DenyAll Detect

Technical documentation

07/27/2015

denyall

NEXT GENERATION APPLICATION SECURITY

Summary

1. About this document

1.1 Purpose

The DenyAll Detect solutions are shipped in 3 different form factors:

- the Enterprise Edition, a virtual machine automating IT security monitoring,
- the Cloud Edition, available on our website enables on-demand testing for an effective assessment of the organization's out-facing security,
- the Portable Edition, a bootable USB key, shipped with the whole environment required to perform your security testing without any installation.

The technical tests performed by our software are described below.

1.2 History

Version	Date	Author	Comments
V1.3	2015/07/27	V. Maury	

1.3 Context

The DenyAll Detect product line follows the VulnIT software, previously developed and maintained by VULNIT.

This VULNIT company has been acquired by DenyAll in July 2012. Therefore, all the documentation of the previous VulnIT solutions has been adapted to DenyAll's document templates.Detect 4.8 or above

2. Tests list

2.1 Network port scanning

The first acquisition step consists in detecting all the devices reachable in the audit scope provided (target acquisition) and detecting all the services provided by each target (service identification).

The TCP scanner used is nmap. It is a TCP SYN (half open) scanner.

The test depth selected is:

- fast (only the 100 most used ports will be tested),
- normal (the 1000 most used ports will be tested) or
- full (all 65535 ports will be tested).

A SNMP (UDP) scan is also performed using medusa, on a selection of a few common community strings. The SNMP service is the only UDP service scanned at the moment.

2.2 Domain discovery (specific to DenyAll VM Cloud Edition)

DenyAll Edge Tester intends to discover all the assets belonging to a (using DNS, Google, RIR and SPF).

Besides, DenyAll Edge Tester discovers the following vulnerabilities on the domain or the assets belonging to the domain without testing the assets themselves:

- List of all the vulnerable pages identified by Google and Bing,
- Black-listed domain, blocked by anti-spam software (DNS-based Block List),
- Websites containing malwares (Google safe-browsing),
- Documents containing meta-data (user name, etc).

2.3 Vulnerability assessment

The testing phase performs adequate vulnerability assessments, depending on the targets and services selected during the validation step (see the user guide above).

These tests concern the following criteria:

- Patch management,
- Development,
- Access control,
- Configuration,
- Encryption,

On a panel of technologies:

- Windows and Unix systems,
- Websites,
- Networks,
- Databases.

	Patch mgt	Development	Access control	Configuration	Encryption
Windows & Unix (OS and apps)	✓			✓	
Web apps	✓	✓	✓	✓	✓
Databases	✓		✓	✓	
Network	✓		✓	✓	✓

These tests are detailed hereunder.

2.4 Website testing

All websites (Internet, Intranet, Extranet) are first discovered. This crawling phase enumerates all the accessible web pages of the website, either they are naturally linked (HTML links, Javascript, Flash banners) or hidden (dictionary-based approach). Web services are also crawled.

Once these pages enumerated, DenyAll Detect automates the identification of the following development vulnerabilities:

- SQL injection (blind SQLi, supporting 4 technologies of underlying databases: Oracle, SQL Server, MySQL and PostgreSQL),
- Injection on web services,
- LDAP injection,
- Command/OS injection,
- XSS (Cross-site scripting),
- File inclusion, either local (LFI) or remote (RFI),
- CSRF (Cross-Site Request Forgery),
- Session management,
- Unvalidated redirect,
- Trivial authentication vulnerabilities (in web forms or http .htaccess security).

The OWASP classifies these vulnerabilities as the most critical and also the most frequent vulnerabilities on websites.

DenyAll Detect also detects misconfigurations which could lead to information leakage:

- Temporary files (development or backup files),
- FPD (Full Path Disclosure) indicating the web server architecture,
- The TRACE function activated on the web server,
- Detecting the web server version.

2.5 Patch management

Patch management is tested using OpenVAS, which runs a collection of plugins dedicated for each patch to check.

As of July 2015, around 38,000 plugins were included in our tests and cover the following flavors of operating systems:

- CentOS,
- Debian,
- Fedora,
- FreeBSD,
- Gentoo,
- HP-UX,
- MAC OS-X,
- Mandrake,
- RedHat,
- Solaris,
- Suse,
- Ubuntu,
- Windows (security bulletins and advisories)

And also databases and web servers.

