

NETWORK SECURITY PRACTICES – ATTACK AND DEFENSE

Reconnaissance – Vulnerability Scanning

Reconnaissance

- Systematic and methodical understanding of a system's security posture
 - Domain names, IP addresses, routers, servers,...
- Network Scanning
- **Vulnerability Scanning**
- LAN Reconnaissance
- Wireless Reconnaissance
- Custom Packet Generation

Vulnerability Scanning

- Look for known vulnerabilities in known products
- An *intrusive* test tries to exercise the vulnerability, which can crash or alter the remote target.
- A *non-intrusive* test tries not to cause any harm to the target. (by checking versions / options)
- * Pros and Cons between the two?
- * (intrusive) vulnerability scanning ≠ penetration test
- * Good idea to use vulnerability scanning to test IDS ?



Nessus

- The best known tool in vulnerability scanning (<http://www.nessus.org>)
- Local Vulnerabilities
 - Require login (SSH/SMB) to local machines
 - Check for security vulnerabilities, file permissions, configuration files
- Network Scan
 - Intrusive / Non-intrusive
- Client-Server architecture
 - Can control the scan engine (server) remotely
 - Scan engine can inspect multiple machines on the network

Nessus / Scan Policy

Nessus - Windows Internet Explorer

https://localhost:8834/ Certificate Error Live Search

File Edit View Favorites Tools Help

Nessus

am is Help About

Policies Reports Scans Policies Users

+ Add Policy

General

Credentials

Plugins

Preferences

Basic

Name test1

Visibility Private

Description

Scan

Save Knowledge Base ☐

Safe Checks ☒

Silent Dependencies ☒

Log Scan Details to Server ☐

Stop Host Scan on Disconnect ☐

Avoid Sequential Scans ☐

Consider Unscanned Ports as Closed ☐

Designate Hosts by their DNS Name ☐

Network Congestion

Reduce Parallel Connections on Congestion ☐

Use Kernel Congestion Detection (Linux Only) ☐

Port Scanners

TCP Scan ☒ UDP Scan ☐ SYN Scan ☐

SNMP Scan ☒ Netstat SSH Scan ☒ Netstat WMI Scan ☒

Ping Host ☒

Port Scan Options

Port Scan Range default

Performance

Max Checks Per Host 5

Max Hosts Per Scan 80

Network Receive Timeout (seconds) 5

Max Simultaneous TCP Sessions Per Host unlimited

Max Simultaneous TCP Sessions Per Scan unlimited

Cancel Next

Done Local intranet 100%

Nessus / Plugins

The screenshot shows the Nessus web interface with the 'Edit Policy' page selected. The left sidebar contains navigation links: General, Credentials, **Plugins**, and Preferences. The main content area is titled 'Edit Policy' and includes a filter section with a 'Name' dropdown and a search input. Below the filter, there are two columns: 'Families' and 'Plugins'. The 'Families' column lists various security check categories, with 'SMTP problems' selected. The 'Plugins' column lists specific vulnerability checks, including 'Ability Mail Server < 2.61 Multiple Remote DoS', 'ASN.1 Multiple Integer Overflows (SMTP check)', 'BaSoMail SMTP Multiple Command Remote Overflow DoS', 'BusinessMail Multiple SMTP Command Remote Buffer Overflow', 'Canon ImageRUNNER SMTP Arbitrary Content Printing', 'Citadel SMTP makeuserkey Function RCPT TO Command Remote Overflow', 'ClamAV clamav-milter black-hole-mode Sendmail Recipient File Overflow', 'CMail MAIL FROM Command Remote Overflow', and 'CommuniGate Pro LISTS Module Malformed Multipart Message'. Below these columns, a 'Plugin Description' section provides details about the selected plugin, including a description of the vulnerability and a 'Solution' section. At the bottom, there are statistics for 'Enabled Families' (43) and 'Enabled Plugins' (34086), along with buttons for 'Enable All', 'Disable All', 'Cancel', and 'Submit'.

