

Preparing Targets for Penetration Tests

Dr. Alexander Schinner, T-Systems GEI GmbH



Agenda

1. **Why prepare targets for penetration tests?**
2. **How to prepare targets**
 - Terms and conditions
 - Tools and examples
3. **Take-home message**

Why prepare targets for penetration tests?

This presentation will NOT ...

- teach you how to become a hacker or penetration tester.
 - Long time is needed to gather knowledge, experience and feeling
- require deep knowledge of system internals.
 - Most problems are really simple to detect and fix
- save you a lot of work.
 - The security problems must be fixed sooner or later

This presentation will ...

- help you to learn a lot about your network and system,
- help you to save you time and money and
- help you to “survive” the visit of a penetration tester

Why prepare targets for penetration tests?

Based on long experience as penetration tester, there are two kinds of systems:

Highly secure systems

- Up-to-date operating system
 - Up-to-date application software
 - Well-configured network configuration
 - Well-configured server configuration
- A challenge for the tester



Open systems

- Operating System: No patches applied
 - Application software: Not configured
 - Default network configuration
 - Default server configuration
- Filling material for the report



Why prepare targets for penetration tests?

Because a penetration test for an **open system** is

- waste of time,
- waste of money and
- hides possible security issues.

Reason →

The penetration tester needs expensive time to analyze unimportant systems.

Before bringing their car to inspection, most people

- change oil
- check windscreen wiper and
- control tire pressure

because it is **simple** and the garage is **expensive**.



→ Why not do the same for your server?

What can we do? What are common problems?

We will try to detect:

- Unmanaged systems
 - Missing operating system patches
 - Outdated services
 - Forgotten systems
- Faulty network configuration
 - Too many open ports
 - Faulty firewall configuration
- Default server configuration
 - Demo pages, examples or management interfaces

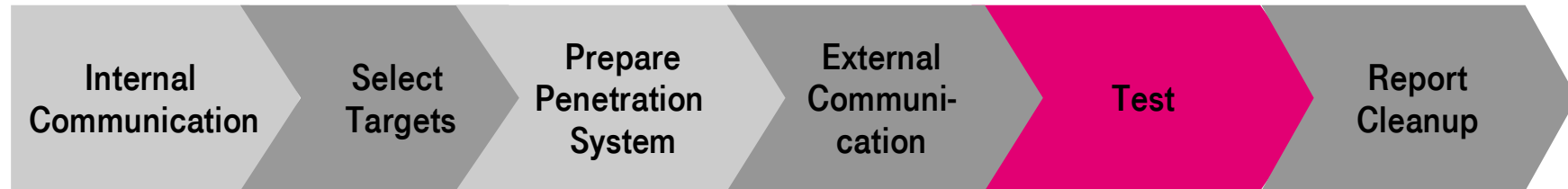
Examples:

- Worms welcome!
- Port 135,137,139 NBT
- Relicts in the rack

- Old Suse systems
- How about IPv6?

- JBoss JMX Console

Proceeding



- Approval by a manager
- Inform system operating
- Inform intrusion detection team
- Inform Firewall team

- Hostname, IP-address, subnet, etc.
- Placement of penetration system (internal, external)

