Curs 11
Hardening a server

Gestiunea serviciilor de rețea (GSR)
22 decembrie 2016

Departamentul de Calculatoare, Comunitatea RLUG

Cuprins

Câteva întâmplări

- 6.46 million LinkedIn passwords leaked online (June 2012)
  - `http://www.zdnet.com/article/6-46-million-linkedin-passwords-leaked-online/`
- $12,000 computer (Project Erebus v2.5), 8 AMD Radeon HD7970 GPU cards (August 2012)
  - are nevoie de 12 ore pentru a folosi *brute force* pe întreg spațiul de parole de 8 caractere printabile
  - `http://arstechnica.com/security/2012/08/passwords-under-assault/`
- NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say (October 2013)
  - `http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html`
- The Heartbleed Bug (April 2014)
  - vulnerabilitate în biblioteca OpenSSL, cea mai răspândită pentru comunicare criptate
  - `http://heartbleed.com/`
- Celebrity photo leak (September 2014)
  - ,,Security researcher reported brute force attacks were possible in March.''
  - `http://arstechnica.com/security/2014/09/apple-knew-of-icloud-api-weakness-months-before-celeb-photo-leak-broke/`

Și alte întâmplări

- Los Angeles Hospital Hit (February 2016)
  - răscumpărare plătită pentru recuperarea conturilor de email și a informațiilor pacienților
  - `https://www.theguardian.com/technology/2016/feb/17/los-angeles-hospital-hacked-ransom-bitcoin-hollywood-presbyterian-medical-center`
- IRS Security Breach (February 2016)
  - accesarea datelor personale a peste 700 000 de americani
  - `http://www.usatoday.com/story/money/2016/02/26/cyber-hack-gained-access-more-than-700000-irs-accounts/80992822/`
- Mossack Fonseca Leak (May 2016)
  - publicarea a 2.6 TB de documente private
  - `http://www.bbc.com/news/world-latin-america-36232142`
- Banner Health (August 2016)
  - pierderea datelor personale a 3.7 milioane de pacienți
  - `http://www.securityweek.com/37-million-exposed-banner-health-breach`
- Bitfinex Heist (August 2016)
  - furtul a echivalentului de 72 milioane USD
  - `http://www.reuters.com/article/us-bitfinex-hacked-hongkong-idUSKCN10E0KP`
- suma medie cererilor de răscumpărare: 679$ (față de 342$ în 2015)

Automotive

I was driving 70 mph on the edge of downtown St. Louis when the exploit began to take hold.

- *...the vents in the Jeep Cherokee started blasting* **cold air** *at the maximum setting...*
- *...the* **radio** *switched to the local hip hop station... at full volume.*
- *I spun the control knob left and hit the power button, to no avail.*
- *...the windshield* **wipers** *turned on, and wiper fluid blurred the glass.*
- *Immediately my* **accelerator** *stopped working.*

`https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/`

Cuprins

De ce securizăm un sistem?

- Securizarea are ca scop protejarea integrității, confidențialității și disponibilității datelor
- Trebuie avute in vedere atât atacurile externe cât și cele interne
- Consecințele unei breșe de securitate sunt uriașe (e.g. `https://techcrunch.com/2016/12/14/yahoo-discloses-hack-of-1-billion-accounts/`)

- După instalarea și configurarea inițială a oricărui serviciu urmează neapărat securizarea sa
  - Configurația implicită este generică și cunoscută

Ce protejăm?

- Ceva ce prezintă valoare
- În general informații care au un impact direct/indirect asupra lumii reale
- Protejăm trei proprietăți importante ale datelor: confidențialitatea, integritatea și disponibilitatea

Definiții

- Vulnerabilitate: defect care poate fi explotat în cadrul unui sistem
- Atac: metoda de exploatare a unei vulnerabilități
- Threat / Threat model: Strategia de planificare folostă de un atacator
- Trusted Computing Base: mulțimea componentelor considerate sigure peste care se construiesc mecanisme de securitate

Suprafață de atac

- Suprafața de atac reprezintă suma tuturor aplicațiilor și bibliotecilor care pot fi folosite de un atacator pentru a modifica starea sistemului
- Scopul securizării unui sistem constă în a minimiza această suprafață până la minimul necesar astfel încât sistemul să poată executa funcțiile pentru care a fost instalat și configurat

