Laborator 10. Securitatea Rețelelor Locale

Cunoștințe și abilități ce vor fi dobândite

- Descoperirea de informații despre o anumită rețea sau entitate
- Înțelegerea taxonomiei folosite în industrie pentru identificarea vulnerabilităților
- Folosirea utilitarelor în vederea descoperirii de vulnerabilități
- Înțelegerea tipului de atac MiTM (Man in the Middle) folosind ARP spoofing și DNS spoofing

Cheat sheet

- Cheat Sheet

Pregătire infrastructură de laborator

- **Reminder**: avem nevoie de o mașină virtuală a laboratorului. Vă rugăm urmăriți pagina aceasta pentru instrucțiuni, apoi reveniți.
- Schimbați utilizatorul curent în `root` folosind comanda

```
student@host:~$ sudo su
```

- Pentru a pregăti configurația de laborator, pe mașina virtuală (stația `host`) folosiți comenzile următoare din contul utilizatorului `root` de pe stația `host` (puteți da copy/paste la comenzi în terminal):

```
root@host:~# update_lab --force
root@host:~# start_lab mitm
```

- Deschideți trei tab-uri noi în terminal (folosiți combinația de taste `Ctrl+Shift+t`), și conectați-vă, din nou, la mașina virtuală folosind comanda `ssh` de mai sus.
- De pe cele trei noi tab-uri, conectați-vă la cele trei containere (`red`, `green` și `blue`).
- Pentru o conectare mai ușoară puteți folosi aliasul `go` (ex. `go red`)

În mod implicit folosiți contul `root` pentru conectare pe toate stațiile. Aveți nevoie de drepturi privilegiate pentru configurare. Folosiți contul `student` doar unde vi se cere explicit.

Introducere

Conform legilor în vigoare, scanarea IP-urilor în vederea obținerii de informații este ilegală. Pentru exercițiile de scanare utilizați doar IP-urile/Domeniile specificate în laborator.

Este estimat că la nivel global, companiile vor pierde aproximativ 10.5 trilioane de dolari până în 2025, o creștere de 15% per an.

Odată cu necesitatea digitalizării lumii în care trăim numărul de aplicații utilizate în medie de un om a crescut considerabil. Această creștere a numărului de aplicații a venit însă și cu un risc crescut în fața atacurilor cibernetice. Fiecare aplicație nouă introdusă în infrastructura digitală a unei entități duce și la creșterea **suprafeței de atac** a acesteia. Prin suprafața de atac [https://en.wikipedia.org/wiki/Attack_surface] se înțelege numărul total de puncte prin care o persoană neautorizată ar putea accesa un sistem.

Pentru a ne putea proteja în fața atacurilor cibernetice, este necesar să înțelegem fazele unui atac și ce reprezintă acestea.

În încercarea unui atacator de a avea acces la un sistem, acesta va trece prin următoarele faze generale:

1. Recunoașterea țintei

În această fază se urmărește culegerea de informații pentru ținta în cauză. Informațiile de interes pentru un atacator constau în detecția de hardware și software prezente. Această fază este extrem de importantă deoarece pe baza detecției aplicațiilor se pot identifica posibilele vulnerabilități.

În cadrul fazei de recunoaștere ne întâlnim cu două standarde foarte importante:

- **CPE (Common Platform Enumeration)** reprezintă o metoda structurată de identificare a unui software/hardware.

Exemplu: `cpe:2.3:a:microsoft:exchange_server:2016:cumulative_update_23:*:*:*:*:*:*` reprezentând:
`part="o",vendor="microsoft",product="exchange_server",version="2016", update="cumulative_update_23",edition=NA,language=NA,sw_edition="NA", target_sw=NA,target_hw="NA",other=NA)`

- **CVE (Common Vulnerabilities and Exposures)** reprezintă o metoda structurată de identificare a unei vulnerabilități. (exmplu: `CVE-2022-21978`)

Asocierea dintre cele două standarde este dată de faptul că unui **CPE** îi sunt asociate toate **CVE**-urile descoperite, spre exemplu pentru **CPE** folosit ca exemplu avem următoarele **CVE**-uri: `CVE-2022-21978, CVE-2022-21979, CVE-2022-21980, CVE-2022-24477, CVE-2022-24516, CVE-2022-30134, CVE-2022-34692, CVE-2022-41040, CVE-2022-41082, CVE-2022-41078, CVE-2022-41079, CVE-2022-41080, CVE-2022-41123`

2. Înarmarea pentru atac

Pe baza informațiilor obținute anterior, atacatorul va alege cele mai potrivite metode prin care va exploata vulnerabilitățile descoperite.