- Linux
 - Backtrack
 - Knoppix
 - Ubuntu/Debian



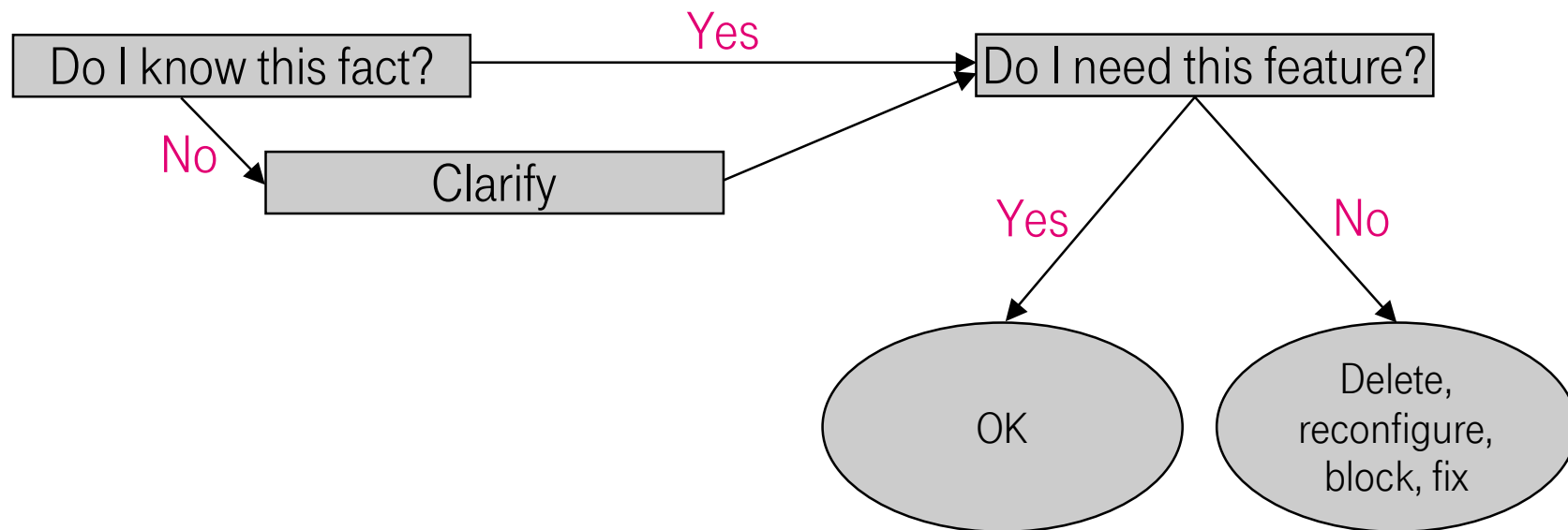
- Inform your ISP Provider
- Inform Customers

- Document what you did!

- Document the results
- Fix possible problems
- Explain results to management

Is it a finding?

For any information you get from a tool, please ask yourself the following questions:



How to prepare targets

Scanning Hosts with Nmap



- **Port scanner** written by Fyodor
- Probably the most frequently used tool for information gathering
- Discovers
 - computers and
 - open ports.
- Identifies the operating system
- Determines the application name and version number
- Command line tool, but GUI available (NmapFE, Zenmap)

Scanning Hosts with Nmap – IP Protocols



- Protocol scan

```
#> nmap -vv -sO -P0 host.name.test
Starting Nmap 4.53 ( http://insecure.org )
Scanning host.name.test (XX.XX.XX.XX) [256 ports]
Not shown: 249 open|filtered protocols
PROTOCOL STATE SERVICE
1 open icmp ok
6 open tcp ok
17 open udp ok
41 open ipv6 really necessary? → check
47 closed gre ok
50 closed esp ok
51 closed ah ok
```

Scanning Hosts with Nmap – Ping



- Echo request – classical ping

```
#> nmap -sP -PE host.name.test
```

```
Note: Host seems down ← If it is really up, but blocking  
our ping probes, try -PN
```

- Echo request – Timestamp request

```
#> nmap -sP -PP host.name.test
```

```
Host host.name.test (XX.XX.XX.XX) appears to be up.
```

illogical

- Echo request – Netmask request

```
#> nmap -sP -PM host.name.test
```

```
Host host.name.test (XX.XX.XX.XX) appears to be up.
```

Scanning Hosts with Nmap – TCP





- Service and Operating System

```
#> nmap -vv -sS -I -O -A -p1-65535 -P0 host.name.test
...
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          PureFTPd
22/tcp    open  ssh          OpenSSH 2.1.1p1
25/tcp    open  smtp         Sendmail smtpd
53/tcp    open  domain
80/tcp    open  http         Apache httpd
443/tcp   open  ssl/http     Apache httpd
993/tcp   open  ssl/imap     Dovecot imapd
Device type: general purpose|WAP|firewall|broadband router|media
device|VoIP gateway|server appliance
Running (JUST GUESSING) : Linux 2.6.X|2.4.X (96%)
```

plain text protocol → check
very old → check
sendmail vs. security → check
DNS → try zone transfer
try web scan
try web scan
??? → wait for penetration tester

Scanning Hosts with Nmap



Finding	Internal Scan	External Scan
ICMP echo, netmask and timestamp requests	Try to remove, if possible	Filter if possible
Plain text protocols like telnet, rsh, rlogin	Switch to ssh, if possible	Remove
Typical MS Windows ports 135, 137, 139, 445	It depends	Remove 
IPv6, IPsec, GRE, etc.	It depends	It depends
Oracle, MySQL, PostgrSQL	It depends	Remove 

