PRACTICAL PORTS

Security Scanning a Jail

BY BENEDICT REUSCHLING

This column covers ports and packages for FreeBSD that are useful in some way, peculiar, or otherwise good to know about. Ports extend the base OS functionality and make sure you get something done or, simply, put a smile on your face. Come along for the ride, maybe you'll find something new.

In this installment, I stray a bit from presenting a bouquet of ports and just focus on a single one: security/lynis.

Lynis is a tool for security auditing, hardening, and compliance testing. What lynis does differently from other security scanners is that it tries to detect available components on a system such as a webserver or database. Once it finds them, it checks them further for vulnerabilities, missing patches, etc. This way, the scans are different on each system based on the configured software and purpose. For example, your firewall host may receive different examinations than your backup server. Plugins extend lynis's functionality to cover specific software. A comprehensive security report is generated at the end, eliciting either a pat on the back from your security-minded superiors or your next security sensitivity training.

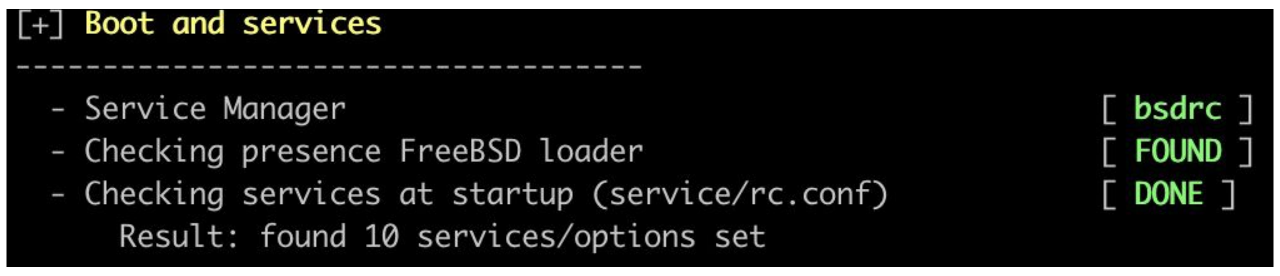
Available as open source as well as a commercial enterprise tool, it scans a range of operating systems for security anomalies. Sysadmins as well as penetration testers, developers, and auditors can use it to assess if there are any vulnerabilities, not only in installed software but also in their configurations. Since this includes the operating system as well as third-party software, running it on a FreeBSD jail should prove to be an interesting experiment.

Available as open source as well as a commercial enterprise tool, lynis scans a range of operating systems for security anomalies.

