What software is running on those things?

CSC 2: Inventory and Control of Software Assets

OpenBSD

```
$ pkg_info
```

MacOS X

```
$ system_profiler SPApplicationsDataType
$ lsappinfo
```

Alpine

```
$ apk info
```

Debian

```
$ dpkg --get-selections
$ apt list –installed
```

RedHat/CentOS

```
$ yum list installed
$ rpm -qa
```

Gentoo

```
$ equery list “*”
$ cat /var/lib/portage/world
```

Are those things exploitable?

CSC 3: Continuous Vulnerability Management

Continuous Vulnerability Management **Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.**	
Run Automated Vulnerability Scanning Tools	Utilize an up-to-date Security Content Automation Protocol (SCAP) compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.
Perform Authenticated Vulnerability Scanning	Perform authenticated vulnerability scanning with agents running locally on each system or with remote scanners that are configured with elevated rights on the system being tested.
Protect Dedicated Assessment Accounts	Use a dedicated account for authenticated vulnerability scans, which should not be used for any other administrative activities and should be tied to specific machines at specific IP addresses.
Deploy Automated Operating System Patch Management Tools	Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.
Deploy Automated Software Patch Management Tools	Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.
Compare Back-to-Back Vulnerability Scans	Regularly compare the results from consecutive vulnerability scans to verify that vulnerabilities have been remediated in a timely manner.
Utilize a Risk-Rating Process	Utilize a risk-rating process to prioritize the remediation of discovered vulnerabilities.

http://www.cisecurity.org/controls/