Host Hardening – Achieve or Avoid

Nilesh Kapoor

Auckland 2016

OWASP

The Open Web Application Security Project

Introduction

OWASP
The Open Web Application Security Project

Nilesh Kapoor

- Senior Security Consultant @ Aura Information Security
- Core 8 years experience in Security Consulting
- Co-Author – Security testing handbook for Banking Applications
- CREST & CEH Certified

aura
INFORMATION SECURITY

POWERED
BY KORDIA

Outline

OWASP
The Open Web Application Security Project

- Real world attack on a SECURE server
- Statistics
- What is host review & hardening?
- Standards for secure configuration review & hardening
- Audit tools
- Challenges, Approach & Optimization

aura
INFORMATION SECURITY

POWERED
BY KORDIA

Real World Attack

OWASP
The Open Web Application Security Project

- Performed a external website and supported infrastructure review for a very well-known NZ e-commerce company
- Website running latest Magento CMS
- Found limited website vulnerabilities and open ports

aura
INFORMATION SECURITY

POWERED
BY KORDIA

Real World Attack

OWASP
The Open Web Application Security Project

- Next target - website hosting server
- Only SSH & SSL is running
- No issues with the SSL layer on port 443
- All secure, right?

aura
INFORMATION SECURITY

POWERED
BY KORDIA

Real World Attack

OWASP
The Open Web Application Security Project

- NMAP script scan (-A) shows ssh-hostkey

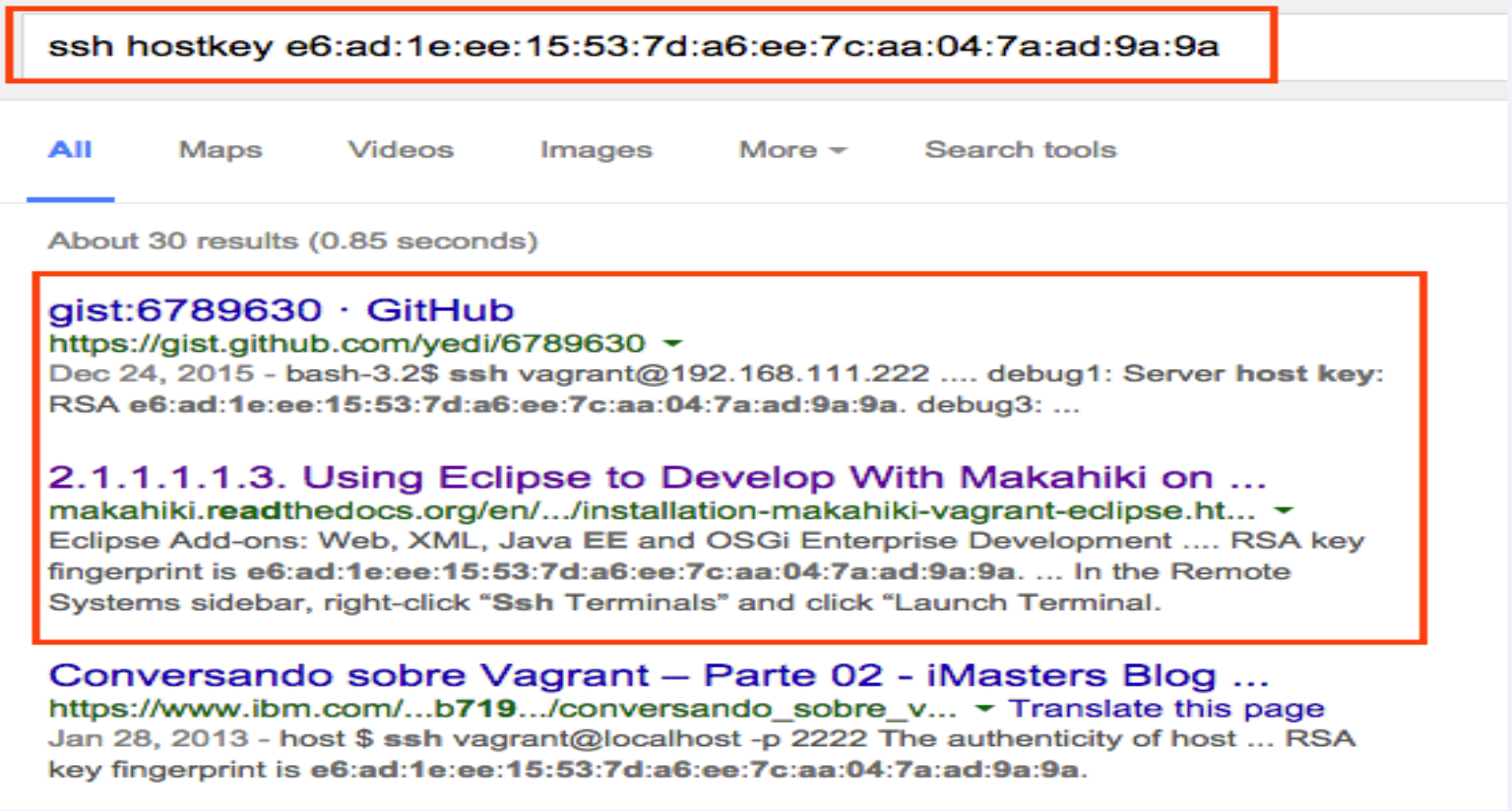
```
hackme@hackme-owasp:~/Documents/vagrant_project$ nmap -A -p22 192.168.0.25

Starting Nmap 6.40 ( http://nmap.org ) at 2016-01-20 15:34 NZDT
Nmap scan report for 192.168.0.25
Host is up (0.053s latency).
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 5.9p1 Debian 5ubuntu1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey: 1024 28:ba:58:9d:6e:b3:86:b4:4d:15:7e:dd:f1:55:be:43 (DSA)
|  2048 e6:ad:1e:ee:15:53:7d:a6:ee:7c:aa:04:7a:ad:9a:9a (RSA)
|_256 32:53:5d:95:d9:2b:c0:92:ab:1d:a4:87:95:a6:5a:e2 (ECDSA)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 5.81 seconds
```

