



Auditarea Securitatii Retelelor

Laborator

⌘ Descoperirea vulnerabilitatilor

[Vulnerabilitati]

Exista 2 categorii de vulnerabilitati tehnice:

- ⌘ **Erori de configurare**
- ⌘ **Erori de programare**

Si a 3-a categorie....

- ⌘ **Slabiciunea umana**

Descoperirea vulnerabilitatilor

⌘ Vulnerabilitati cunoscute

- ⌘ Manual (silentios, mai mult timp, false negatives)
 - ⌘ Necesita experienta
 - ⌘ Cautare vulnerabilitati in functie de serviciul descoperit
 - ⌘ <http://www.securityfocus.com/bid> , <http://www.kb.cert.org/vuls/>
<http://nvd.nist.gov/>, <http://osvdb.org/>
- ⌘ Automat (zgomotos, rapid, false positives)
 - ⌘ Scannere de vulnerabilitati
 - ⌘ Nessus, OpenVAS, QualisGuard, GFI LANGuard, Retina
 - ⌘ Nikto, w3af, Paros, BurpSuite, WebScarab, DirBuster

⌘ Vulnerabilitati noi (0-day)

- ⌘ Manual
 - ⌘ probleme de configurare, erori de logica in aplicatii
- ⌘ Automat
 - ⌘ Fuzzers: Spike, Peach, Sulley, JBroFuzz, etc

Exercitiul 0: Gasiti IP-ul masinii virtuale Windows

- ⌘ Parola de access a fost schimbata
- ⌘ Gasiti IP-ul in subnetul *vmnet8*
(configuratie NAT)
 - ⌘ You should know how to do this...

Exercitiul 1 – Instalare Nessus

1. Instalati Nessus pe masina virtuala BackTrack

✂ **Download:**

http://www.nessus.org/download/nessus_download.php (Ubuntu 8.10, 32 bit)

✂ **Instalare:** dpkg -i Nessus-4.2.2-ubuntu810_i386.deb

✂ **Adaugare user:** /opt/nessus/sbin/nessus-adduser

2. Activati Nessus si faceti update la plugin-uri

✂ **Obtineti un cod de activare pentru Home Feed**

<http://www.nessus.org/register/>

✂ **Primiti codul pe email**

✂ **Activati Nessus**

/opt/nessus/bin/nessus-fetch --register 1B31-4CF4-645B-699A-D515

✂ **Update plugins**

/opt/nessus/sbin/nessus-update-plugins

3. Porniti serverul Nessus

✂ /etc/init.d/nessusd start

✂ Verificati ca a pornit: netstat -ltnp

4. Porniti clientul Nessus

✂ Web browser: <https://localhost:8834> + autentificare

Exercitiul 2: Scanati masina virtuala Windows folosind Nessus

- ⌘ Creati o noua politica de scanare
 - ⌘ Performance tuning
 - ⌘ Dezactivati categoriile: Brute force attacks, Denial of service
 - ⌘ Pentru a gasi codul sursa al plugin-ului cu id 47030: `grep -r script_id\(47030\) /opt/nessus/lib/nessus/plugins/`
 - ⌘ NASL
- ⌘ Configurati o noua 'scanare' si porniti-o
- ⌘ Vizualizati raportul obtinut. Vulnerabilitati?
- ⌘ Salvati raportul in format html si nbe

Exercitiul 3: Scanarea serverului web folosind Nikto

- ⌘ `cd /pentest/web/nikto`
- ⌘ `./nikto -Help`
- ⌘ Scanati serverul web de pe masina virtuala specificand urmatorii parametri:
 - ⌘ Target host
 - ⌘ Target port
 - ⌘ Output file
 - ⌘ Output format
- ⌘ Vizualizati rezultatele. Vulnerabilitati?

[Exercitiul 4: Scanare aplicatie web – Paros (1)]

⌘ Configurati Paros proxy

⌘ `cd /pentest/web/paros`

⌘ `java -jar paros.jar&`

⌘ Firefox ⌘ Preferences ⌘ Network ⌘ Settings ⌘ Manual proxy configuration ⌘ [localhost : 8080]

⌘ Accesati aplicatia web in browser

⌘ Vizualizati cererile si raspunsurile HTTP in Paros

[Exercitiul 4: Scanare aplicatie web – Paros (2)]

- ⌘ Porniti crawler-ul pentru a gasi toate paginile din site (Paros ⌘ Analyse ⌘ Spider)
- ⌘ Configurati politica de scanare (Paros ⌘ Analyse ⌘ Scan Policy)
- ⌘ Porniti scanarea (Paros ⌘ Analyse ⌘ Scan)
- ⌘ Vizualizati rezultatele. Vulnerabilitati?
- ⌘ Salvati raportul in format html

[Exercitiul 5: Descoperirea directoarelor prin forta bruta]

- ⌘ `cd /pentest/web/dirbuster`
- ⌘ `java -jar DirBuster.jar`
- ⌘ Identificati subdirectoarele din directorul radacina al aplicatiei
- ⌘ Identificati subdirectoarele din directorul /vicnum al aplicatie