Nessus am is | Help | About | Log out

Policies Reports Scans Policies Users

Edit Policy

Filter Name Show Only Enabled Plugins ☐ **Reset Filter**

Families

- Mandriva Local Security Checks
- Misc.
- Netware
- Peer-To-Peer File Sharing
- Port scanners
- RPC
- Red Hat Local Security Checks
- SCADA
- SMTP problems**

Plugins

- 28289 Ability Mail Server < 2.61 Multiple Remote DoS
- 12065 ASN.1 Multiple Integer Overflows (SMTP check)
- 11674 BaSoMail SMTP Multiple Command Remote Overflow DoS
- 19365 BusinessMail Multiple SMTP Command Remote Buffer Overflow
- 14819 Canon ImageRUNNER SMTP Arbitrary Content Printing
- 30123 Citadel SMTP makeuserkey Function RCPT TO Command Remote Overflow
- 29830 ClamAV clamav-milter black-hole-mode Sendmail Recipient File Overflow
- 10047 CMail MAIL FROM Command Remote Overflow
- 17985 CommuniGate Pro LISTS Module Malformed Multipart Message

Plugin Description

overflow vulnerabilities. These issues could lead to a heap buffer overflow. A remote attacker could exploit these issues to execute arbitrary code.

This particular check sent a malformed SMTP authorization packet and determined that the remote host is not patched.

Solution

Enabled Families: 43 Enabled Plugins: 34086

Enable All **Disable All**

Cancel **Submit**

Nessus / Plugins

Nessus amis | Help | About | Log out

Policies Reports Scans Policies Users

[Edit Policy](#)

Families

- Mandriva Local Security Checks
- Misc.
- Netware
- Peer-To-Peer File Sharing
- Port scanners
- RPC
- Red Hat Local Security Checks
- SCADA
- SMTP problems

Plugins

- 11022 eDonkey Detection
- 42833 eMule IRC Module / Web Server DecodeBase16 Function Remote
- 11473 eMule Malformed Data Handling Remote DoS
- 11844 FastTrack (FT) Crafted Packet Handling Remote Overflow
- 35468 GigaTribe Detection
- 10408 Gnapster Absolute Path Name Request Arbitrary File Access
- 11716 Gnutella Root Directory Misconfiguration
- 10946 Gnutella Servent Detection
- 29729 iMesh P2P Client Detection

Plugin Description

Description
According to its version, the eMule Web Server listening on this port contains a buffer overflow vulnerability in the 'DecodeBase16' function due to a lack of length checks on its inputs. An anonymous remote attacker may be able to leverage this issue to execute arbitrary code on the affected host.

Solution

Enabled Families: 43 Enabled Plugins: 34086

Enable All Disable All

Cancel Submit

Nessus / Add Scan

Nessus

Home | Reports | Scans | Policies | Users

+ Add Scan

Name: scan1

Policy: test1

Scan Targets: 192.168.0.103

Targets File: Browse...

Cancel Launch Scan

Nessus / Credentials

The screenshot shows the Nessus web interface. At the top, the 'Policies' tab is selected in the main navigation bar. On the left sidebar, the 'Credentials' section is highlighted. The main content area is titled 'Edit Policy' and shows the configuration for 'Windows credentials'. The 'Credential Type' is set to 'Windows credentials'. The form includes fields for 'SMB account' (containing 'H'), 'SMB password' (masked with asterisks), 'SMB domain (optional)', and 'SMB password type' (set to 'Password'). Below these are three sets of 'Additional SMB' fields for account, password, and domain, each with a corresponding input field. At the bottom right, there are 'Cancel' and 'Submit' buttons.

Nessus

amls | Help | About | Log out

Policies Reports Scans Policies Users

Edit Policy

Credential Type Windows credentials

SMB account : H

SMB password : *****

SMB domain (optional) :

SMB password type : Password

Additional SMB account (1) :

Additional SMB password (1) :

Additional SMB domain (optional) (1) :

Additional SMB account (2) :

Additional SMB password (2) :

Additional SMB domain (optional) (2) :

Additional SMB account (3) :

Additional SMB password (3) :

Cancel Submit

Nessus / Scan summary

The screenshot displays the Nessus web interface. At the top, the 'Reports' tab is selected in the navigation bar. On the left, the 'Report Info' sidebar shows details for 'scan1': Name: scan1, Last Update: Feb 27, 2010 10:44, and Status: Completed. Below this are buttons for 'Download Report', 'Show Filters', and 'Reset Filters', followed by an 'Active Filters' section. The main content area shows a table for 'scan1' with 1 result. The table has columns: Host, Total, High, Medium, Low, and Open Port. The first row shows Host '192.168.0.103' with a Total of 159 (highlighted by a callout box), 85 High vulnerabilities, 20 Medium vulnerabilities, 44 Low vulnerabilities, and 10 Open Ports.

