Pogled na sigurnost računalnih sustava s „tamne strane“

Na treningu se, kroz tri dana, obrađuje sljedeće:

Sigurnosni koncepti – polaznik će se upoznati s osnovnim konceptima sigurnosti, CIA i DAD trokut, sveobuhvatna zaštita (Defense in depth), te će biti diskutirano zašto sigurnost često pada u vodu

Upravljanje rizicima – osnove – polaznik će se upoznati s osnovnim pojmovima vezanim uz upravljanje rizicima, bit će definirani kvalitativni i kvantitativni pristup procjeni rizika. U vježbama koje slijede nakon teoretskog dijela predavanja, polaznik će odraditi treath modeling po STRIDE modelu i napraviti kvalitativnu procjenu rizika.

Faze hakerskog napada – obradit će se koraci napada po metodologiji koju koristi većina hakera (Reconnaisance, Scanning, Gainig access, Maintaining acces, Covering tracks), a kroz vježbe će polaznik odraditi reconnaisance javno dostupnih informacija, provest će skeniranje portova korištenjem nmap alata, te će enumerirati DNS, SNMP i LDAP protokole.

Penetracijski test – kao nastavak na prethodnu cjelinu, u ovoj će cjelini biti definiran napad kako ga provode profesionalni penetracijski testeri, bit će definirana svrha i faze penetracijskog testa (koji se u nekim koracima razlikuje od hakerskog napada). U vježbi će se koristiti neki od dostupnih besplatnih alata za skeniranje ranjivosti kao uvod u penetracijsko testiranje.

Osnove mreža i MitM napadi – polaznici će se upoznati s osnovnim pojmovima vezanim uz mreže i mrežnu komunikaciju koji su potrebni za razumijevanje nadgledanja (snifanja) prometa i MitM (Man in the midle) napada. Kroz vježbe će koristiti wireshark i MS message analyzer za analizu prometa, te će napraviti MitM napade na DNS, HTTPS, RDP isl. Protokole.

Vrste autentikacija i napadi na Windows passworde – cilj ove cjeline je upoznati korisnika s autentikacijom i autorizacijom, te protokolima koji se koriste. Bit će definirani načini kreiranja dobrog passworda i načini kako se password može probiti (dictionary, brute force, precalculated hashes ...). U vježbi će polaznici imati priliku promijeniti password lokalnog i domenskog administratora u situaciji kad imaju fizički pristup serveru i okušat će se u razbijanju passworda raznim spomenutim metodama.

Napadi na WEB aplikacije – polaznici će se kroz ovo poglavlje upoznati s osnovama web tehnologija koje se danas koriste i samim HTTP protokolom, te nekim od napada koji su mogući: SQL injection, XSS, parameter tampering, directory traversal isl. Koristit će se alati poput Burp, Zap i fiddler proxy servera kroz vježbe u kojima će se iskoristiti SQL injection, parameter tampering isl.

Napadi na WiFi (WEP, WPA, WPA2) – s obzirom da je bežično umrežavanje rasprostranjeno, a mreže su i dalje poprilično nesigurne, kroz ovu cjelinu polaznik će se upoznati s WiFi protokolima i načinima kako probiti WEP, WPA i WPA2 protokole. Kroz live demo vidjet će lakoću probijanja WEP protokola i u nekim situacijama WPA i WPA2 prtokola.

Za svaku od navedenih cjelina bit će difiniran i način kako se od spomenutih napada zaštititi i kako ih u potpunosti spriječiti ako je to moguće.

Potrebno predznanje:

- Osnove administracije linux ili windows OS-a
- Osnove poznavanja mreža

DAN 1

1. Sigurnosni koncepti
   - Općenito o sigurnosti
   - CIA/DAD trokut
   - Sveobuhvatna zaštita
   - U čemu je bit sveobuhvatne zaštite
   - Zašto hakeri uspijevaju u onome što rade
2. Upravljanje rizicima
   - Općenito o risk managementu
   - Kvalitativni pristup
   - Kvantitativni pristup
   - Procjena rizika
   - Upravljanje rizicima
   - VJEŽBA: threath modeling igra s kartama
   - VJEŽBA: kvalitativna risk management analiza
3. Faze napada
   - Reconnaisance
   - Scanning
   - Gaining access
   - Maintaining access
   - Covering tracks
   - VJEŽBA: reconnaisance – javno dostupne informacije
   - VJEŽBA: skeniranje portova i servisa
   - VJEŽBA: enumeracija DNS-a SNMP-a, AD-a
4. Penetracijski test
   - Svrha penetracijskog testa
   - Faze penetracijskog testa
     - Definiranje opsega i potpisivanje ugovora (formalni okvir)
     - reconnaisance
     - Scanning
     - Vulnerability scanning
     - Exploiting
     - Reporting
   - VJEŽBA: nessuss ili OpenWAS skeniranje ranjivosti

DAN 2

5. Mreža
   - Osnovno o mrežama
     - OSI model
     - TCP/IP model
     - TCP protokol
       - Zastavice (flags)
       - Trostruko rukovanje
   - Snifanje i analiza prometa
     - Promisc mod mrežnog adaptera
     - Wireshark
     - Microsoft message analyzer
   - VJEŽBA: snifanje prometa i clear text passworda
   - MitM napadi
     - DNS
     - MAC (ARP) spoofing
     - Kako pretvoriti switch u HUB
     - Evil twin
   - VJEŽBA: ARP spoofing
   - VJEŽBA: HTTPS MitM napad
   - VJEŽBA: SSL strip MitM napad
   - VJEŽBA: RDP MitM napad
6. Windows passwords
   - Općenito o passwordima
   - Kako odabrati dobar password
     - Dužina
     - Karakter set
     - passfraza
   - Vrste napada na passworde
     - Brute force
     - Dictionary
     - Hybrid
     - Precomputed hashes (rainbow tables)
     - Snifanje
     - Netehnički napadi
   - AAA (A) – Autentikacija, autorizacija, auditing, (accounting)
     - Autentikacija i autentikatori
       - Tip 1
       - Tip 2
       - Tip 3
     - Pohrana autentikatora
       - SAM baza podataka
       - AD
       - LM

        - NTLM
- Autentikacijski protokoli
    - Nezaštićeni protokoli
    - Challange response protokoli
    - AAA protokoli
- Autorizacija
    - DAC
    - Nediskrecijska kontrola pristupa
    - MAC
    - RBAC
    - Windows token
    - UAC
- Auditing
- Accounting
- VJEŽBA: Razbijanje passworda
    - Offline mod: brute force
    - Offline mod: dictionary
    - Offline mod: precomputed hashes
- VJEŽBA: izrada custom dictionary-a
- VJEŽBA: resetiranje admin passworda na domenskom kontroleru (bez znanja admin passworda – naravno ☺)

DAN 3 (nastavak cjeline 6 ako se ne završi u drugom danu – a moglo bi se ne završiti ☺)

7. WEB aplikacije
   - Osnovno o web tehnologijama
     - HTTP protokol
     - Arhitektura web aplikacija
   - SQL injection
   - Parameter tampering
   - Directory traversal
   - XSS
   - Web debugger proxy
     - Burp
     - Zap
     - Fiddler
     - ...
   - VJEŽBA: skeniranje web ranjivosti – ZAP
   - VJEŽBA: parameter tampering – BURP
   - VJEŽBA: SQL injection
8. WiFi
   - općenito o standardima (A, B, G, N)
   - WEP
   - WPA
   - WPA2
   - VJEŽBA (ili DEMO): probijanje WEP protokola
   - VJEŽBA (ili DEMO): probijanja WPA2 protokola