In order to avoid affecting the target availability, we excluded ‘aggressive’ plugins (by default) on the following criteria: the plugin is explicitly described as aggressive, it attempts brute forcing, or it falls into one of the ‘aggressive’ categories (‘ACT_DENIAL’, ‘ACT_DESTRUCTIVE_ATTACK’, ‘ACT_FLOOD’, ‘ACT_KILL_HOST’ or ‘ACT_MIXED_ATTACK’, as described in NASL documentation).

These aggressive plugins can still be activated using a specific parameter in the software (in the scanning task definition).

By default, all vulnerabilities are displayed, but the user may choose to only focus on high-risk issues by setting the risk threshold in the configuration menu.

2.6 OS configuration checks

Windows configuration checks include:

- Authentication policy
- Presence of local administrator accounts
- Presence of local ‘guest’ account
- Antivirus installed and up to date (similar to the security center vision)
- Firewall activated (similar to the security center vision)

Performing these checks remotely requires:

- TCP ports 135 and 445 are open
- The ‘remote registry” service is started
- The account provided has access to the registry (with UAC deactivated)
- The firewall of the targeted device allows WMI (wmi-in)

Unix configuration checks support Linux, BSD, MacOS, Solaris, AIX, HP-UX, NeXT, Tru64 and UNICOS. They rely on the TIGER open source tool and mostly fit in the CIS benchmark guidelines.

More than 250 tests are integrated in Detect, including:

- User accounts and groups
- Rights on files and folders

- Exported PATH in Shell configuration files
- Remote commands (.rhosts …)
- root account configuration, root folder rights
- Alias
- Apache configuration
- Cron tasks
- File systems
- Inet services
- Classical intrusion trails
- Misc (abnormal files, umask, rootkits...)
- NFS, NIS+
- netrc files
- files signature checks

Unix whitebox tests also retrieve the list of accounts and password hashes and try a trivial check offline using “john the ripper”.

Note: most of these tests do not require a ‘root’ account, except of course for accessing the password (shadow) file to perform authentication checks on all accounts.

2.7 File shares

Dedicated tests are performed on file shares:

- Anonymous access on FTP servers,
- Windows folders shares (or samba shares on Unix) open to everyone.

2.8 Databases

Authentication tests (for trivial accounts) are performed on 5 technologies of database management systems:

- Microsoft SQL Server,
- Oracle,
- MySQL
- PostgreSQL,
- DB2 (Unix/Windows).

Moreover, configuration tests (security policies, etc) and password offline brute force testing (whitebox) are performed on:

- Microsoft SQL Server,
- Oracle,
- MySQL.

These whitebox checks require top role access to be performed, eg ‘sa’ for MSSQL, ‘SYS” for ORACLE and ‘root’ for MySQL.

2.9 WiFi console (specific to DenyAll VM Portable Edition)

A wifi console providing information on the access points accessible: SSID (name), power, channel, and security settings (open, WEP, WPA).

We do not offer the ability to crack a WEP password for instance.

The WiFi console is specific to the Auditor USB key.

2.10 Network security

A few common network security checks are performed:

- SSL encryption (null or weak ciphers allowed, SSLv2, renegociation, etc)
- SSH and Telnet authentication tests (using a dictionary of trivial accounts),
- Read/write SNMP access using common community strings,
- Open mail relay (attempting to send 10 unauthenticated emails),
- Microsoft RPC/SMB information leakage,
- DNS zone transfer,
- Unencrypted protocols (Telnet, Rexec/Rsh/Rlogin, FTP)

3. List of open-source tools used by DenyAll Detect

This chapter describes all the open source tools used by Detect in each phase:

- Network inventory:
  - nmap (port scanner),
  - medusa (SNMP),
  - dhcping (DHCP),
  - DB2Discover, MSSQLDiscover & OracleDiscover to discover databases.
- Web crawling:
  - whatweb to profile applications
- Network tests:
  - DBMS: db2_luw, medusa
  - FTP: medusa
  - RPC: rpcclient
  - SMB: smbclient, smbat
  - SNMP: medusa, net-snmp
  - SSH: openssh, medusa
  - SSL: openssl, sslscan
  - Telnet: medusa
  - OS configuration: jtr (john the ripper), tiger
- Web tests:
  - File inclusion: fimap
  - SQL injection in HTTP: sqlmap
  - SQL injections in web services: sqlmap

denyall

NEXT GENERATION APPLICATION SECURITY

Headquarter

6 avenue de la Cristallerie
92310 Sèvres - FRANCE

Tel : +33 (0)1 46 20 96 00
Fax : +33 (0)1 46 20 96 02

Email : info@denyall.com

www.denyall.com