Scanning Hosts with Nessus



- **Vulnerability scanning** software from Tenable Network Security
- World's most popular vulnerability scanner
- Detects potential vulnerabilities on the tested systems like
 - Access to sensitive data on a system
 - Misconfigurations like an open mail relay
 - Default passwords, a few common passwords, and blank/absent passwords
 - Denials of service against the TCP/IP stack.
- Two components:
 - `nessusd` (daemon) does the scanning,
 - `nessus` (client) controls scans and presents results
- Different GUI for version 2.x and 3.x

Scanning Hosts with Nessus - Starting Nessus



```
root@host:~# nessus-adduser

Login : bobo
Authentication (pass/cert) [pass] : pass
Login password : *****
Login password (again) : *****

Enter the rules for this user,
and hit ctrl-D once you are done :
ctrl-D

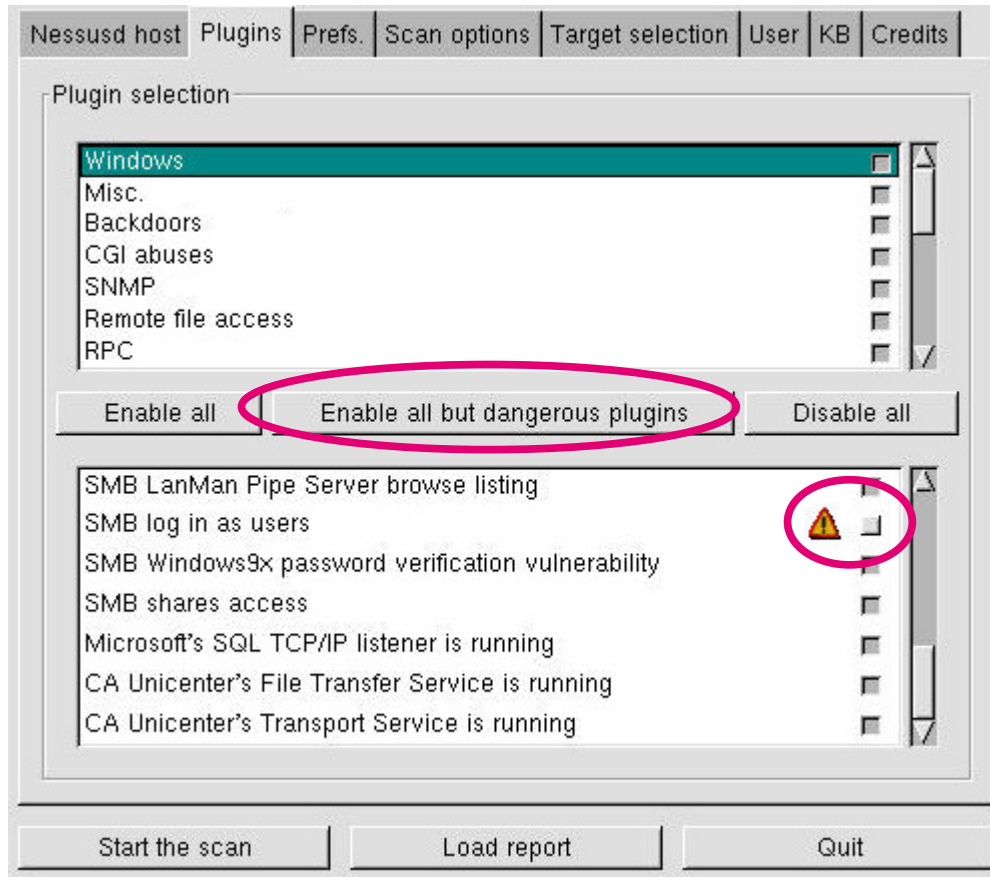
Login          : bobo
Password       : *****
DN             :

Is that ok ? (y/n) [y] y
user added.
root@host:~# nessusd -D
All plugins loaded
root@host:~# NessusClient
```

... **T** ... Systems ...