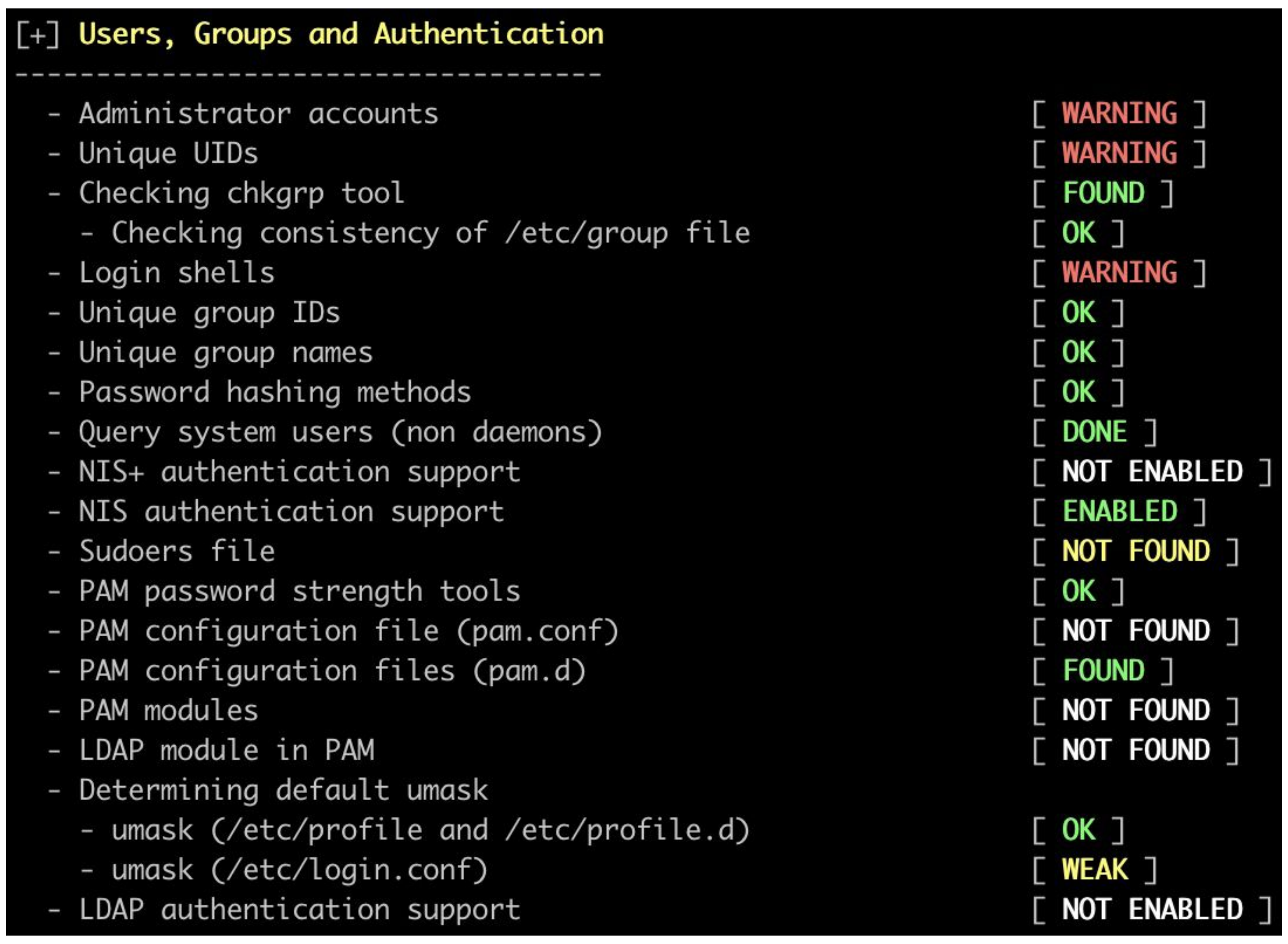
For this purpose, I created an iocage jail from a freshly updated FreeBSD 13.0 host. Note that you can use any other jail management framework or build a jail by hand to repeat this experiment yourself. Entering the console, I run "pkg install lynis" and nothing else (not even my favorite shell), just a plain vanilla jail. This way, we can see what lynis detects in a default installation. If something comes up before any to-be-jailed software is installed, this is something every FreeBSD 13.0 installation (and possibly versions before that) is concerned about—inside or outside a jail.

Before I ran the scan, I looked at the current settings using "lynis show settings". Don't worry about the license-key line, the software works just fine without any limitations in the open-source version. Without further ado, I start the scan by issuing "lynis audit system".

After some initialization, my correctly-detected OS version and hardware platform (amd64) are echoed to the screen. No big surprise there, but it gets interesting further on. The "Boot and Services" section found that by default, 10 services are running ("service -e" will display them in a standard FreeBSD system). Eight modules, including the kernel itself, are loaded, which was actually detected from the host running the jail and forwarded into it. But still, all green so far, until we get to the "Users, Groups and Authentication" section, where the first red warnings are issued. Administrator accounts, unique UIDs, and login shells all seem to be a problem for lynis.



