Informatikai biztonság alapjai

Oláh Norbert

2022.

Tartalom

Bevezetés

A Nessus sebezhetőségeket detektáló szkenner a világ vezető aktív szkennere, amely gyors felderítést, konfigurációs auditálást, eszközprofilkészítést, érzékeny adatok felderítését és a biztonsági helyzetkép vizsgálatát kínálja. – Tenable

Bevezetés

A Nessus egy automatizált biztonsági ellenőrző eszköz, amely átvizsgálja a számítógépet, és riasztást ad, ha olyan sebezhetőségeket fedez fel, amelyeket rosszindulatú támadók kihasználva hozzáférhetnek a hálózathoz csatlakoztatott számítógépekhez. Ezt úgy teszi, hogy több mint 1200 ellenőrzést futtat le az adott számítógépen (célponton), és azt vizsgálja, hogy ezek közül bármelyik támadással tudja-e kompromittálni, vagy más módon kárt okozni az adott vizsgálandó eszközön.

Képességek

- Patch teszt
- Hibás konfigurációk észlelése
- Port vizsgálat
- Szolgáltatás észlelése
- A legismertebb hitelesítő adatok tesztelése
- Az exploit használatának képessége
- Hitelesítő adatok keresésének lehetősége
- 70 000+ bővítmény
- Jelentés készítés

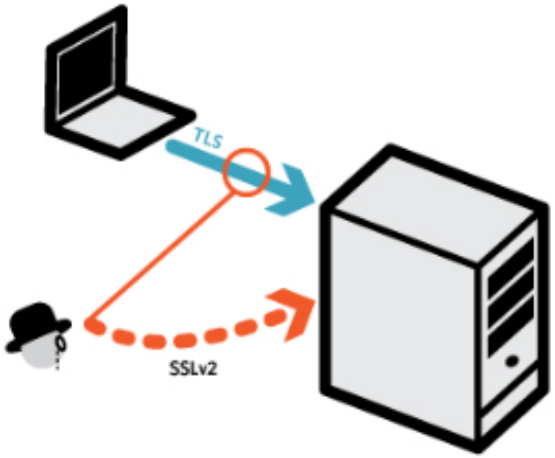
Funkciók

- Alap hálózati szkennelés
- Malware szkennelés
- Host feltérképezés
- Szabályok auditálása
- Drown (Decrypting RSA with Obsolete and Weakened eNcryption) detektálása
- PCI (Payment Card Industry) külső szkenner

Labor feladat

A server is vulnerable to DROWN if:

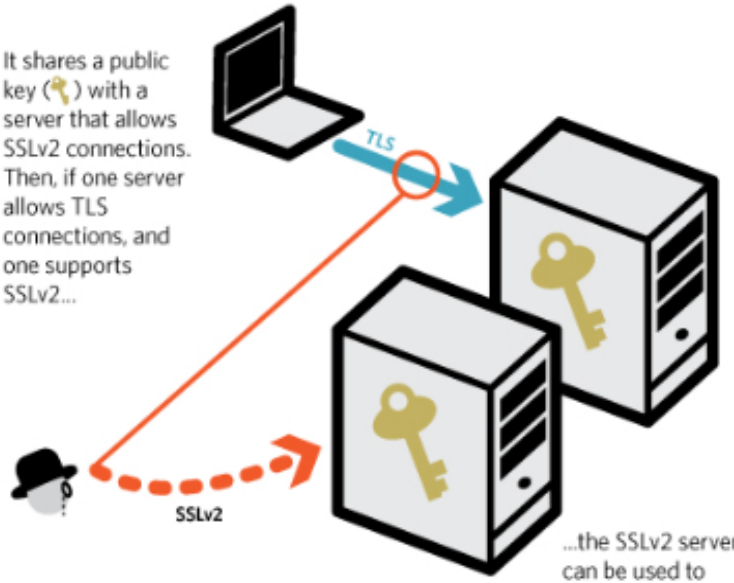
It allows both TLS and SSLv2 connections



17% | 83%

17% of HTTPS servers still allow SSLv2 connections

It shares a public key ( ) with a server that allows SSLv2 connections. Then, if one server allows TLS connections, and one supports SSLv2...