- Next, bit of Google

Real World Attack

OWASP
The Open Web Application Security Project

- ssh-hostkey indicates Vagrant running on hosting server



Real World Attack

OWASP
The Open Web Application Security Project

- What is Vagrant?
  - Software that allows developers spin virtual development environment with pre-installed tools. Sounds interesting!!!
  - Runs Ubuntu virtual machine without a UI
  - By default, SSH accessible virtual machine
  - Default SSH-key based authentication

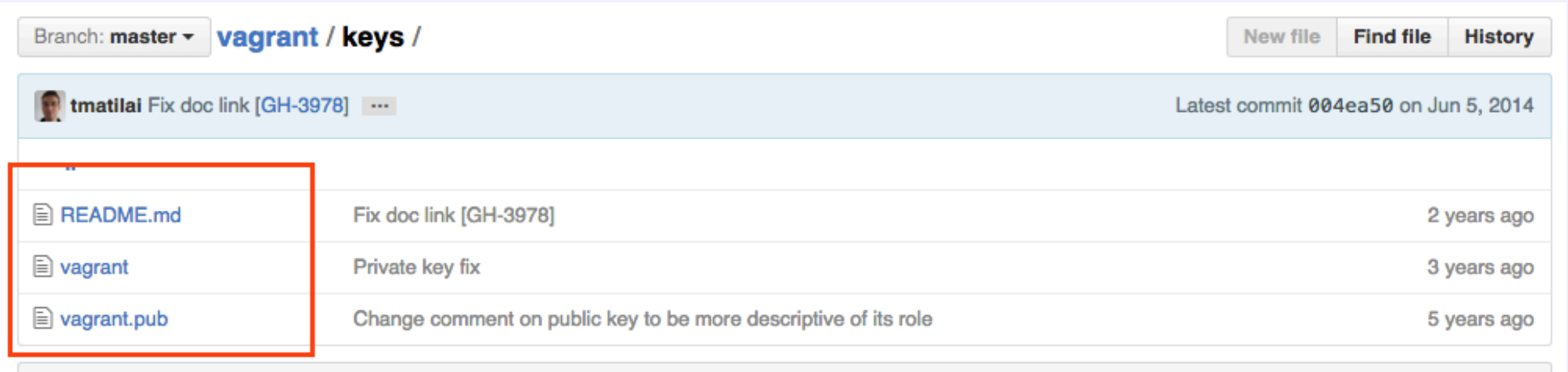
aura
INFORMATION SECURITY

POWERED
BY KORDIA

Real World Attack

OWASP
The Open Web Application Security Project

- What next??
- SSH keys are publicly accessible
- Default SSH user: vagrant



aura
INFORMATION SECURITY

POWERED
BY KORDIA

Real World Attack

OWASP
The Open Web Application Security Project

- One command to get a shell…☺

```
ssh vagrant@<IP_Address> -i /etc/ssh/vagrant
```