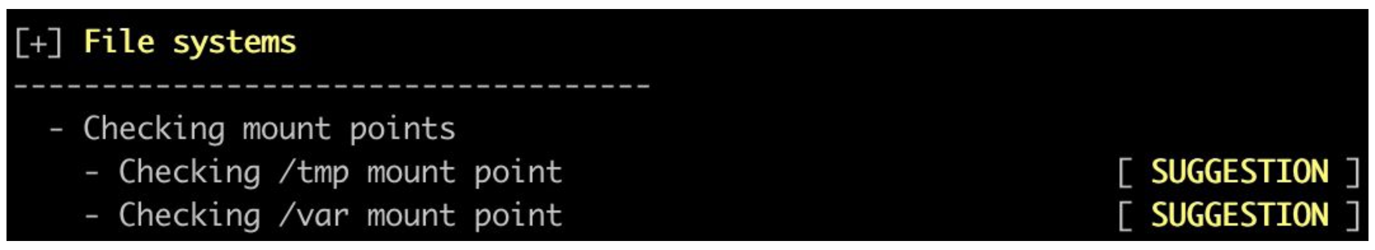
```
[+] Boot and services
------------------------------------
  - Service Manager                                           [ bsdrc ]
  - Checking presence FreeBSD loader                          [ FOUND ]
  - Checking services at startup (service/rc.conf)            [ DONE ]
      Result: found 10 services/options set
```



```
[+] Users, Groups and Authentication
------------------------------------
  - Administrator accounts                                    [ WARNING ]
  - Unique UIDs                                               [ WARNING ]
  - Checking chkgrp tool                                      [ FOUND ]
    - Checking consistency of /etc/group file                 [ OK ]
  - Login shells                                              [ WARNING ]
  - Unique group IDs                                          [ OK ]
  - Unique group names                                        [ OK ]
  - Password hashing methods                                  [ OK ]
  - Query system users (non daemons)                          [ DONE ]
  - NIS+ authentication support                               [ NOT ENABLED ]
  - NIS authentication support                                [ ENABLED ]
  - Sudoers file                                              [ NOT FOUND ]
  - PAM password strength tools                               [ OK ]
  - PAM configuration file (pam.conf)                         [ NOT FOUND ]
  - PAM configuration files (pam.d)                           [ FOUND ]
  - PAM modules                                               [ NOT FOUND ]
  - LDAP module in PAM                                        [ NOT FOUND ]
  - Determining default umask
    - umask (/etc/profile and /etc/profile.d)                 [ OK ]
    - umask (/etc/login.conf)                                 [ WEAK ]
  - LDAP authentication support                               [ NOT ENABLED ]
```

The shells section lists unsecured console TTYs. Note that I only list the offenders here, the rest is either OK-ish or simply not active yet due to missing software. Checking and re-checking the scan after installing additional software for any changes that may have opened an attack vector is good practice.

Lynis not only scolds you for things you should have done better, but it also suggests things like checking /tmp and /var mount points in the "File systems" section. Don't be discouraged if a first scan finds a bunch of issues. Consider it as an overview and a general guideline for improvement. Some of these things are trivial to fix, which subsequent audits should identify as such. If you set up another host in the future, you can already check for these to avoid repeating that mistake.

