
ORACLE®

Tools Used For Security and Compliance

on Linux

Dan Norris
Platform Integration MAA Team

Program Agenda

1. Host-based scanning tools
2. Network-based scanning tools
3. Commercial tools
4. Government tools

Host-based scanning tools

Host-based scanning tools (free)

- lsof
- netstat
- snort
- nessus (free for home use)
- Some tools are only host-based when doing "authenticated" scans

Network-based tools

Network scanning tools

- These scan the subnet/network specified and identify hosts online
- nmap - free
- arp-scan - free
- netdiscover - free
- Autoscan-network.com - free
- Angry IP Scanner (angryip.org) - free
- ** **Beware:** network admins may not like you if you use these without permission

nmap on a single host

```
$ nmap -6 2001:db8::4fff:ffff:ffff:a2ac -p 1-40000

Starting Nmap 5.51 ( http://nmap.org ) at 2016-04-13 08:39 PDT
Nmap scan report for somehost.us.oracle.com (2001:db8::4fff:ffff:ffff:a2ac)
Host is up (0.021s latency).
Not shown: 39989 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
1521/tcp  open  oracle
1830/tcp  open  unknown
3260/tcp  open  iscsi
(continued…)
```

nmap on a single host

```
3872/tcp  open  oem-agent
5000/tcp  open  upnp
6200/tcp  open  unknown
9127/tcp  open  unknown
23792/tcp open  unknown
32190/tcp open  unknown
38372/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 12.33 seconds
$
```

Commercial tools

Commercial scanning tools

- Most tools can do *authenticated* or *unauthenticated* scans
- BeyondTrust Retina
- Qualys QualysGuard
- Tripwire/CIS
- Nessus
- Rapid7 Nexpose
- SAINT - also includes SCAP module

Commercial scanning tools

Exadata-specific

- exachk (MOS 1070954.1) has password check feature
- ./exachk -profile security
- This will check all known passwords on the system to see if they are using default passwords.

Government tools

Government scanning tools

- STIG = Secure Technical Implementation Guide
  - OS: RHEL, OL, Solaris, AIX, Windows, HPUX, etc
  - DB: Oracle, SQL Server
  - More: smart phones, web servers, etc, etc, etc

- NIST STIG - http://iase.disa.mil/stigs/Pages/index.aspx
- SCAP - http://iase.disa.mil/stigs/scap/Pages/index.aspx
  - SCAP only checks about 60% of the STIG criteria

Scanning Operational Considerations

Scanning Operational Considerations

- Regularly patch/update OS - stay ahead of vulnerabilities
- Regularly scan - Monthly, weekly, quarterly?
- Do you have a network crawler that looks for new hosts on the network?
- On existing hosts, will your scan find new ports that are listening?


ORACLE®