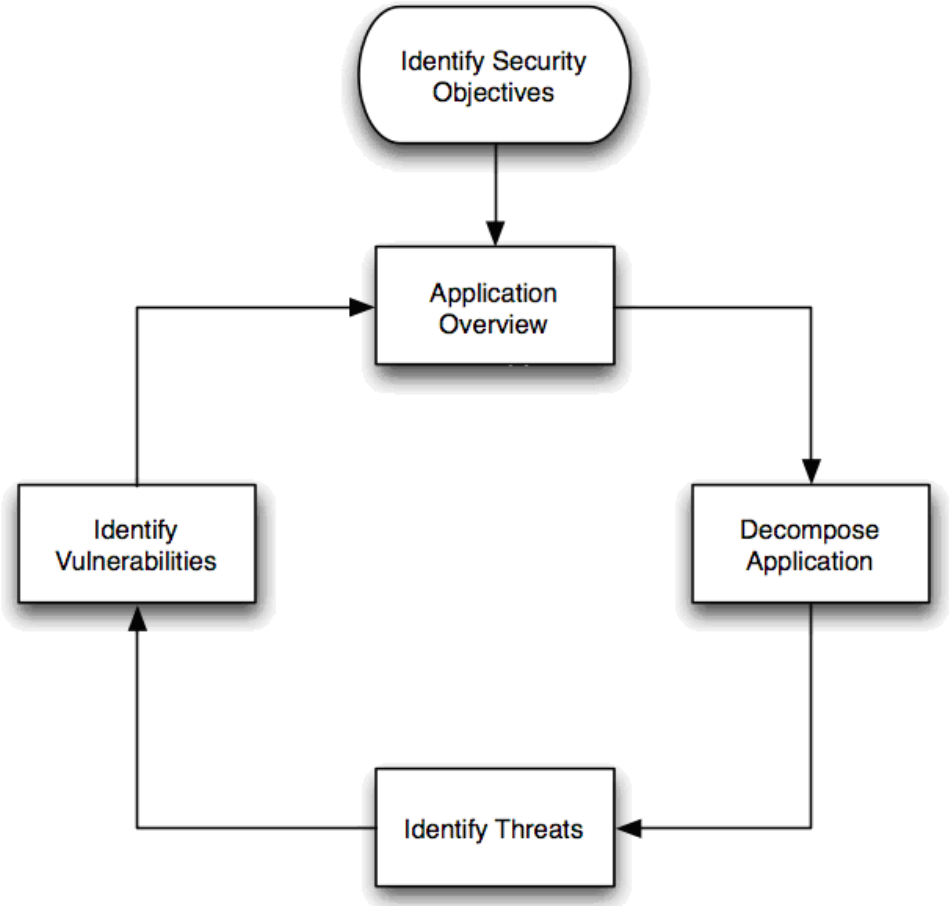
Principii

- Securitatea este un proces
- Least Privilege
  - Least Privilege este unul din principalele principii de securitate
  - Reprezintă executarea unei funcții folosind cel mai mic privilegiu posibil pentru realizarea ei
  - Exemple triviale: drepturi pe fișiere, folosirea sudo
- Minimizarea Trusted Computing Base
- Defense in depth