Host	Total	High	Medium	Low	Open Port
192.168.0.103	159	85	20	44	10

Nessus / Scan Summary (no local vulnerability check)

The screenshot shows the Nessus web interface. The top navigation bar includes the Nessus logo and links for 'amls', 'Help', 'About', and 'Log out'. Below this is a secondary navigation bar with 'Reports', 'Scans', 'Policies', and 'Users'. The 'Reports' section is active, displaying a sidebar on the left with 'Report Info' (Name: scan2 no local vulnerabil..., Last Update: Feb 27, 2010 10:57, Status: Completed), 'Download Report', 'Show Filters', 'Reset Filters', and 'Active Filters'. The main content area shows a table for the scan 'scan2 no local vulnerabilities' with 1 result. The table has columns for Host, Total, High, Medium, Low, and Open Port. The first row shows Host 192.168.0.103 with a Total of 58, 14 High vulnerabilities, 4 Medium, 30 Low, and 10 Open Ports. A callout box highlights the 'Total' value of 58.

Host	Total	High	Medium	Low	Open Port
192.168.0.103	58	14	4	30	10

Nessus / Detailed scan result

MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (unauthenticated check)

Synopsis:

Arbitrary code can be executed on the remote host due to a flaw in the 'Server' service.

Description:

The remote host is vulnerable to a buffer overrun in the 'Server' service that may allow an attacker to execute arbitrary code on the remote host with the 'System' privileges.

Risk factor:

Critical

CVSS Base Score:10.0

CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Solution:

Microsoft has released a set of patches for Windows 2000, XP, 2003, Vista and 2008 :
<http://www.microsoft.com/technet/security/bulletin/ms08-067.msp>

Plugin ID:

34477

CVE:

CVE-2008-4250

BID:

31874

Other references:

OSVDB:49243

National Vulnerability Database

- <http://nvd.nist.gov/>

Sponsored by
DHS National Cyber Security Division/US-CERT

NIST
National Institute of
Standards and Technology

National Vulnerability Database

automating vulnerability management, security measurement, and compliance checking

Vulnerabilities	Checklists	Product Dictionary	Impact Metrics	Data Feeds	Statistics
-----------------	------------	--------------------	----------------	------------	------------

Home	SCAP	SCAP Validated Tools	SCAP Events	About	Contact	Vendor Comments
------	------	----------------------	-------------	-------	---------	-----------------

Mission and Overview

NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA).

National Vulnerability Database Version 2.2

NVD is the U.S. government repository of standards based vulnerability management data represented using the [Security Content Automation Protocol \(SCAP\)](#). This data enables automation of vulnerability management, security measurement, and compliance. NVD includes databases of security checklists, security related software flaws, misconfigurations, product names, and impact metrics.

Federal Desktop Core Configuration settings (FDCC)

NVD contains content (and pointers to tools) for performing configuration checking of systems implementing the [FDCC](#) using the Security Content Automation Protocol ([SCAP](#)). [FDCC Checklists](#) are available here (to be used with SCAP FDCC capable tools). [SCAP FDCC Capable Tools](#) are available here.