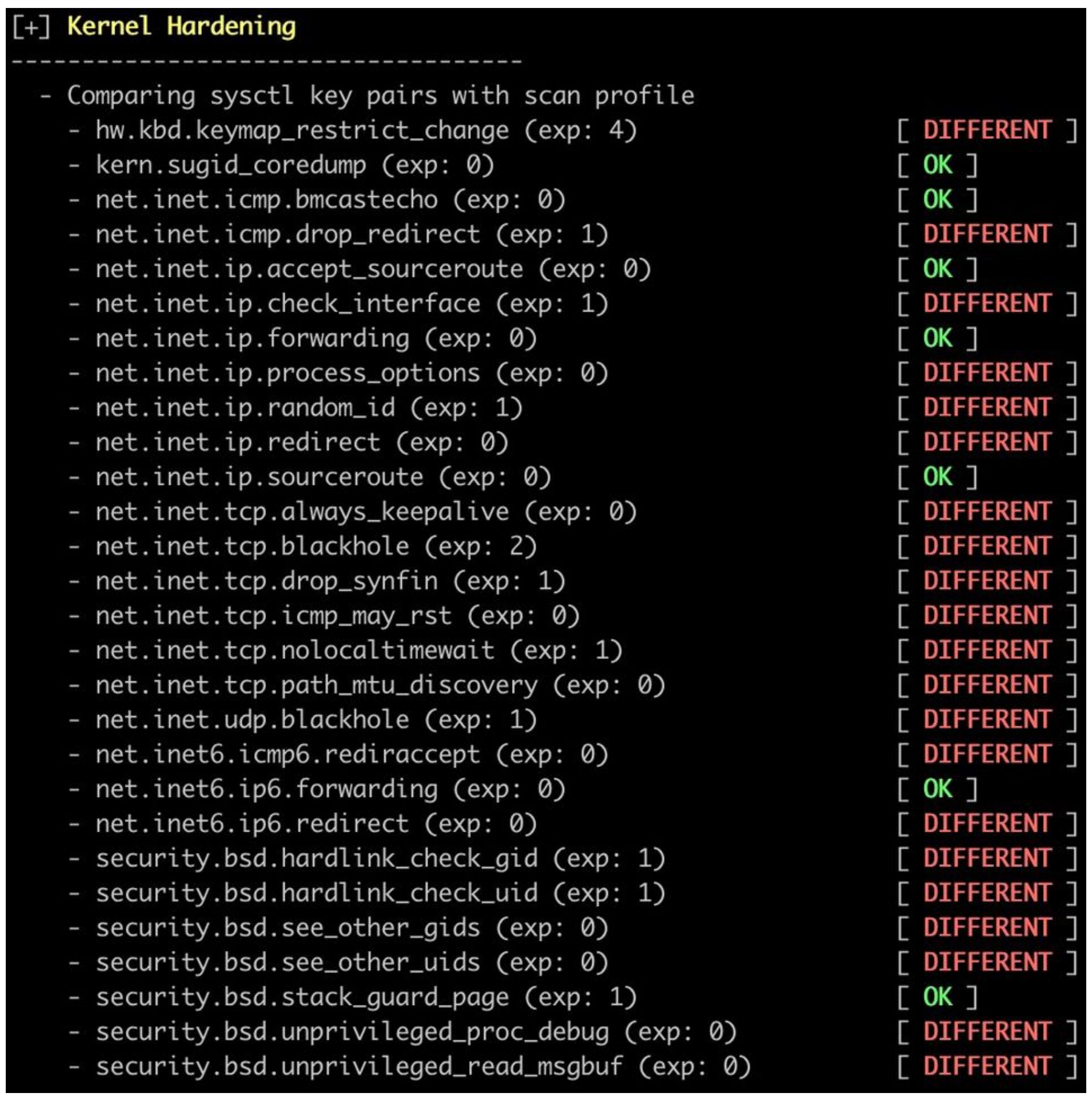


```
[+] File systems
------------------------------------
  - Checking mount points
    - Checking /tmp mount point                               [ SUGGESTION ]
    - Checking /var mount point                               [ SUGGESTION ]
```

Many sections in the lynis report are empty simply because we did not yet install anything. If there would have been some software prone to be a typical attack target, lynis would scan that more thoroughly and add additional results to the report. Overall, this FreeBSD jail does not appear to have many issues. Looking at what was found, one problem seems to be the ownership of home directories. I'm not worried yet since there are at present no users other than root itself on this jail. I do make a note to myself to re-check this, though.

In the "Kernel Hardening" section, there is a list of TCP/IP related sysctl settings that should have a different setting than the default. This means that i.e. net.inet.icmp.drop_redirect is set to 0 by default, but should have been set to 1 (active). There is probably a reason other than "oversight" why this is not set. Perhaps the reason is to make FreeBSD work by default in as many networking environments as possible, where this option might prevent or cause problems. Since the whole list is presented, one can easily set each of those to the recommended value and see if networking still runs normally. If it does, keeping this option on is a good idea.

