Security of Distributed Software

SS 2020 – 1. Tutorial

Valentin Siegert M.Sc.

Shovra Das M.Sc.

VSR.Informatik.TU-Chemnitz.de

Form:

- Detailing course knowledge
- Discussion
- Homework (voluntary)

News, Materials:

- http://vsr.informatik.tu-chemnitz.de/news/
- http://vsr.informatik.tu-chemnitz.de/edu/2020/svs/
- Opal: Security of Distributed Software SS2020

Contact

- valentin.siegert@informatik.tu-chemnitz.de
- shovra.das@informatik.tu-chemnitz.de
- 1/B204

Repetition

Which types of malware do you know?

Virus, worm, trojan horse, spywares, rootkits, a logic bomb, ransomware...

What are the differences?

Explain the following:

- Flooding
- Sniffing
- Spoofing
- (D)DOS
- Man-in-the-Middle

Task 1

The following activities are usually performed to take control over a network device:

Activity	Goals	Defence mechanisms
Network analysis	Finding potential attack targets	Forbid ping responses, VLAN, disconnect end devices
Target System scanning	Identifying of software and services on target system	Avoid using standard ports, honeypots, disable unused servies, firewalls
Break-in	Take-over of control of target system	Block senders with unusal behavior, use strong password, update software
Exploitation	Exploits the weaknesses or failures of a system or an application to obtain privileges	Patch system and applications to fix weak points

Task 2

Which IT entities can become a target of attack? Name examples for attacks. Fill in the table.

Users

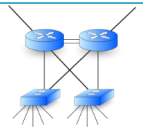

Applications



Operation systems




End devices



Network

Which IT entities can become a target of attack?

Class	Objects	Examples
Network infrastructure	Router, Switches, Connections	Cable break, Flooding, Sniffing, MAC-Spoofing, Routing/Switching-Tables
End devices	Clients (PC, Laptops, Smartphones, IoT), Server, Proxies, Gateways	Physical takeover / destruction
Operating systems	Protocols, Libraries, Data stock (user & rights management, certificates)	SYN-Flooding, updates restraint, ping-of-death, Rootkits, Exploits, Virus, Worms
Applications and services	DNS/Mail/Web services, Browser, Firewalls, FTP, Database, Web apps	XSS, CSRF, Brute-Force, SQL-Injection, Dictionary attack, Port scanning
Users	Laziness, Inattention, Ignorance (Social Engineering)	Password guessing, phishing