Preparing Targets for Penetrati

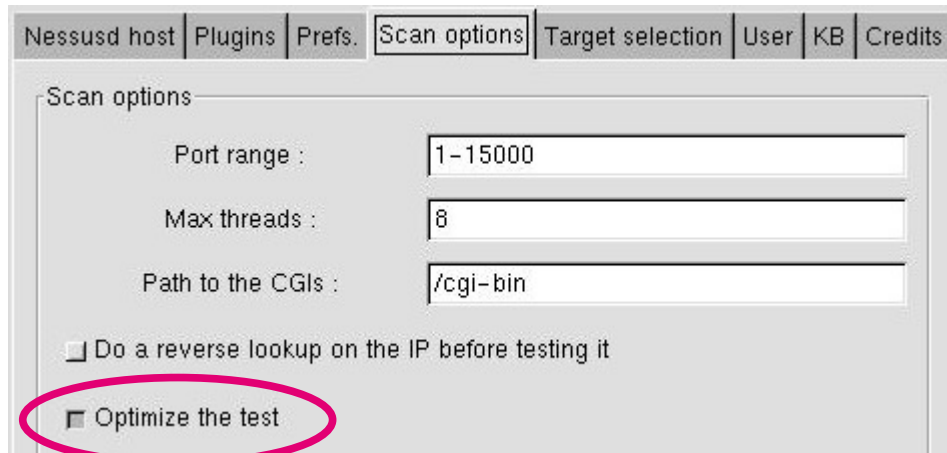
Scanning Hosts with Nessus - Configuration



Plugins

- List of all vulnerability tests available
- Grouped by family
- Tick box to enable or disable plugins
- Yellow triangle: test has the potential to interrupt or even crash services
- Try “Enable all but dangerous plugins”

Scanning Hosts with Nessus - Configuration

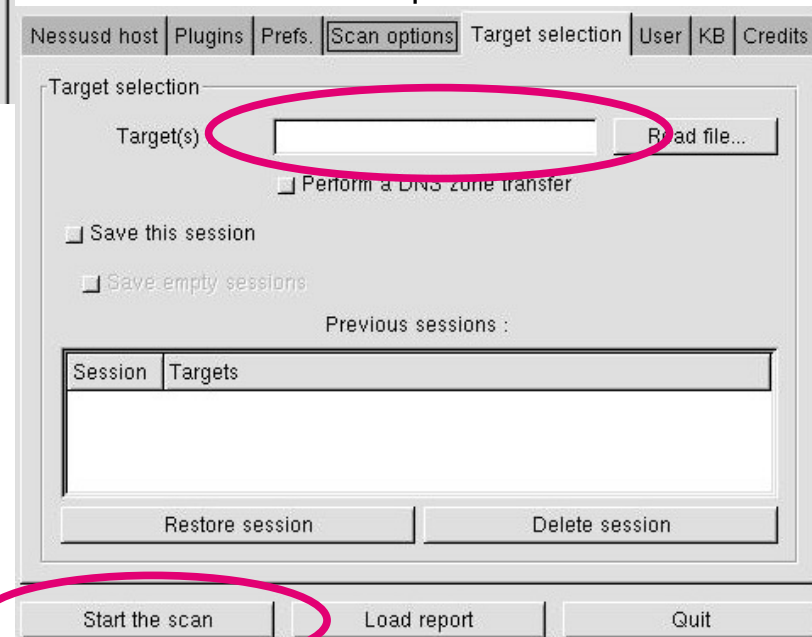


“Optimize the test”

- Avoids all apparently inapplicable tests
- May result in false negatives
- Speeds up tests

“Target(s)”

- Hostnames
- IP addresses
- Subnets $x.x.x.x/y$
- Comma-separated list.



Scanning Hosts with Nessus – Typical results



Synopsis: Old OpenSSH

Description: You are running a version of OpenSSH which is **older than 3.1**. Versions prior than 3.1 are vulnerable to an off by one error that allows local users to **gain root access**, and it may be possible for remote users to similarly compromise the daemon for remote access. In addition, a vulnerable SSH client may be compromised by connecting to a **malicious SSH daemon** that exploits this vulnerability in the client code, thus compromising the client system.

Solution: Upgrade to OpenSSH 3.1 or apply the patch for prior versions.