3. Livrarea atacului

Prin livrarea atacului se înțelege orice metodă prin care atacatorul ar putea obține acces in sistem. Aici putem discuta despre exploatarea factorului uman prin mesaje de tip phishing sau în funcție de vulnerabilitățile descoperite, acesta poate trimite diverse payload-uri către țintă. Odată cu livrarea atacului, dacă acesta a avut succes, atacatorul își va putea exercita controlul asupra sistemului.

În cadrul acestui laborator, vom trece prin toate fazele unui atac, folosind utilitare cunoscute sau servicii puse la dispoziție de CODA Intelligence [https://www.codaintelligence.com/product-overview//].

Navigare

Laboratorul 10

Exerciții

01. [10p] Aflare adresă IP publică

Pentru început, vrem să aflăm adresa IP publică cu ajutorul căreia ieșim în internet de pe mașina virtuală. Sistemul pe care lucrați în cadrul acestui laborator se află în spatele unei rețele cloud private și poate accesa Internetul datorită unei configurații NAT (Network Address Translation) și are un IP privat alocat de controller-ul de rețea cloud. Cum aflăm adresa noastră publică?

Reamintiți-vă care sunt clasele de adrese IP private și care sunt cele pentru adrese IP publice.

02. [10p] Aflare informații despre adresa IP publică

Mai departe, vrem să aflăm din ce subnet face parte adresa publică, cine se ocupă de aceasta, cărei organizații îi aparține și cărei țări i-a fost alocată.

Whois este un protocol cerere răspuns care este folosit pentru a interoga informații despre resurse din Internet precum: numele de domeniu, subnet-uri de adrese IP sau sistemul autonom (autonomous system) din care face parte. Vom folosi utilitarul **whois** pentru a afla aceste informații despre adresa IP descoperită la exercițiul anterior:

```
root@host: whois <ip_ex_1>
```

Ce informații putem observa în output-ul obținut în urma rulării acestei comenzi? Care este subnet-ul din care face parte adresa noastră publică?

03. [10p] DNS Resolution

Scopul acestui exercițiu constă în aflarea unor informații de DNS despre un domeniu.

Tipurile de înregistrări DNS pot oferi informații despre resursele înregistrate și legătura dintre ele:

- **A** - înregistrare directă către IP-ul care găzduiește aplicația
- **CNAME** - un alias către altă înregistrare unde ar putea fi găzduită aplicația
- **MX** - înregistrare către adresa serverului de e-mail

Vom folosi utilitarul `nslookup` din pachetul `dnsutils` pentru a afla informații despre înregistrările DNS. Este posibil ca pachetul `dnsutils` să fie deja instalat pe `host`. Dacă nu este instalat, atunci puteți folosi următoarea comandă pentru a-l instala:

```
student@aldebaran:~$ apt install dnsutils
```

Folosim utilitarul `nslookup` pentru a afla informații despre înregistrări DNS specifice:

```
student@aldebaran:~$ nslookup -querytype=CNAME erp.codacloud.net
```

```
student@aldebaran:~$ nslookup -querytype=NS cs.pub.ro
```

```
student@aldebaran:~$ nslookup -querytype=MX cs.pub.ro
```

```
student@aldebaran:~$ nslookup -querytype=A erp.codacloud.net
```

04. [15p] Descoperirea porturilor TCP deschise

Mai departe, ne propunem să aflăm ce porturi sunt deschise pe anumite servere pentru a identifica serviciile care rulează și versiunile acestora ce pot avea vulnerabilități.