  - If password authentication is enabled on remote server
  - Default password: vagrant

aura
INFORMATION SECURITY

POWERED
BY KORDIA

Real World Attack

OWASP
The Open Web Application Security Project

```
hackme@hackme-owasp:~$ ssh vagrant@192.168.0.25 -i /home/hackme/vagrant
Welcome to Ubuntu 12.04 LTS (GNU/Linux 3.2.0-23-generic-pae i686)

 * Documentation:  https://help.ubuntu.com/
New release '14.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Welcome to your Vagrant-built virtual machine.
Last login: Mon Feb  1 00:55:40 2016 from 192.168.0.1
vagrant@precise32:~$ whoami
vagrant
vagrant@precise32:~$
```

Solution

OWASP
The Open Web Application Security Project

- Host review and hardening should have fixed this
- Remove default user ”vagrant”
- Disable password based authentication
- Regenerate ssh keychain

```
sudo rm -rf /etc/ssh/ssh_host_*
sudo dpkg-reconfigure openssh-server
sudo service ssh restart
```

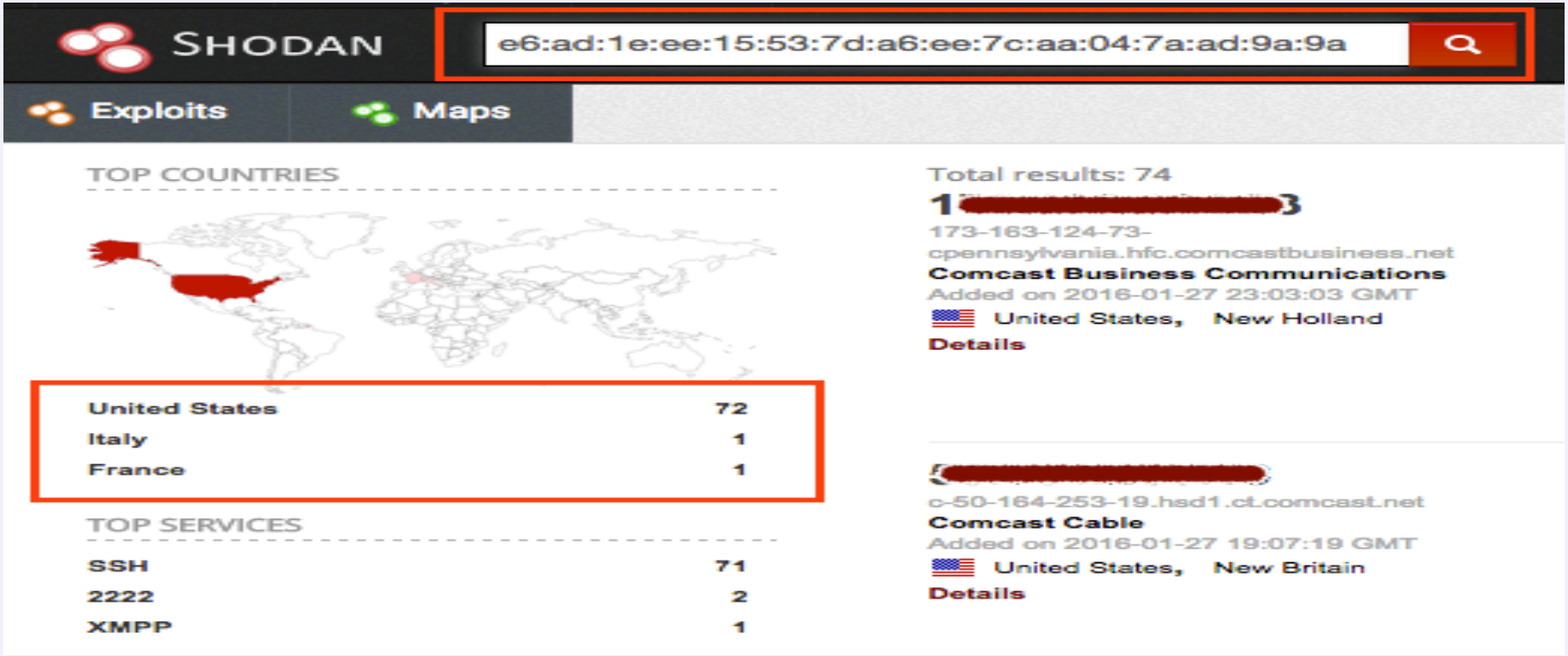
aura
INFORMATION SECURITY

POWERED
BY KORDIA

Statistics

OWASP
The Open Web Application Security Project

- Search ssh-hostkey on shodan.io



- List of Vagrant running servers
  - Do not attempt exploiting without authorisation