Resource Status

NVD contains:

- 40837 [CVE Vulnerabilities](#)
- 131 [Checklists](#)
- 191 [US-CERT Alerts](#)
- 2371 [US-CERT Vuln Notes](#)
- 2517 [OVAL Queries](#)

Last updated: 02/26/10
CVE Publication rate:
 11 vulnerabilities / day

Email List

NVD provides four mailing lists to the

NVD Primary Resources

- [Vulnerability Search Engine](#) (CVE software flaws and CCE misconfigurations)
- [National Checklist Program](#) (automatable security configuration guidance in XCCDF and OVAL)
- [SCAP](#) (program and protocol that NVD supports)
- [SCAP Compatible Tools](#)
- [SCAP Data Feeds](#) (CVE, CCE, CPE, CVSS, XCCDF, OVAL)
- [Product Dictionary](#) (CPE)
- [Impact Metrics](#) (CVSS)
- [Common Weakness Enumeration](#) (CWE)

NVD: Security Configuration Checklist

Home SCAP SCAP Validated Tools SCAP Events About Contact Vendor Comments

National Checklist Program Repository

The National Checklist Program (NCP), defined by the [NIST SP 800-70 Rev. 1](#), is the U.S. government repository of publicly available security checklists (or benchmarks) that provide detailed low level guidance on setting the security configuration of operating systems and applications. NCP is migrating its repository of checklists to conform to the Security Content Automation Protocol (SCAP). SCAP enables standards based security tools to automatically perform configuration checking using NCP checklists. For more information relating to the NCP please visit the [information page](#) or the [glossary of terms](#).



Search for Checklist using the fields below. The keyword search will search across the name, and summary.

Tier: Any.....

Target Product: Any.....

Product Category: Any.....

Authority: Any.....

Keyword:

Checklist Results

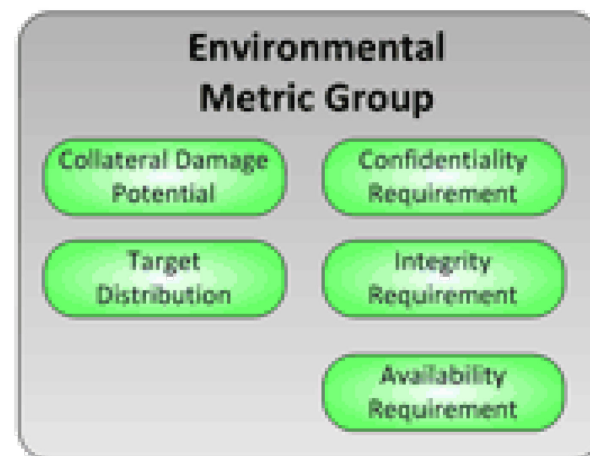
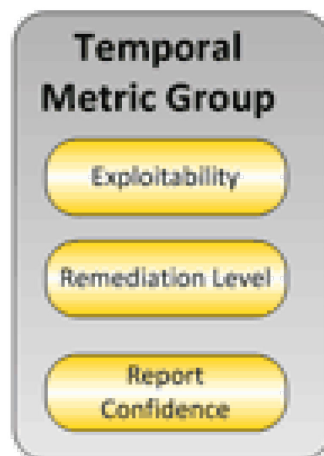
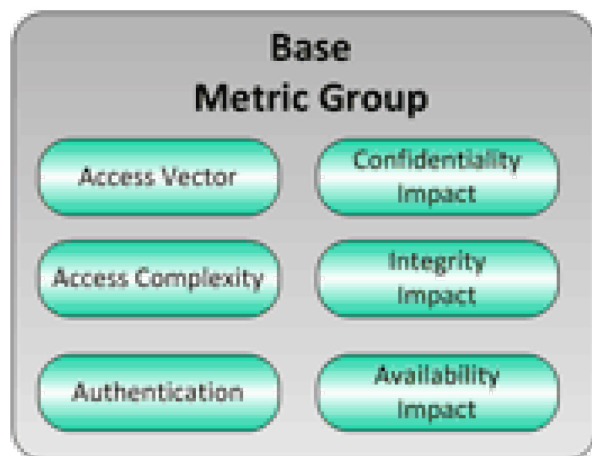
<u>Tier</u>	<u>Target Product</u>	<u>Product Category</u>	<u>Authority</u>	<u>Publication Date</u>	<u>Checklist Name (Version)</u>	<u>Resources</u>
IV	• Microsoft Internet Explorer 7	• Web Browser	• OMB	06/19/2008	FDCC IE7 (1.2)	<ul style="list-style-type: none"> • SCAP Content - OVAL 5.3 • SCAP Content - OVAL 5.4 • GPOs • Prose
IV	• Microsoft Windows Vista	• Operating System	• OMB	06/19/2008	FDCC Windows Vista (1.2)	<ul style="list-style-type: none"> • SCAP Content - OVAL 5.3 • SCAP Content - OVAL 5.4 • GPOs • Prose
IV	• Microsoft Windows Vista	• Operating System	• OMB	06/19/2008	FDCC Windows Vista Firewall (1.2)	<ul style="list-style-type: none"> • SCAP Content - OVAL 5.3 • SCAP Content - OVAL 5.4

