Entwicklung von Schwachstellen-Tests für OpenVAS

Workshop-Intro @ UnFUCK 2016

Christian Fischer

07.05.2016

Inhalt

- Bis 2005: Nessus
- Fork als GNessUs
- 2007: Open Vulnerability Assessment System 1.0 (`http://www.openvas.org`)
- Haupt-Entwicklung durch Greenbone Networks GmbH (`http://www.greenbone.net`)
- Großteil der Komponenten unter der GPL veröffentlicht
- Aktuell: OpenVAS 8, OpenVAS 9 in der Beta-Phase

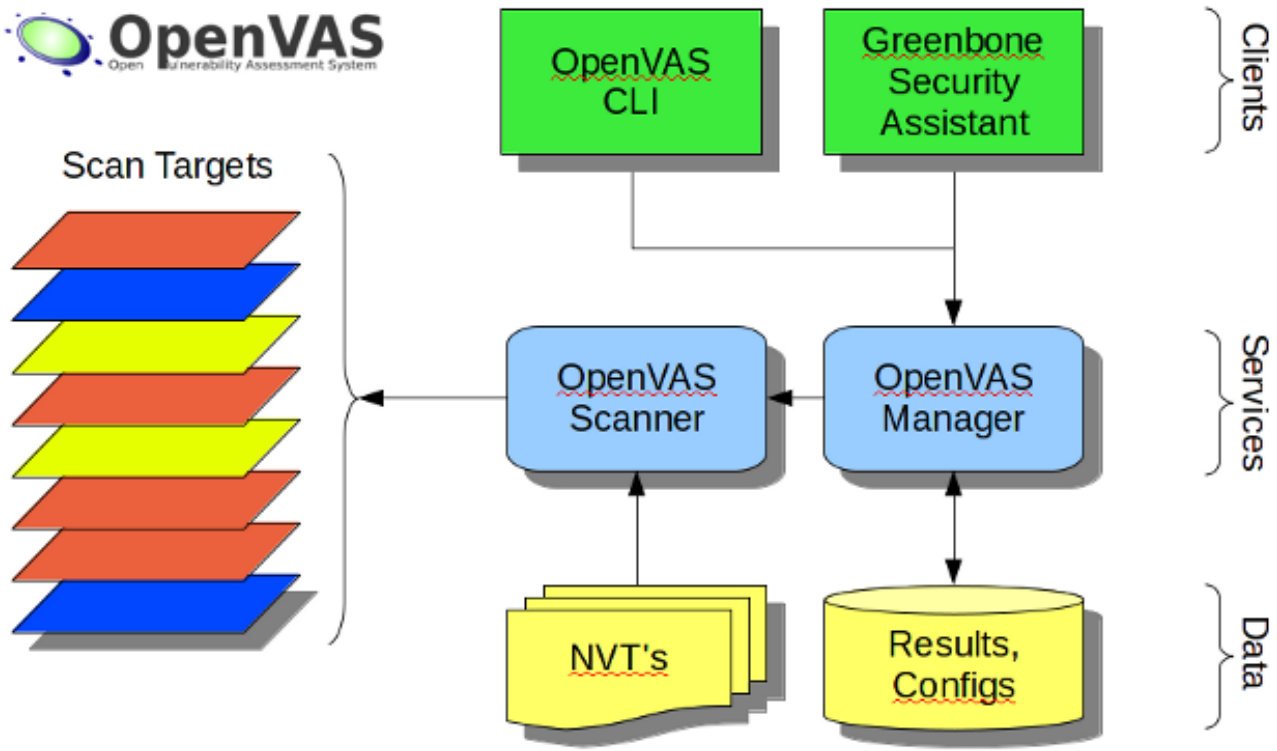

Abbildung: OpenVAS Architektur

Quelle: `http://www.openvas.org/about.html`

- NASL = Nessus Attack Scripting Language
- NVT = Network Vulnerability Test
- LSC = Local Security Check

- https://www.exploit-db.com/
- http://www.securityfocus.com/
- uvm.

- https://www.shodan.io/
- https://censys.io/
- Google Dorks (z.B. https://www.exploit-db.com/google-hacking-database/)

```
if(description) {

  ...metadaten...

  exit(0);
}

# Code
```

- Aktuelles Template immer unter `https://svn.wald.intevation.org/svn/openvas-nvts/template.nasl` zu finden.

- NVTs lesen / schreiben in Knowledgebase

```
set_kb_item( name:"/foo/bar", value:123 );

get_kb_item( "/foo/bar" ); # kann forken

get_kb_list( "/foo/bar" ); # gibt Liste zurück
```

```
set_kb_item( name:"/hello/world",
             value:"Hello World!!!!" );

item = get_kb_item( "/hello/world" );
if( "Hello World" >< item ) {
  log_message( data:item );
}
```

```
openvas-nasl -X -i $includedir helloworld.nasl

$includedir = /var/lib/openvas/plugins
$includedir = /usr/local/var/lib/openvas/plugins
$includedir = /path/to/svn
```

- OpenVAS Kompakt (`http://www.brain-media.de/freebooks/OpenVAS.pdf`)
- The NASL2 reference manual (`http://michel.arboi.free.fr/nasl2ref/nasl2_reference.pdf`)
- `http://openvas.org/nvt-dev.html`
- Vorhandene NVTs

Let’s go to work...