Pași generali în securizarea unui sistem

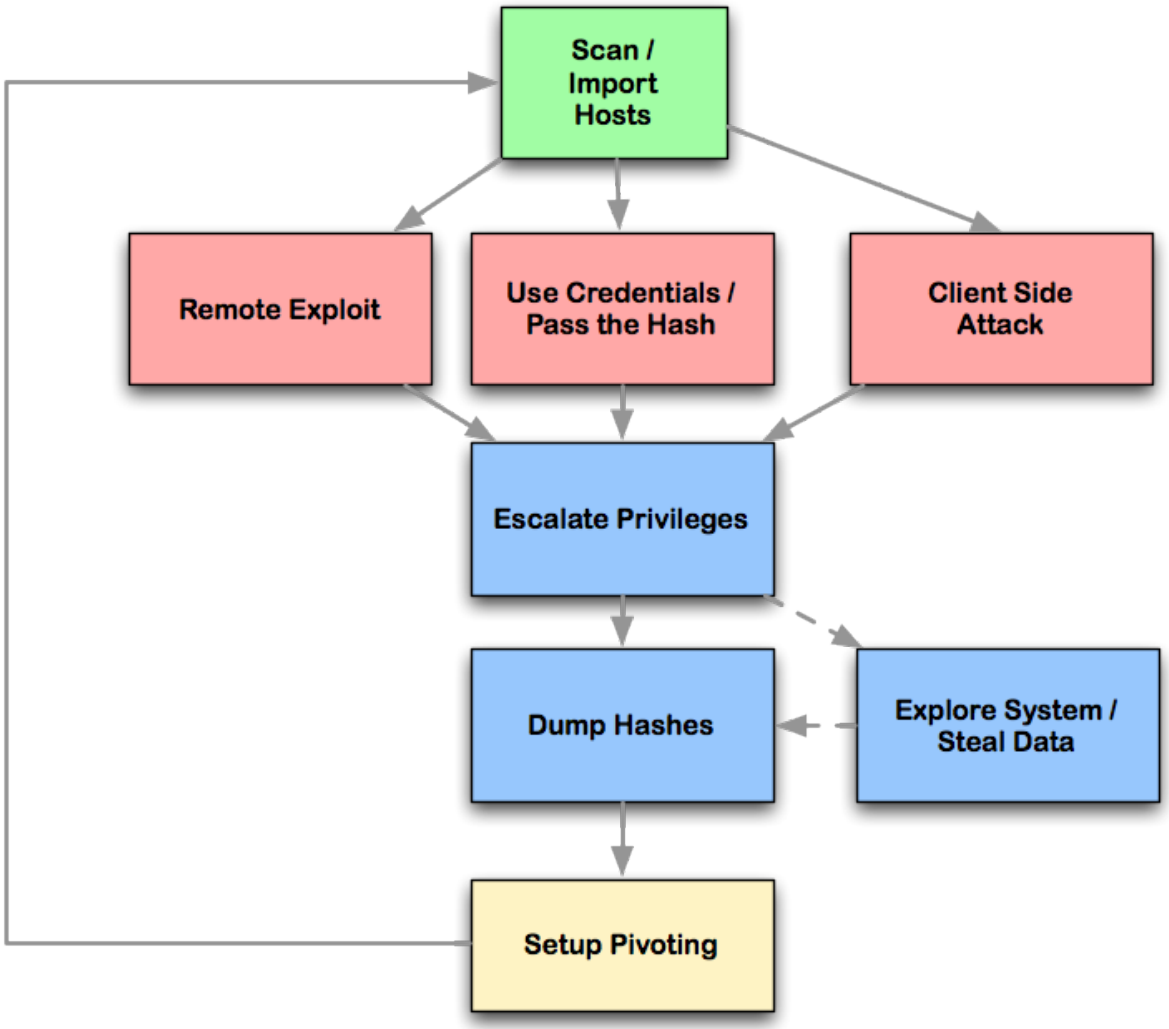
- Ștergerea pachetelor inutile pentru funcționarea sistemului (chiar dacă sistemul a fost instalat în mod minimal)
- Instalarea pachetelor necesare funcționării serviciului sau serviciilor pentru care sistemul a fost instalat
- Verificarea porturilor deschise (`netstat`) și
  - închiderea aplicațiilor care nu sunt necesare
  - modificarea configurației și punerea anumitor aplicații să asculte doar pe localhost
  - permiterea prin firewall doar a conexiunilor de încredere (cele de management pentru SSH)
- Configurarea permisiunilor minime pentru sistem
- Folosirea `chroot` acolo unde este posibil pentru limitarea accesului la sistemul de fișiere (de exemplu BIND)