În cadrul acestui exercițiu (precum și a exercițiilor urmatoare), vom folosi următoarele host-uri:

- `hermes.codacloud.net`
- `hefaistos.codacloud.net`

Folosiți comanda `nmap` pentru a scana aceste adrese doar pe conexiuni TCP, utilizând porturile următoare: `21, 22, 23, 25, 53, 80, 138, 443, 8000 și 8080` (am ales aceste porturi deoarece sunt cele mai uzuale porturi pentru expunerea serviciilor/aplicațiilor în rețea).

Veți observa porturi care se află în starea `open`, `closed`, `filtered` (port filtrat de un firewall) și alte tipuri pe care le puteți găsi descrise aici [https://nmap.org/book/man-port-scanning-basics.html].

05. [10p] Determinarea versiunilor aplicațiilor descoperite

Pe lângă porturile expuse, descoperite anterior, dorim să aflăm și versiunile aplicațiilor și serviciilor care rulează pe acele porturi.

Aceste informații sunt foarte importante în contextul securității, pentru că anumite vulnerabilități sunt prezente doar în anumite versiuni.

Folosiți comanda `nmap` pentru a determina versiunile serviciilor care rulează peste protocolul TCP, identificate la exercițiul anterior.

Căutați în manual după `Version detection`.

Procesul de detectare a versiunilor îngreunează scanarea. Astfel, recomandăm folosirea parametrului de `timing template` cu valoarea maximă 5 (`-T5`). Acesta ne spune că scanarea va fi foarte agresivă cu ținta (default-ul este `-T3` normal mode).

Folosind această valoare (insane mode), se pot depista mult mai ușor sistemele de securitate implementate în infrastructura țintă. Tot pentru a economisi timp, putem folosi parametrul `-n` pentru a nu face rezolvare de DNS.

Pentru a fi mai greu de detectat de către sistemele de securitate, este recomandat să se evite trimiterea pachetelor de ICMP (fără ping) folosind opțiunea `-Pn`

Pentru ca utilitarul nmap să ofere mai multe informații despre ceea ce a scanat, puteți utiliza opțiunea de `verbosity`.

Mai exact, puteți crește nivelul de detaliu al informațiilor afișate prin adăugarea parametrului `-v`. Puteți, de asemenea, crește nivelul de abundență a informației prin utilizarea unui număr mai mare de v-uri.

06. [10p] Analiza securității rețelei prin intermediul browser-ului

Așa cum a fost menționat anterior, livrarea atacului poate consta într-un atac de tip phishing prin care un utilizator ar putea descărca un executabil malițios. Serviciul următor verifică din perspectiva utilizatorului, securitatea browser-ului folosit, de la încercarea de descărcare a unui virus până la metodele de criptare folosite de browser.

First Name: `student`

Last Name: `rl`

E-mail: `student.rl@codaintelligence.com`

Company website: `laboratorrl.codaintelligence.com`

Utilizați serviciul de mai jos, folosind credențiale oferite mai sus, pentru a verifica securitatea browser-ului folosit: CODA Intelligence | Fingerprint (codacloud.net) [https://dev-catalina.codacloud.net/checkup/]

07. [10p] Utilizarea serviciilor de detectare a vulnerabilităților

Culegerea informațiilor despre ținta aleasă poate fi realizată manual, așa cum am observat în cadrul exercițiilor 1-5, sau se pot utiliza servicii existente.

Două astfel de platforme pe care le vom folosi sunt dnsdumpster [https://dnsdumpster.com/] și shodan [https://www.shodan.io/].

- Dnsdumpster este o platformă care ne permite să descoperim hosturi într-un domeniu, precum și informații suplimentare despre acestea.
- Shodan este o platformă care stochează date despre sisteme conectate la internet și pe care o putem interoga pentru a obține informații precum tehnologiile folosite, vulnerabilitățile și porturile deschise ale hosturilor.

1. Utilizați **dnsdumpster** pentru a scana hermes.codacloud.net în vederea obținerii de informații despre serverele ce sunt legate de domeniu, precum și despre adresa sau adresele IP ale acestuia.

1. Utilizați **shodan** pentru a descoperi vulnerabilitățile hostului pe baza adresei IP obținute la subpunctul 1. Introduceți adresa IP în câmpul `Search` al paginii web.