...the SSLv2 server can be used to attack the TLS server

17% | 16% | 67%

When taking key reuse into account, an additional 16% of HTTPS servers are vulnerable, putting 33% of HTTPS servers at risk

Előnyök

- Nagy pontosságú szkennelés alacsony hamis pozitív értékekkel
- Átfogó vizsgálati képességek és funkciók
- Több százezer rendszerre skálázható
- Egyszerű telepítés és karbantartás
- Alacsony adminisztrációs és üzemeltetési költségek
- Teljes lefedettség, beleértve a laptopokat és a mobil eszközöket is

Nessus letöltés

- https://www.tenable.com/downloads/nessus?loginAttempted=true
- Activation code https://www.tenable.com/products/nessus/nessus-essentials
- Tenable oktatási kézikönyv https://www.tenable.com/whitepapers/tenable-for-education-guide
- Dokumentáció https://docs.tenable.com/nessus/Content/GettingStarted.htm

Nessus telepítés és indítás

- sudo dpkg -i Nessus-10.3.0-debian9_amd64.deb
- start nessus (password kali)
  - /opt/nessus/sbin
    service nessusd start
  - /etc/init.d/
    nessusd start
- web browser host
  https://kali:8834/

Policies

Egyéni sablonok létrehozása
A vizsgálat során végrehajtott műveletek meghatározása

- Policies – New Policy
  - Advanced Scan
    Minden lehetőséget mi választunk ki útmutatás vagy javaslatok nélkül.
  - Basic Network scan
    Általában bármilyen host számára alkalmas.
  - Internal PCI network scan
    Belső szkennelés a Payment Card Institute számára
  - Web application test

Advanced Scan

Settings

- Name
- Discovery
  - Ping the remote host
  - Port Scanning
    Port scan range : default - Nessus service file
    find / -name ”nessus-services”
    less paranccsal láthatjuk a fájl tartalmát
    cat /opt/nessus/var/nessus/nessus-services |wc
    1. sorok száma, 2. szavak száma, 3. karakterek száma
    all ports: 1-65535

Advanced Scan

- Advanced
  - Scan IP addresses in a random order
    Scan legyen lopakodóbb.
  - Max simultaneous hosts per scan (30)
    Elkerülni a késéseket és a hálózati forgalmat.
  - Max number of concurrent TCP sessions per host (800)
    Felső korlát a hostok biztonsága érdekében.
  - Max number of concurrent TCP sessions per scan (2000)
    A hálózati forgalom biztonságban tartása.

Advanced Scan

Credentials
Megadhatja a hitelesítő adatokat, ha rendelkezik ezekkel az egyes szolgáltatások mélyreható vizsgálatához.
Plugins
Plugin family - plugins name
Enabled - Disabled

Scan eredmény

- Hosts
- Vulnerabilities
- History

Sérülékenységek szintjei

A Nessus öt szintre osztja a sebezhetőségeket:

- Info: nem sebezhetőségi információ (jó tudni)
- Alacsony: A támadó az információ alapján finomítja támadást, de a hiba nem lesz elegendő a kompromittáláshoz.
- Közepes: Információ szivárog a távoli hostról. (a támadó esetleg olyan fájlt is el tud olvasni, amelyhez nem lenne szabad hozzáférnie)
- Magas: A támadó tetszőleges fájlokat olvashat vagy parancsokat hajthat végre a távoli hoston.
- Kritikus: Egy eszköz ki tudja használni ezeket a sebezhetőségeket, és a legtöbb esetben a támadónak nem kell különösebb erőfeszítéseket tennie a kihasználásukhoz.

Sérülékenységek

- A sebezhetőség neve
- Rövid leírás
- Megoldási módszer
- Linkek, amelyek segítségével többet tudhat meg róla.
- Host és portok, ahol a sebezhetőség megjelenik.

További információk (kockázat, sebezhetőség, hivatkozás, kihasználó eszköz stb.)

