Universitatea Politehnica Bucuresti
Facultatea de Automatica si Calculatoare
Master – Securitatea Retelelor Informatice Complexe

Auditarea Securitatii Retelelor

Laborator 2

- Descoperirea vulnerabilitatilor

Adrian Furtună, Ph.D.
adif2k8@gmail.com

Vulnerabilitati

- Tehnice:
  - Erori de proiectare / design
  - Erori de programare (bug-uri)
  - Erori de implementare / configurare
- Umane [1]
  - Atractia sexuala
  - Lacomia
  - Mandria
  - Increderea excesiva
  - Neglijenta
  - Compasiunea excesiva
  - Raspunsul la cereri ‘urgente’

[1] http://blogs.sans.org/securingthehuman/files/2011/01/Cisco.png

Descoperirea vulnerabilitatilor

- Vulnerabilitati cunoscute / publice
  - Manual (silentios, mult timp, false negatives)
    - Cautarea vulnerabilitatilor in baze de date publice si validare manuala:
      - http://www.securityfocus.com/bid, http://www.kb.cert.org/vuls/, http://nvd.nist.gov/, http://www.zerodayinitiative.com/advisories/published/, etc
  - Automat (zgomotos, rapid, false positives)
    - Folosind scannere de vulnerabilitati:
      - Generale: Nessus, OpenVAS, QualisGuard, GFI LAN Guard, Retina
      - Pentru web: skipfish, w3af, nikto, paros, burp, webscarab, dirbuster
- Vulnerabilitati noi (0-day)
  - Manual
    - Pot fi descoperite erori de configurare si erori de logica in aplicatii
  - Automat
    - Fuzzers: Spike, Peach, Sulley, JBroFuzz, FileFuzz, AxMan, etc

Exercitiul 1 – Instalare Nessus

Instalati Nessus pe masina virtuala BackTrack:

- **Download:** http://www.nessus.org/download/nessus_download.php (Ubuntu 10.04, 32 bit)
- **Instalare:** `dpkg -i Nessus-4.4.1-ubuntu910_i386.deb`
- **Adaugare user:** `/opt/nessus/sbin/nessus-adduser`
- **Activati Nessus** si faceti update la plugin-uri
  - Obtineti un cod de activare pentru Home Feed (pe email)

    http://www.nessus.org/register/
  - Activati Nessus:

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

    `/opt/nessus/sbin/nessus-update-plugins`
- **Porniti serverul Nessus:** `/etc/init.d/nessusd start`
- Verificati ca a pornit: `netstat –ltnp`
- **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/
```

- Configurati o noua ‘scanare’ si porniti-o
- Vizualizati raportul obtinut. Vulnerabilitati?
- Salvati raportul in format html si nbe

Exercitiul 3 – Scanati serverul 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 – Scanati aplicatia web folosind 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 – Scanati aplicatia web folosind 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 aplicatiei

Intrebari

?