NVD: Security Configuration Checklist

```
<definition id="oval:gov.nist.fdcc.ie7:def:1198" version="1" class="compliance">
  <metadata>
    <title>Disable Automatic Install of Internet Explorer Components</title>
    <affected family="windows">
      <platform>Microsoft Windows XP</platform>
      <platform>Microsoft Windows Server 2003</platform>
      <platform>Microsoft Windows Vista</platform>
      <product>Microsoft Internet Explorer 7</product>
    </affected>
    <reference source="http://cve.mitre.org" ref_id="CVE-2006-3956"/>
    <reference source="cve.mitre.org/version/4" ref_id="CVE-2006-3956"/>
    <description>This Disable Automatic Install of Internet Explorer components setting prevents
      Internet Explorer from automatically installing components.</description>
  </metadata>
  <criteria>
    <extend_definition comment="Microsoft Internet Explorer 7 is installed"
      definition_ref="oval:gov.nist.fdcc.ie7:def:627"/>
    <criteria comment="Computer Configuration\Network\Internet Explorer\Disable Automatic Install of
      Internet Explorer Components" test_ref="oval:gov.nist.fdcc.ie7:tst:3956"/>
    <!--
      <criteria comment="Computer Configuration\Network\Internet
        Explorer\Disable Automatic Install of Internet Explorer Components"
        test_ref="oval:gov.nist.fdcc.ie7:tst:3957"/>-->
  </criteria>
</definition>
```

CVSS (Common Vulnerability Scoring System)

- <http://www.first.org/cvss/cvss-guide.html>
- Too many vulnerabilities to deal with
 - Prioritize the vulnerabilities and remediate the most risky ones first
- Three metric groups



CVSS / Metric Groups

- **Base**: represents the intrinsic and fundamental characteristics of a vulnerability that are constant over time and user environments.
- **Temporal**: represents the characteristics of a vulnerability that change over time but not among user environments.
- **Environmental**: represents the characteristics of a vulnerability that are relevant and unique to a particular user's environment.

CVSS Score and Vector

MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (unauthenticated check)

Synopsis:

Arbitrary code can be executed on the remote

Description:

The remote host is vulnerable to a buffer over
execute arbitrary code on the remote host w

Risk factor:

Critical

CVSS Base Score:10.0

CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Solution:

Microsoft has released a set of patches for Wi
<http://www.microsoft.com/technet/security/b>

Plugin ID:

34477

CVE:

CVE-2008-4250

BID:

31874

Other references:

OSVDB:49243

AV:**N** exploitable via *network access*

AC:**L** (low complexity) specialized
access conditions or extenuating
circumstances do not exist

Au:**N** no authentication required to
exploit

C:**C** Total (complete) information
disclosure

I:**C** Total (complete) compromise of
system integrity

A:**C** Total (complete) shutdown of the
affected resource

CVSS Score and Vector

```
BaseScore = round_to_1_decimal(((0.6*Impact)+(0.4*Exploitability)-1.5)*f(Impact))
```

$$\text{Impact} = 10.41 * (1 - (1 - \text{ConfImpact}) * (1 - \text{IntegImpact}) * (1 - \text{AvailImpact}))$$
$$\text{Exploitability} = 20 * \text{AccessVector} * \text{AccessComplexity} * \text{Authentication}$$
$$f(\text{impact}) = 0 \text{ if Impact} = 0, 1.176 \text{ otherwise}$$

```
AccessVector      = case AccessVector of
    requires local access: 0.395
    adjacent network accessible: 0.646
    network accessible: 1.0
```

```
AccessComplexity = case AccessComplexity of
  high: 0.35
  medium: 0.61
  low: 0.71
```

```
Authentication    = case Authentication of
                    requires multiple instances of authentication: 0.45
                    requires single instance of authentication: 0.56
                    requires no authentication: 0.704
```

