



VSR://EDU/SVS

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

0 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 services, firewalls
Break-in	Take-over of control of target system	Block senders with unusual 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

2 Task 2

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



Users



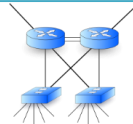
Applications



Operation systems



End devices

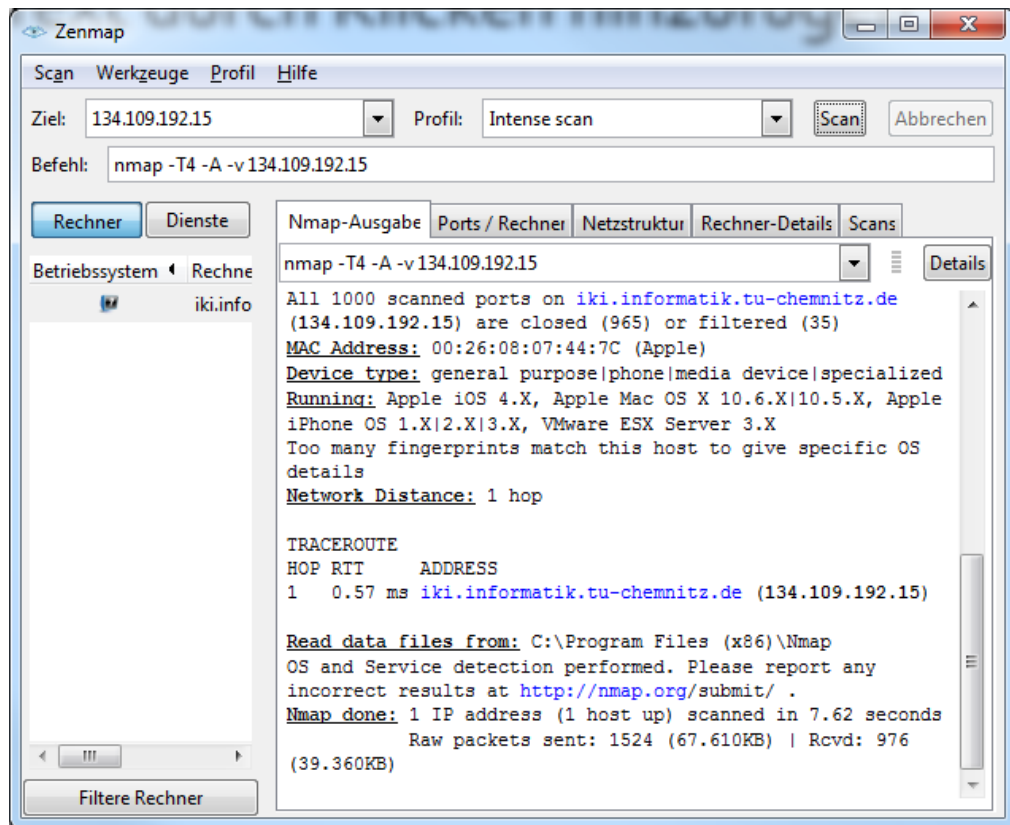


Network

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



Network analysis: Cain & Abel, Wireshark

The image shows two network analysis tools side-by-side. On the left is Cain & Abel, displaying a list of IP addresses and MAC addresses. On the right is Wireshark, showing a packet capture list and a detailed view of a selected packet (Frame 122).

Cain & Abel Interface:

IP address	MAC address
134.109.192.15	00260807447C
134.109.192.254	0008E3FFFC04
134.109.192.3	56535200AA09
134.109.192.9	00219B3A6000
134.109.192.14	001999090629
134.109.192.13	0017A4323F1E
134.109.192.18	000E0CAAD3C1
134.109.192.10	002618F1954A
134.109.192.29	002436F40FA4
134.109.192.32	00148514555A
134.109.192.31	00500438B13F
134.109.192.34	008077EAD357
134.109.192.28	001A92D6A4F1
134.109.192.36	002680DEBACE
134.109.192.40	00237D85C6A2
134.109.192.46	08002750DE7A

Wireshark Interface:

The Wireshark Network Analyzer

File Edit View Go Capture Analyze Statistics Help

Filter: + Expression... Clear Apply

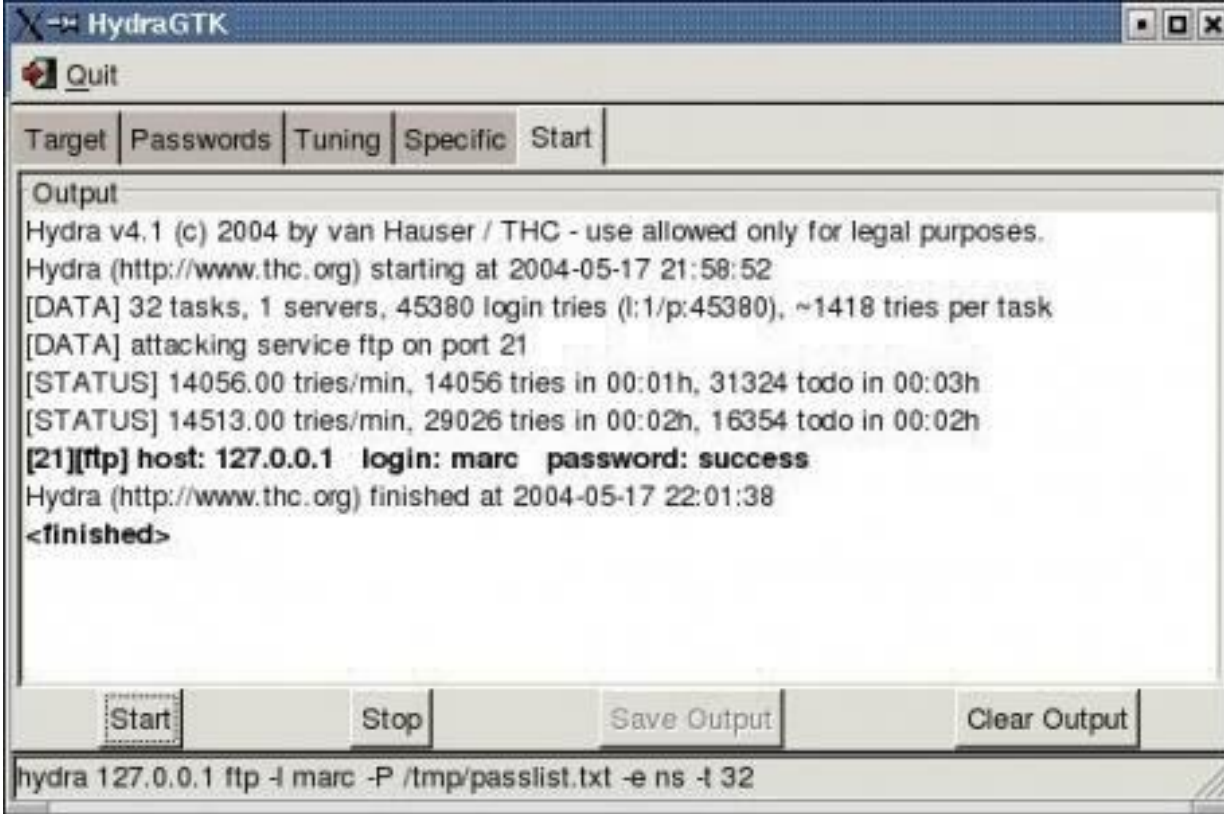
No. .	Len	Time	Source	Destination	Protocol	Info
114	54	53.550000	207.183.142.87	204.252.103.16	TCP	1013 > 22 [F]
115	60	53.550000	204.252.103.16	207.183.142.87	TCP	22 > 1013 [A]
116	60	53.550000	204.252.103.16	207.183.142.87	TCP	22 > 1013 [F]
117	54	53.550000	207.183.142.87	204.252.103.16	TCP	1013 > 22 [A]
118	342	53.920000	204.252.103.79	255.255.255.255	BOOTP	[Packet size
119	240	54.210000	00000000.00609739b071	00000000.ffffffffffff	NMPI	[Packet size
120	189	54.250000	00:20:af:92:d4:5f	03:00:00:00:00:01	SMB	[Packet size
121	60	54.650000	08:00:4e:08:5d:56	01:80:c2:00:00:00	STP	Conf. Root =
122	60	54.710000	207.183.142.87	204.252.102.2	POP	Request: STA
123	66	54.710000	204.252.102.2	207.183.142.87	POP	Response: +0
124	60	54.710000	207.183.142.87	204.252.102.2	POP	Request: +0

Frame 122 (60 bytes on wire, 60 bytes captured)

- Ethernet II, Src: 00:c0:4f:c7:eb:c0 (00:c0:4f:c7:eb:c0), Dst: 00:00:0c:36:00:19 (00:00:0c:36:00:19)
- Internet Protocol, Src: 207.183.142.87 (207.183.142.87), Dst: 204.252.102.2 (204.252.102.2)
- Transmission Control Protocol, Src Port: 22587 (22587), Dst Port: 110 (110), Seq: 29, Ack: 124, Len: 60, Win: 0, Flags: [RST, FIN]

Source port: 22587 (22587)
Destination port: 110 (110)
Sequence number: 29 (relative sequence number)
[Next sequence number: 35 (relative sequence number)]
Acknowledgment number: 124 (relative ack number)

Break-in: Hydra



The screenshot shows the HydraGTK application window. The title bar reads "HydraGTK". Below the title bar is a menu bar with a "Quit" option. A tabbed interface is visible with tabs for "Target", "Passwords", "Tuning", "Specific", and "Start", with "Start" being the active tab. The main area is labeled "Output" and contains the following text:

```
Hydra v4.1 (c) 2004 by van Hauser / THC - use allowed only for legal purposes.  
Hydra (http://www.thc.org) starting at 2004-05-17 21:58:52  
[DATA] 32 tasks, 1 servers, 45380 login tries (l:1/p:45380), ~1418 tries per task  
[DATA] attacking service ftp on port 21  
[STATUS] 14056.00 tries/min, 14056 tries in 00:01h, 31324 todo in 00:03h  
[STATUS] 14513.00 tries/min, 29026 tries in 00:02h, 16354 todo in 00:02h  
[21][ftp] host: 127.0.0.1 login: marc password: success  
Hydra (http://www.thc.org) finished at 2004-05-17 22:01:38  
<finished>
```

At the bottom of the window, there is a status bar with four buttons: "Start", "Stop", "Save Output", and "Clear Output". Below the status bar, the command line is visible:

```
hydra 127.0.0.1 ftp -l marc -P /tmp/passlist.txt -e ns -t 32
```



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?

4 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