URE
- ODMOR ZA KOSILO V ORGANIZACIJI IZVAJALCA SEMINARJA (VKJUČENO V CENO)
- UČILNICA ADD, TBILISIJSKA 85, LJUBLJANA
- CENA: 195 Eur + DDV
- PRIJAVE IN INFORMACIJE:
  - E-POŠTA: rz@hicsalta.si
  - TEL. 01 244 7820
- ŠTEVILO MEST JE OMEJENO

TEMA SEMINARJA: METASPLOIT

Metasploit je brez dvoma eno izmed najbolj močnih in uporabnih orodij za varnostne strokovnjake in upravljalce sistemov, ki v svoji *community* (free-ware) in komercialni različici v resnici omogoča izgradnjo učinkovitejših zaščitnih mehanizmov in postopkov ter nadgradnjo nivoja znanja na različnih področjih računalniške varnosti.

Za **METASPLOIT** velja, da je eno najbolj "razvpitih" orodij s področja računalniške varnosti. Njegov "multipraktik" pristop, omogoča uporabo orodja v različnih vlogah. METASPLOIT je lahko:

- Orodje za **avtomatizirano** izvajanje korakov pri varnostnih testih na sistemov in aplikacij.
- Orodje za **potrjevanje** ranljivosti.
- Orodje za nazoren **prikaz posledic** prisotnosti varnostnih pomanjkljivosti – „Proof of concept" pristop in ozaveščanje okolja.
- Orodje za razumevanje delovanja procesa **„hackinga"** – izobraževanje upravljalcev/nadzornikov okolja IT.

Platforma METASPLOIT omogoča prek svojih modulov uporabo vseh metod in tehnik, ki jih napadalci uporabljajo za izvajanje napadov na sisteme, aplikacije in omrežja. Ko se pojavi nova oblika ranljivosti, velika skupnost uporabnikov (več kot 200.000 uporabnikov) poskrbi za njen prenos v okolje METASPLOIT. Zato je METASPLOIT odlično orodje za spoznavanje naprednih oblik hekerskih napadov. Na seminarju bomo spoznali naslednje scenarije:

- Škodljiva koda in izogibanje detekciji antivirusni porogramski opremi
- Napad na sistem kot posledica odsotnosti varnostnih popravkov
- Napad na Windows 10 - vsi popravki, nameščena AV programska oprema
- Napad na domenski kontroler kot posledica uspešnega napada na uporabniško delovno postajo
- Napad na Android napravo
- Zloraba ranljivosti brskalniških tehnologij na delovni postaji
- Postavitev lažnega spletnega strežnika
- In še veliko več….

Za udeležence:

Udeležencem seminarja priporočamo, da s seboj prinesejo prenosne računalnike z nameščeno distribucijo Kali 2.0 (virtualno okolje). Za omrežje in demo sisteme bo poskrbel organizator seminarja. Vsem udeležencem bo omogočen dostop do spletnih učilnic na http://rz.hicsalta.si, kjer bodo na voljo dodatne informacije in "step-by-step" navodila posameznih lekcij in demo scenarijev.