Vulnerability Assessment Report: sacnme.nmap.org

1. Network Scan Results (Nmap)

Port	Service	Version	State
22	ssh	7.4	open
70	gopher		closed
80	http	2.4.6	open
113	ident		closed
443	http	2.4.6	open
31337	Elite		closed

2. Web Vulnerability Results (Nikto)

```
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP: 50.116.1.184
+ Target Hostname: sacnme.nmap.org
+ Target Port: 80
+ Start Time: 2026-01-29 11:37:31 (GMT0)
---------------------------------------------------------------------------
+ Server: Apache/2.4.6 (CentOS)
+ The anti-clickjacking X-Frame-Options header is not present.
+ Root page / redirects to: https://nmap.org/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ /cfappman/index.cfm - Redirects (301) to https://nmap.org/cfappman/index.cfm ,
susceptible to ODBC/pipe-style exploit; see RFP9901
http://www.wiretrip.net/rfp/p/doc.asp/i2/d3.htm
+ /cfdocs/examples/cvbeans/beaninfo.cfm - Redirects (301) to
https://nmap.org/cfdocs/examples/cvbeans/beaninfo.cfm , susceptible to our ODBC
exploit; see RFP9901 http://www.wiretrip.net/rfp/p/doc.asp/i2/d3.htm
+ /cfdocs/examples/parks/detail.cfm - Redirects (301) to
https://nmap.org/cfdocs/examples/parks/detail.cfm , susceptible to our ODBC exploit;
see RFP9901 http://www.wiretrip.net/rfp/p/doc.asp/i2/d3.htm
+ /kboard/ - Redirects (301) to https://nmap.org/kboard/ , KBoard Forum 0.3.0 and prior
have a security problem in forum_edit_post.php, forum_post.php and forum_reply.php
+ /lists/admin/ - Redirects (301) to https://nmap.org/lists/admin/ , PHPList pre 2.6.4
contains a number of vulnerabilities including remote administrative access, harvesting
user info and more. Default login to admin interface is admin/phplist
+ /splashAdmin.php - Redirects (301) to https://nmap.org/splashAdmin.php , Cobalt Qube
3 admin is running. This may have multiple security problems as described by
www.scan-associates.net. These could not be tested remotely.
+ /ssdefs/ - Redirects (301) to https://nmap.org/ssdefs/ , Siteseed pre 1.4.2 has
'major' security problems.
+ /sshome/ - Redirects (301) to https://nmap.org/sshome/ , Siteseed pre 1.4.2 has
'major' security problems.
+ /tiki/ - Redirects (301) to https://nmap.org/tiki/ , Tiki 1.7.2 and previous allowed
restricted Wiki pages to be viewed via a 'URL trick'. Default login/pass could be
admin/admin
+ /tiki/tiki-install.php - Redirects (301) to https://nmap.org/tiki/tiki-install.php ,
Tiki 1.7.2 and previous allowed restricted Wiki pages to be viewed via a 'URL trick'.
Default login/pass could be admin/admin
+ /scripts/samples/details.idc - Redirects (301) to
https://nmap.org/scripts/samples/details.idc , See RFP 9901; www.wiretrip.net
```

```
+ /includes/conexion.inc - Redirects (301) to https://nmap.org/includes/conexion.inc ,
Database connection file found.
+ /.svn/entries - Redirects (301) to https://nmap.org/.svn/entries , Subversion Entries
file may contain directory listing information.
+ /.svn/wc.db - Redirects (301) to https://nmap.org/.svn/wc.db , Subversion SQLite DB
file may contain directory listing information.
+ /.git/index - Redirects (301) to https://nmap.org/.git/index , Git Index file may
contain directory listing information.
+ /.hg/dirstate - Redirects (301) to https://nmap.org/.hg/dirstate , Mercurial DirState
file may contain directory listing information.
+ 26 items checked: 0 error(s) and 2 item(s) reported on remote host
+ End Time: 2026-01-29 11:38:07 (GMT0) (36 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```