08. [15p] Rulare Denial of Service pe un server web

În acest exercițiu ne propunem să provocăm un comportament distructiv asupra unui anumit serviciu. Astfel, vom realiza un atac de tip Denial of Service asupra unui server web. Pe `red` există un server web (apache2) deja instalat. Verificați dacă acesta este pornit.

```
root@red:~# /etc/init.d/apache2 status  # Verificați dacă serverul web este pornit
```

Pe sisteme aveți instalat un text web browser. Rulați comanda `elinks` și accesați adresa `http://192.168.1.2/ [http://192.168.1.2/]`. Ar trebui să obțineți pagina implicită a serverului web Apache2 Ubuntu.

În continuare, vom folosit un utilitar de Denial of Service numit `slowloris` pe care îl avem deja instalat pe `green`. Urmăriți README-ul de la această adresă [https://github.com/gkbrk/slowloris].

Porniți un nou terminal pe sistemul `host`. Rulați `tcpdump` pe interfața de rețea `veth-red`, urmărind pachetele primite. Acum puteți porni tool-ul asupra serverului web de pe `red`. Încercați să accesați din nou serverul web. Mai funcționează?

```
root@student:~# tcpdump -i veth-red -n
```

- Dacă server-ul web încă vă răspunde, folosiți combinația de taste CTRL+R pentru a da refresh la pagina din `elinks`.
- Dacă încă funcționează serverul, încercați să rulați tool-ul din mai multe terminale până când nu mai răspunde.

9. [Bonus - 20p] Rulare Man in The Middle

În cadrul acestui exercițiu, ne propunem să simulăm un atac de tip Man in the Middle (MitM). Pentru aceasta, vom considera stația `red` ca fiind sistemul de pe care se inițiază atacul și stația `green` sistemul victimă. Vom încerca să capturăm traficul către `https://curs.upb.ro/ [https://curs.upb.ro/]` și să îl redirecționăm către un server web malițios aflat pe stația `red`. Într-un scenariu real, un atacator ar putea să creeze o replică a unui site web cu scopul de a captura comportamentul victimei sau informații cu caracter personal (parole, adrese, opțiuni etc.).

Folosind ARP spoofing și DNS spoofing, vom crea un atac de tip MitM.

Pentru început, vom porni arpspoof:

```
root@red:~# arpspoof -i <interfață (red-eth0)> -t <ip_victimă 192.168.2.2> <ip_gateway 192.168.0.100> -r # apoi, în alt terminal:
root@red:~# ip a s    # pentru a vedea adresa MAC
root@green:~# arp -n    # comparați adresa MAC a statiei ''red'' cu cea înregistrată pentru gateway. Se poate observa pe mașina victimei faptul că adresa MAC a gatewa
```

Deoarece am pornit mai sus ARP spoofing, pachetele victimei trec pe la atacator, inclusiv cererile de tip DNS. Astfel, sistemul atacator (MiTM) va răspunde la aceste cereri în locul serverelor dedicate și va trimite drept rezoluție de nume pentru domeniul `curs.upb.ro` adresa IP scrisă într-un fișier `hosts` pe care va trebui sa îl creăm. În cazul de față aceasta adresa este adresa IP a atacatorului unde rulează o copie malițioasă a site-ului http://curs.upb.ro/ [http://curs.upb.ro/].

```
root@red:~# cat hosts
<adresa_mea_ip>    curs.upb.ro
(folosiți TAB!)
root@red:~# dnsspoof -f hosts
```

Pentru a valida succesul atacului, de pe stația `green` rulați browser-ul text `elinks` și accesați pagina `curs.upb.ro`. Veți observa faptul că, în locul paginii clasice, vă va apărea o pagină web diferită (pagina implicită Apache).

Resurse:

- http://www.irongeek.com/i.php?page=security/arpspoof [http://www.irongeek.com/i.php?page=security/arpspoof]
- http://techgenix.com/Understanding-Man-in-the-Middle-Attacks-ARP-Part [http://techgenix.com/Understanding-Man-in-the-Middle-Attacks-ARP-Part]

Navigare

Laboratorul 10