Nessus might be right because:

- Nessus often relies on the version strings
- E.g., Debian backports patches to old versions and leaves version unchanged
- Check, whether latest patch is installed

Scanning Hosts with Nessus – Typical results



Synopsis: Debugging functions are enabled on the remote web server

Description: The remote webserver supports the **TRACE** and/or **TRACK** methods. **TRACE** and **TRACK** are HTTP methods which are used to **debug** web server connections. In addition, it has been shown that servers supporting the **TRACE** method are subject to **cross-site scripting** attacks, dubbed XST for "Cross-Site Tracing", when used in conjunction with various weaknesses in browsers. An attacker may use this flaw to trick your legitimate web users to give him their credentials.

Solution: Disable these methods.

Nessus is absolutely right, this should be disabled!

Scanning Hosts with Nessus – Typical results

Synopsis: Zone Transfer



Description: The remote name server allows DNS **zone transfers** to be performed. A zone transfer will allow the remote attacker to instantly populate a list of potential targets. In addition, companies often use a naming convention which can give hints as to a servers primary.

As such, this information is of great use to an attacker who may use it to gain information about the topology of your network and spot new targets.

Solution: Restrict DNS zone transfers to only the servers that absolutely need it.

Nessus is right, but:

- Check, whether zone transfer reveals valuable information.
- For internal networks, this might not be the biggest problem.
- Do not excluded your secondary name server.

Scanning Hosts with Nessus – Typical results



Synopsis: MS-SQL Server

Description: Microsoft SQL server is running on this port. You should never let any unauthorized users establish connections to this service.

Solution: Block this port from outside

Nessus is right, but maybe it is necessary? If so, check passwords!

Plugin output :The following credentials were discovered for the remote SQL Server:
Account 'sa' has password 'password'

Remember the last message? Absolutely deadly... 

Scanning Hosts with nikto



- Nikto is a tool for **web scanner**, originally written by Rain Forest Puppy
- Find default web files
- Examine web server
- CGI security
- Can evade Intrusion detection systems
- Not a silent tool, may crash the server
- Command line tool

Scanning Hosts with nikto - HTTPS



```
#> perl nikto.pl -h XX.XX.XX.XX -p 443 -ssl
-----
- Nikto 2.02/2.03      -      cirt.net
+ Target IP:          XX.XX.XX.XX
+ Target Hostname:    host.name.test
+ Target Port:        80
-----
+ Server: Apache
- Allowed HTTP Methods: GET, HEAD, POST, OPTIONS      ok
- /robots.txt - contains 1 'disallow' entry which should be manually
viewed. (GET)                                          ok
+ GET /photo/ : My Photo Gallery pre 3.6 contains multiple
vulnerabilities including .. traversal, unspecified vulnerabilities,
and remote management interface access.              check!
+ 2967 items checked: 3 item(s) reported on remote host
```

Scanning Hosts with nikto - HTTP



```
#> perl nikto.pl -h XX.XX.XX.XX
+ HTTP method ('Allow' Header): 'TRACE' is typically only used
for debugging and should be disabled. This message does not
mean it is vulnerable to XST.
+ Apache/1.3.12 appears to be outdated (current is at least
Apache/2.2.6). Apache 1.3.39 and 2.0.61 are also current.
+ GET /cfappman/index.cfm : susceptible to ODBC/pipe-style
exploit; see RFP9901
+ GET /demo/ : This may be interesting...
+ GET /bc4j.html : Default Oracle page, may allow limited
administration.
+ GET /demo/.../XMLQuery.jsp.txt : Default Oracle code found.
...And so on...
+ 2964 items checked: 30 item(s) found on remote host
```

▪ Why offer this host to the penetration tester?

Additional Information

- <http://www.cryptoweb.de/>
 - Penetration tests explained for beginners – based on this talk
- <http://www.forinsect.de/>
 - Excellent overview on books, links and tools
- <http://sectools.org/>
 - Description of a huge number of tools. Good starting point, but a little bit outdated.
- <http://www.sans.org/top20/>
 - SANS Top-20 2007 Security Risks
- <http://www.owasp.org/>
 - WebScarab Project, security testing on web applications
 - OWASP Testing Guide, security testing procedures and checklists
 - OWASP CAL9000 Project, a JavaScript based web application security testing suite

Take-home message

Take-home message

- Simple penetration tests are easy, everybody can do this!
- While testing, ask yourself two questions:
 - Do I know what this feature is?
 - Do I need this feature?
- If in doubt, wait for the external penetration tester

Thank you for your attention!