At the end of the scan, the report lists 4 warnings and 15 suggestions. The easiest warning to fix is the last one, running pkg audit -F to fetch the latest security vulnerability database for ports. The link provided at each suggestion and warning gives further details about the issues and their impacts. Not all of these are of the we'll-lose-our-customer-database-if-we-don't-fix-this-at-once type. Some of them are good sysadmin practices like "avoid /tmp running full", so don't just ignore them as non-security related. Often, security incidents happen not because of a single issue, but because a malicious person was able to combine several unrelated problems into a bigger nightmare.



```
[+] Kernel Hardening
------------------------------------
  - Comparing sysctl key pairs with scan profile
    - hw.kbd.keymap_restrict_change (exp: 4)               [ DIFFERENT ]
    - kern.sugid_coredump (exp: 0)                         [ OK ]
    - net.inet.icmp.bmcastecho (exp: 0)                    [ OK ]
    - net.inet.icmp.drop_redirect (exp: 1)                 [ DIFFERENT ]
    - net.inet.ip.accept_sourceroute (exp: 0)              [ OK ]
    - net.inet.ip.check_interface (exp: 1)                 [ DIFFERENT ]
    - net.inet.ip.forwarding (exp: 0)                      [ OK ]
    - net.inet.ip.process_options (exp: 0)                 [ DIFFERENT ]
    - net.inet.ip.random_id (exp: 1)                       [ DIFFERENT ]
    - net.inet.ip.redirect (exp: 0)                        [ DIFFERENT ]
    - net.inet.ip.sourceroute (exp: 0)                     [ OK ]
    - net.inet.tcp.always_keepalive (exp: 0)               [ DIFFERENT ]
    - net.inet.tcp.blackhole (exp: 2)                      [ DIFFERENT ]
    - net.inet.tcp.drop_synfin (exp: 1)                    [ DIFFERENT ]
    - net.inet.tcp.icmp_may_rst (exp: 0)                   [ DIFFERENT ]
    - net.inet.tcp.nolocaltimewait (exp: 1)                [ DIFFERENT ]
    - net.inet.tcp.path_mtu_discovery (exp: 0)             [ DIFFERENT ]
    - net.inet.udp.blackhole (exp: 1)                      [ DIFFERENT ]
    - net.inet6.icmp6.rediraccept (exp: 0)                 [ DIFFERENT ]
    - net.inet6.ip6.forwarding (exp: 0)                    [ OK ]
    - net.inet6.ip6.redirect (exp: 0)                      [ DIFFERENT ]
    - security.bsd.hardlink_check_gid (exp: 1)             [ DIFFERENT ]
    - security.bsd.hardlink_check_uid (exp: 1)             [ DIFFERENT ]
    - security.bsd.see_other_gids (exp: 0)                 [ DIFFERENT ]
    - security.bsd.see_other_uids (exp: 0)                 [ DIFFERENT ]
    - security.bsd.stack_guard_page (exp: 1)               [ OK ]
    - security.bsd.unprivileged_proc_debug (exp: 0)        [ DIFFERENT ]
    - security.bsd.unprivileged_read_msgbuf (exp: 0)       [ DIFFERENT ]
```

For me, exploring items like "Umask in /etc/login.conf could be stricter like 027" is worth some time. Who knows, maybe that will become the new default in an upcoming FreeBSD release (better than part of a security advisory) once secteam has had time to review it.

Remember that this small experiment only covered the operating system and may reveal more once the jail is doing what it was set up to do. As additional software and services are run and exposed to the internet or even to users on the local network, it will mean that additional scans are advised. Check out the other modes that lynis provides, including the penetration testing mode, as it may reveal additional items for your security to-do list.

Lynis is not the only tool out there. Wise security-minded folks are known to use multiple tools to cover a wider range of possible issues to find (or confirm) another tools suspicion. Tools like portsentry, nmap, nessus, snort, as well as the not-yet-ported terrascan and openvas-scanner, are all fine tools to detect and help close potential security problems before it is too late. Always be suspicious of these tools not finding everything or not finding the latest incidents. Running them regularly is not an excuse to not check security bulletins for the software you run and subscribe to their notifications.

Oh, I just realized that I did mention more than a single tool here. But who am I to keep these to myself?

BENEDICT REUSCHLING is a documentation committer in the FreeBSD project and member of the documentation engineering team. He serves on the board of directors of the FreeBSD Foundation as vice president. In the past, he served on the FreeBSD core team for two terms. He administers a big data cluster at the University of Applied Sciences, Darmstadt, Germany. He's also teaching a course "Unix for Developers" for undergraduates. Together with Allan Jude, he is host of the weekly bsdnow.tv podcast.