Target system scanning: nmap

Zenmap

Scan Werkzeuge Profil Hilfe

Ziel: 134.109.192.15 Profil: Intense scan Scan Abbrechen

Befehl: nmap -T4 -A -v 134.109.192.15

Rechner Dienste

Betriebssystem Rechne

iki.info

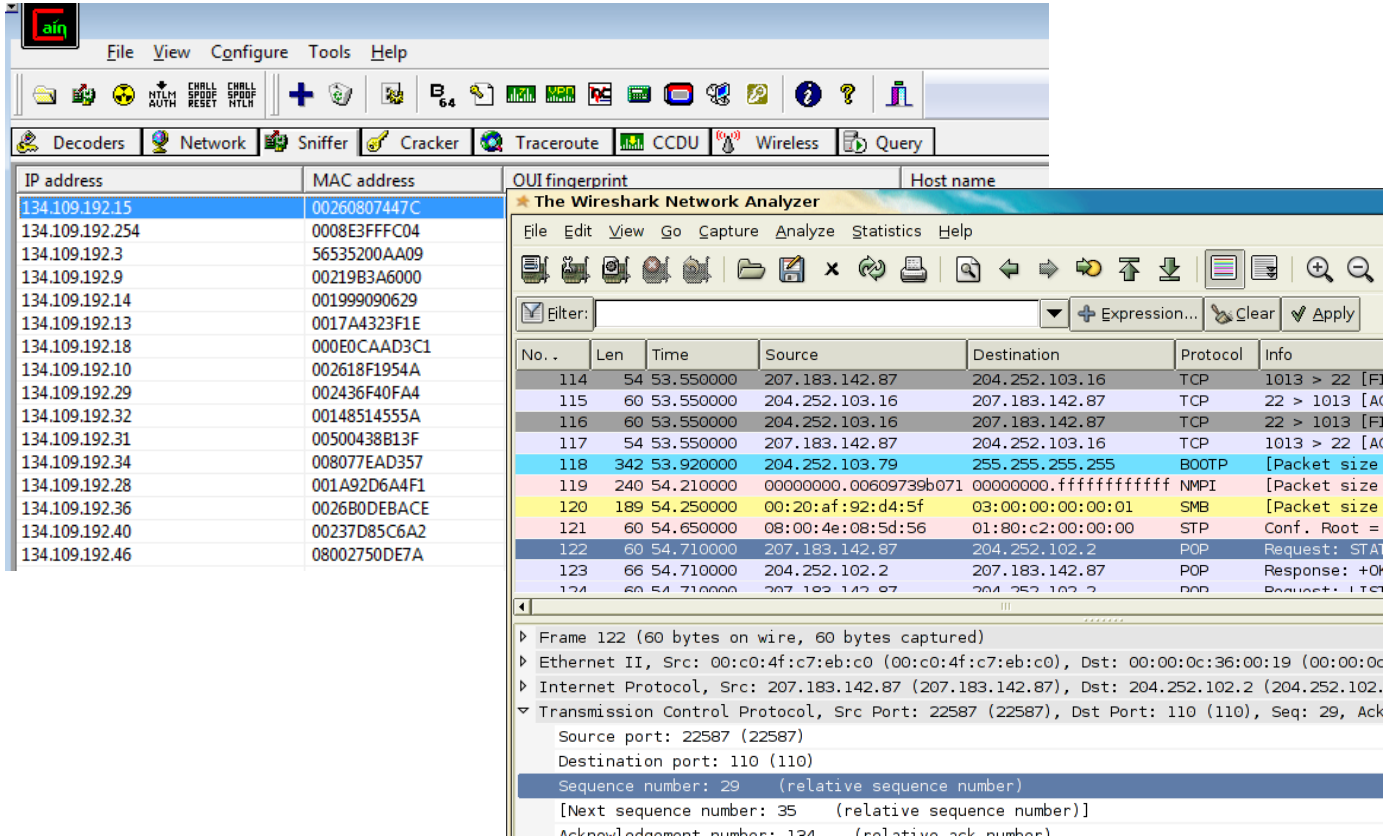
Filtere Rechner

Nmap-Ausgabe Ports / Rechner Netzstruktur Rechner-Details Scans

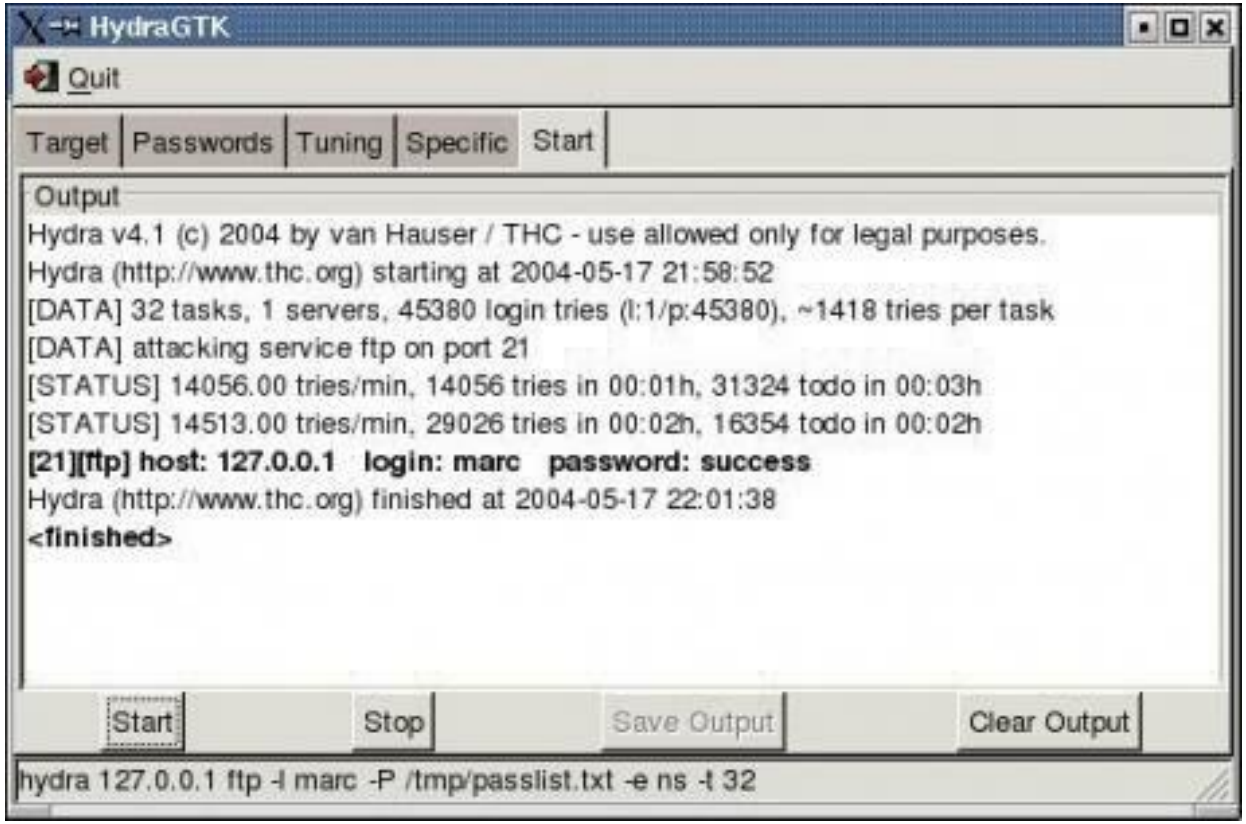
nmap -T4 -A -v 134.109.192.15 Details

```
All 1000 scanned ports on iki.informatik.tu-chemnitz.de
(134.109.192.15) are closed (965) or filtered (35)
MAC Address: 00:26:08:07:44:7C (Apple)
Device type: general purpose|phone|media device|specialized
Running: Apple iOS 4.X, Apple Mac OS X 10.6.X|10.5.X, Apple
iPhone OS 1.X|2.X|3.X, VMware ESX Server 3.X
Too many fingerprints match this host to give specific OS
details
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.57 ms iki.informatik.tu-chemnitz.de (134.109.192.15)

Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any
incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.62 seconds
           Raw packets sent: 1524 (67.610KB) | Rcvd: 976
(39.360KB)
```

Network analysis: Cain & Abel, Wireshark



Break-in: Hydra



Task 3

Inform yourself about the nmap tool.

https://www.stationx.net/nmap-cheat-sheet/

https://nmap.org/book/man.html

Answer the following questions:

- Find the names of all PCs in the IP range 134.109.193.0/24. Which of them are currently online?
- Which services run on the machine tan.informatik.tu-chemnitz.de?
- Which operating system is installed on pauline.informatik.tu-chemnitz.de?

Task 4

Which attacks / possibilities to recover passwords do you know?

Find out the password from the resource http://pauline.informatik.tu-chemnitz.de/webdav_http_basic/secret.jpg (username: hello) by applying the following techniques (using a self written program):

- Dictionary attack (using vocabulary passlist.txt)
- Bruteforce (limited to 3 letters)

VSR

Your feedback on today's session:

mytuc.org/tgxs

Questions?

valentin.siegert@informatik.tu-chemnitz.de

VSR.*Informatik*.TU-Chemnitz.*de*