Nessus Plug-in Code Example

- C:\Program Files\Tenable\Nessus\nessus\plugins\zope.nasl

```

if(description)
{
  script_id(10447); script_version ("$Revision: 1.21 $"); script_cve_id("CVE-2000-0483");
  script_bugtraq_id(1354);
  script_xref(name:"OSVDB", value:"347");
  script_name(english:"Zope < 2.1.7 DocumentTemplate Unauthorized DTML Entity
Modification");
  [.....]
  script_category(ACT_GATHER_INFO);
  exit(0);
}

# The script code starts here
[.....]

port = get_http_port(default:80);
banner = get_http_banner(port:port);

if(banner)
{
  if(egrep(pattern:"^Server: .*Zope 2\\.((0\\.\\.*)|(1\\. [0-6]))", string:banner))
    security_hole(port);
}

```

ACT_GATHER_INFO : the script will be launched among the first. You know it will not harm the remote computer.

ACT_ATTACK : the script will attempt to gain some privileges on the remote host. It may harm the remote system (if it tests a buffer overflow for instance)

ACT_DENIAL : the script will attempt to crash the remote host

ACT_SCANNER : the script is a port scanner

Nessus Plug-in Code Example SMTP OPEN Relay

```
[.....]
send(socket: soc, data: strcat('HELO ', src_name, '\r\n'));
smtp_rcv_line(socket: soc);
for (i = 0; soc && (from_l[i] || to_l[i]); i++)
{
    mf = strcat('MAIL FROM: <', from_l[i], '>\r\n');
    send(socket: soc, data: mf);
    l = smtp_rcv_line(socket: soc);
    if (!l || l =~ '^5[0-9][0-9]')
    {
        smtp_close(socket: soc);
        soc = smtp_open(port: port, helo: domain);
    }
    else
    {
        rt = strcat('RCPT TO: <', to_l[i], '>\r\n');
        send(socket: soc, data: rt);
    }
}
[.....]
l = smtp_rcv_line(socket: soc);
if (l =~ '^2[0-9][0-9]')
{
    flag = 1;
}
[.....]
```

HELO localhost
 MAIL FROM: <nessus@localhost>
 RCPT TO: <nessus@domain.com>

Check for 200~299 response
 code (server agrees to deliver
 the email)

Smtp_relay2.nasl

Nessus Plug-in Code Example / Horde File Disclosure

```
script_category(ACT_ATTACK);

[.....]
# Try to exploit the issue to read a file.
#
# nb: Horde 3.x uses "/services"; Horde 2.x,
"/util".
foreach subdir (make_list("/services", "/util"))
{
  if ("util" >< subdir) file = "horde.php";
  else file = "conf.php";

  r = http_send_recv3(method:"GET",
    item:string(
      dir, subdir, "/go.php?",
      "url=../config/", file, "%00:/&",
      "untrusted=1"
    ),
    port:port
  );
}
[.....]
```

horde_url_file_disclosure.nasl

Actually exploit the vulnerability to see if *go.php* allows accessing arbitrary files (horde's config files)

Other Vulnerability Scanners

- Nikto
 - Dangerous files / CGIs, outdated versions of servers, misconfigurations in a web server
- HP WebInspect
 - Web Application Vulnerability Scanning
 - Cover Adobe Flash, JavaScript/AJAX, .Net, PHP, Cold Fusion,...

Summary

- The scanners covered thus far interact with the **interfaces** of a production system to detect vulnerabilities
 - Check for banners and versions
 - Look for files / settings that make system vulnerable
 - Exploit vulnerability and see if it works
- Deal with **known vulnerabilities**

Alternative Approaches for Vulnerability Scanning

- Static code analysis for vulnerabilities
 - http://en.wikipedia.org/wiki/List_of_tools_for_static_code_analysis
 - <http://www.armorize.com/>
- Software testing
 - Black-box / grey-box / white-box testing
 - http://en.wikipedia.org/wiki/Software_testing#Testing_methods
- Can identify “potential” vulnerabilities