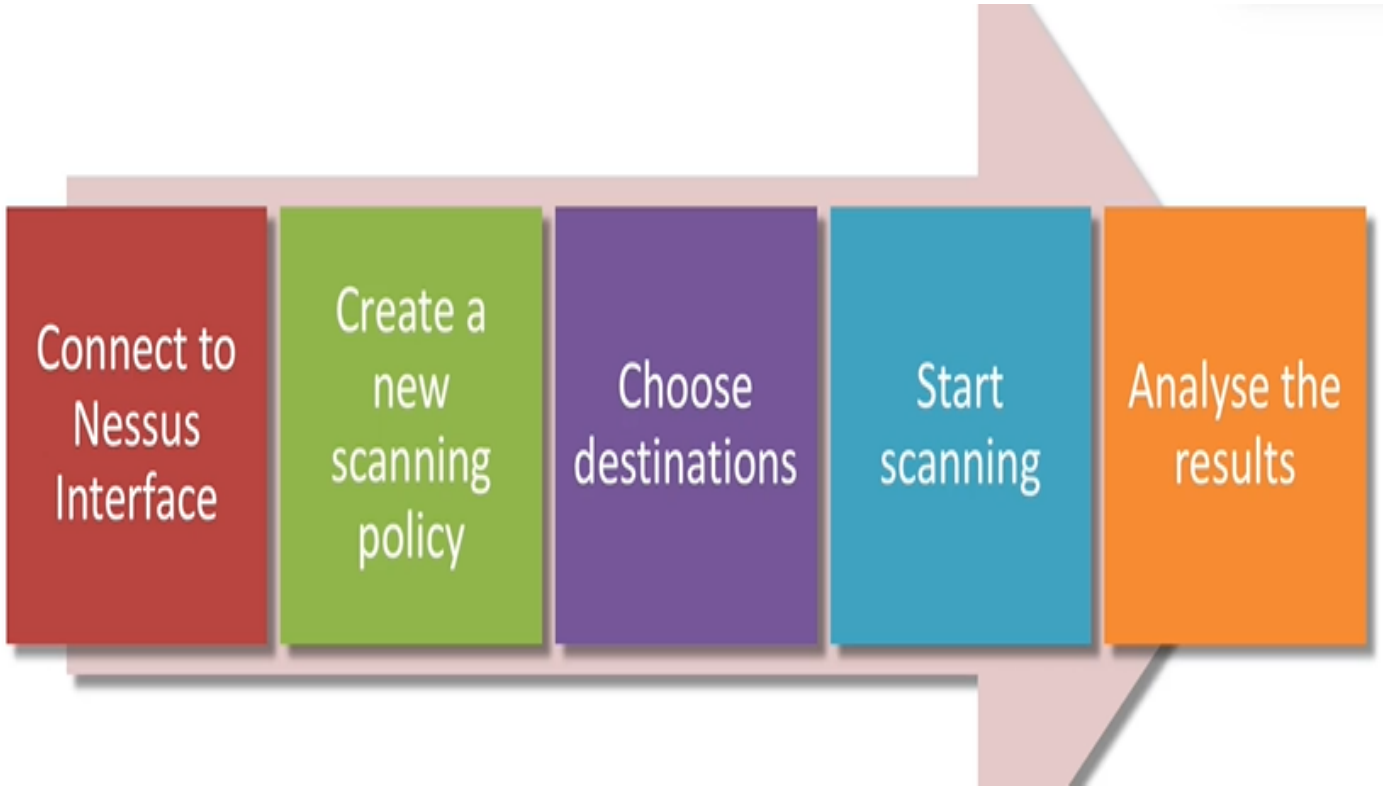
Scan Riport

Export

- PDF
- HTML
- CSV
- Nessus

- Vezetői összefoglaló
- Egyéni (csoportosítás gazdagép vagy bővítmény, sebezhetőségek vagy javítások szerint)
- Exportálás (a professzionális kiadás súlyossági szint szerint rendezve stb.)

Labor feladat



Köszönöm a figyelmet!