

NCSA custom Lynis Security Audit Tool

<https://git.ncsa.illinois.edu/irst/lynis-ncsa-plugins>

Usage:

Method 1:

1. Download the Lynis package from <https://cisofy.com/downloads/lynis/> and extract the tarball with `tar -xf lynis*.tar.gz`
2. Clone the above repository and copy the `plugin_ncsa_phase2` file into the `lynis/plugins` folder.
3. Modify the Lynis profile `lynis/default.prf` to add `plugin=ncsa` under other plugins.
4. Go into the lynis directory and run `./lynis audit system`

Method 2:

1. Install the lynis-ncsa RedHat package.
2. Run lynis audit system

Running Lynis NCSA plugin while skipping Lynis built-in checks:

```
cd /opt/lynis
sudo ./lynis audit system --profile nodefault.prf
```

Running Lynis NCSA version with Lynis built-in checks:

```
sudo lynis audit system
```

Checks inside the plugin:

Each of these checks can be skipped by adding `skip-test=TEST-NAME` to the `default.prf` file.

NCSA-IPTABLES

Checks if the default INPUT chain policy is DROP or REJECT, default policy meaning -A rules without any IP, port, or protocol exceptions. If the iptables is flushed, then check the default -P INPUT policy.

(Legacy) Checks if the policy for ICMP packets is ACCEPT.

Checks if the policy for ICMP type 3, 8, and 11 in IPv4, type 2 and 3 in IPv6 is ACCEPT.

NCSA-QUALYS

Checks if the qualys user exists and has a proper shell as defined in `QUALYS_ALLOWED_SHELLS` on top.

Checks the SSHD config specific to qualys user is compliant with setup specified in [Qualys Authenticated Scanning Host setup](#)

If `pam_access` is enabled in SSHD, checks that qualys from the IP specified by `QUALYS_IP` has access.

Checks iptables INPUT rule for the IP specified by `QUALYS_IP` is ACCEPT.

Checks if qualys owns its home directory.

Checks if qualys has an `authorized_keys` file in its `.ssh` directory and owns that key.

Checks if qualys user has ever logged in.

NCSA-RSYSLOG

Checks if rsyslog remote destination is set per [Syslog Remote Logging Best Practices](#) suggests.

NCSA-NTP

(Lazy version) Checks all the NTP sources from either `chrony` or `ntpd` (whichever is installed) ends in `.illinois.edu`. Since IP can change and might even upgrade to IPv6 one day.

NCSA-DNS

Checks if a local resolver is listening on local port 53, if there is, display the name of the program.

If the local resolver is unbound per [Local Caching Resolver](#) suggests, checks that unbound has the two NCSA DNS servers (141.142.2.2 and 141.142.230.144) set as its upstream DNS resolver.

If there is no local DNS resolver, checks if `/etc/resolv.conf` has the two NCSA DNS resolvers set as nameserver.

NCSA-TLS

Checks if nginx and apache2 TLS settings are set per [Recommended TLS settings](#) recommendations.

Note that future checks can be added or modified to check for any nginx or apache2 setting in the format of `check_webserver_config "${TEST_NO}" (/etc /apache2 or /etc/nginx) 'setting_name' 'expected_value'`

NCSA-SSSD

Checks that some universal LDAP/SSSD settings are set per [SSSD Kerberos and LDAP](#) recommendations.

Note that future checks can be added or modified to check for any SSSD setting in the format of `check_sssd_config "${TEST_NO}" 'setting-name' 'expected-value'`

Packaging Guide:

Reference from: <https://www.redhat.com/sysadmin/create-rpm-package>

```
sudo yum install -y rpmdevtools
rpmdev-setuptree
```

This will setup the rpm packaging environment. Then, download the Lynis tarball from Lynis official website and place it in `~/rpmbuild/SOURCES`, note the filename to use later in the spec file.

Put the `plugin_ncsa_phase2`, `default.prp`, and `nodefault.prp` (which skips default checks) in the `~/rpmbuild/SOURCES` directory as well.

Place the following content into `lynis.sh` under `~/rpmbuild/SOURCES` directory as well.

```
#!/bin/bash
cd /opt/lynis
exec ./lynis "$@"
```

Place the following content into `lynis-ncsa.spec` under `~/rpmbuild/SPECS`

```
Name:          lynis-ncsa
Version:       0.1
Release:       1%{?dist}
Summary:       NCSA custom Lynis package
BuildArch:     noarch
License:       GPL
URL:           https://git.ncsa.illinois.edu/irst/lynis-ncsa-plugins
Source0:       lynis-3.0.6.tar.gz
Source1:       lynis.sh
Source2:       default.prf
Source3:       plugin_ncsa_phase2
Source4:       nodefault.prf
Requires:      bash
```

%description

NCSA custom Lynis package with the NCSA plugin

%prep

```
cd ${HOME}/rpmbuild/BUILD
tar xf ../SOURCES/lynis-3.0.6.tar.gz
cp ../SOURCES/lynis.sh .
cp ../SOURCES/default.prf .
cp ../SOURCES/nodefault.prf .
cp ../SOURCES/plugin_ncsa_phase2 .
```

%build

```
chmod +x lynis.sh
mv default.prf lynis
mv nodefault.prf lynis
mv plugin_ncsa_phase2 lynis/plugins
```

%install

```
rm -rf $RPM_BUILD_ROOT
mkdir -p $RPM_BUILD_ROOT/%{_bindir}
mkdir -p $RPM_BUILD_ROOT/opt
mv lynis $RPM_BUILD_ROOT/opt
mv lynis.sh $RPM_BUILD_ROOT/%{_bindir}/lynis
```

%clean

```
rm -rf $RPM_BUILD_ROOT
```

%files

```
%{_bindir}/lynis
/opt/lynis/
```

Then run

```
rpmbuild -bb ~/rpmbuild/SPECS/lynis-ncsa.spec
```

which will build the rpm package under ~/rpmbuild/RPMS/noarch/