Threat Model



https://www.owasp.org/images/9/97/Threat_Model_Flow.gif

Attack Tree



http://www.fastandeasyhacking.com/images/hackingprocess.png

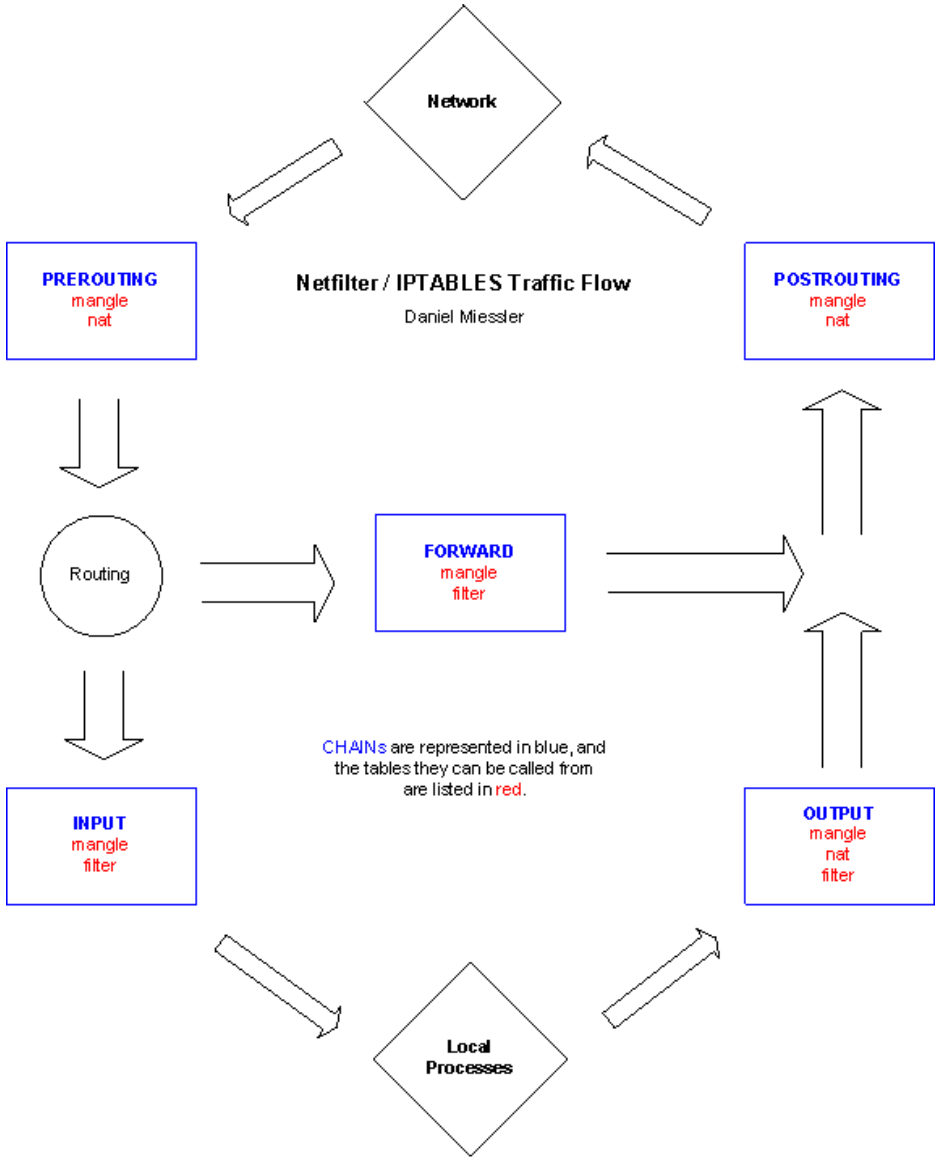
Cuprins

Monitorizarea conexiunilor active - netstat

Exemplu de rulare netstat

```
# netstat -antplu
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      1506/httpd
tcp        0      0 0.0.0.0:21              0.0.0.0:*               LISTEN      1320/vsftpd
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      1301/sshd
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN      1489/sendmail
tcp        0      0 0.0.0.0:443             0.0.0.0:*               LISTEN      1506/httpd
tcp        0      0 127.0.0.1:199           0.0.0.0:*               LISTEN      1289/snmpd
tcp        0      0 0.0.0.0:3306            0.0.0.0:*               LISTEN      1457/mysqld
tcp        0     40 10.1.5.14:22            10.1.3.6:50778          ESTABLISHED 38859/sshd
tcp        0      0 :::22                   :::*                    LISTEN      1301/sshd
tcp        0      0 :::3128                 :::*                    LISTEN      1530/squid
udp        0      0 0.0.0.0:51451           0.0.0.0:*                           1530/squid
udp        0      0 0.0.0.0:161             0.0.0.0:*                           1289/snmpd
udp        0      0 0.0.0.0:69              0.0.0.0:*                           1309/xinetd
udp        0      0 :::34518                :::*                                1530/squid
```

Traversare pachete prin iptables/netfilter



https://danielmiessler.com/images/DM_NF.PNG

Exemplu de configurare de firewall

Configurare firewall folosind `iptables`

```
iptables -t filter -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -t filter -A INPUT -p TCP --dport 22 -s 1.2.3.4/0 -j ACCEPT
iptables -t filter -A INPUT -p TCP --dport 80 -j ACCEPT
iptables -t filter -j DROP
```

Network IPS

- *Intrusion Prevention System*
- Aplicațiile pot fi vulnerabile la atacuri venite de la cereri din rețea
- Un sistem de tip IPS poate inspecta traficul înainte să ajungă la aplicație și să:
  - verifice existența unui conținut malițios (pe bază de semnături)
  - verifice respectarea standardelor pentru protocolul respectiv
- `snort` este IPS-ul `de facto` pe Linux

Cuprins

Integritatea fișierelor

- O dată un sistem instalat și configurat, cu excepția directoarelor de lucru, fișierele nu trebuie să se mai schimbe (doar în cazul în care se fac actualizări de software)
- Dacă, între timp, un fișier se modifică, acest lucru poate semnala faptul au avut loc modificări neautorizate
- Exemplu: Tripwire (în versiunea comercială sau Open-Source)

Rookits & Rootkit hunters

- Un `rootkit` este o aplicație sau o colecție de aplicații al căror scop este permiterea accesului unui atacator la un sistem de interes
- Un `rootkit hunter` este o aplicație care este rulată pe sisteme suspecte pentru a verifica existența unui rootkit
  - se realizează de pe un suport considerat sigur și protejat la scriere

Cuprins

Cursurile 9 și 10

Cuprins

Resurse utile

- https://www.giac.org/paper/gcux/188/introduction-file-integrity-checking-unix-systems/104739
- http://illmatics.com/Remote%20Car%20Hacking.pdf
- https://www.cs.princeton.edu/courses/archive/fall04/cos597B/lectures/systemsprinciples2.ppt