Statistics

OWASP
The Open Web Application Security Project

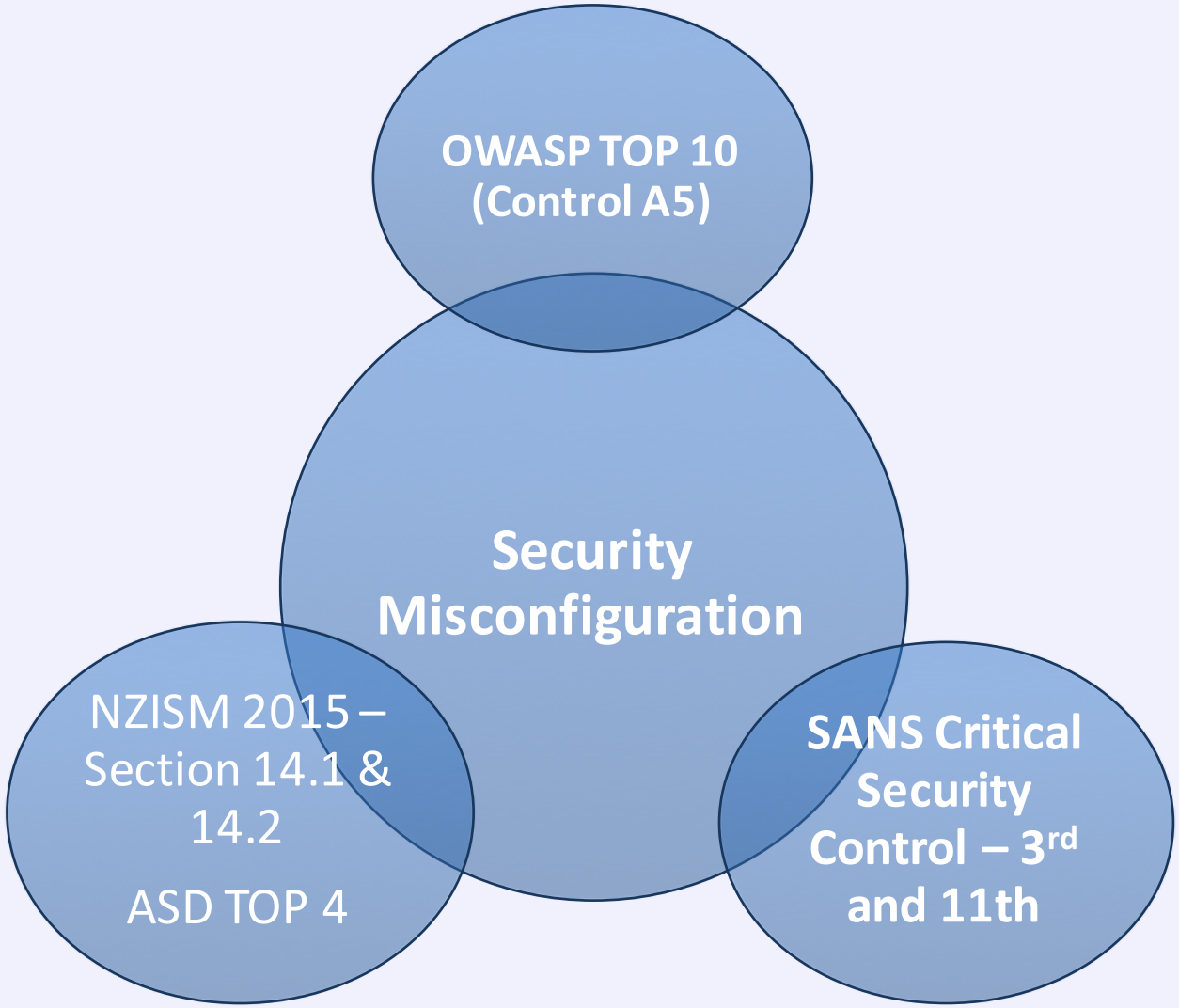
- In 2004, British Telecom & Gartner concluded up to 65% external attacks are due to insecure configuration
- In 2011, Gartner considered secure configuration management a must-have rather than nice-to-have control
- In 2012, SANS lists secure configuration as 3rd and 10th critical security control

aura
INFORMATION SECURITY

POWERED
BY KORDIA

2015/16 Statistics

OWASP
The Open Web Application Security Project



What is Host Review & Hardening?

OWASP
The Open Web Application Security Project

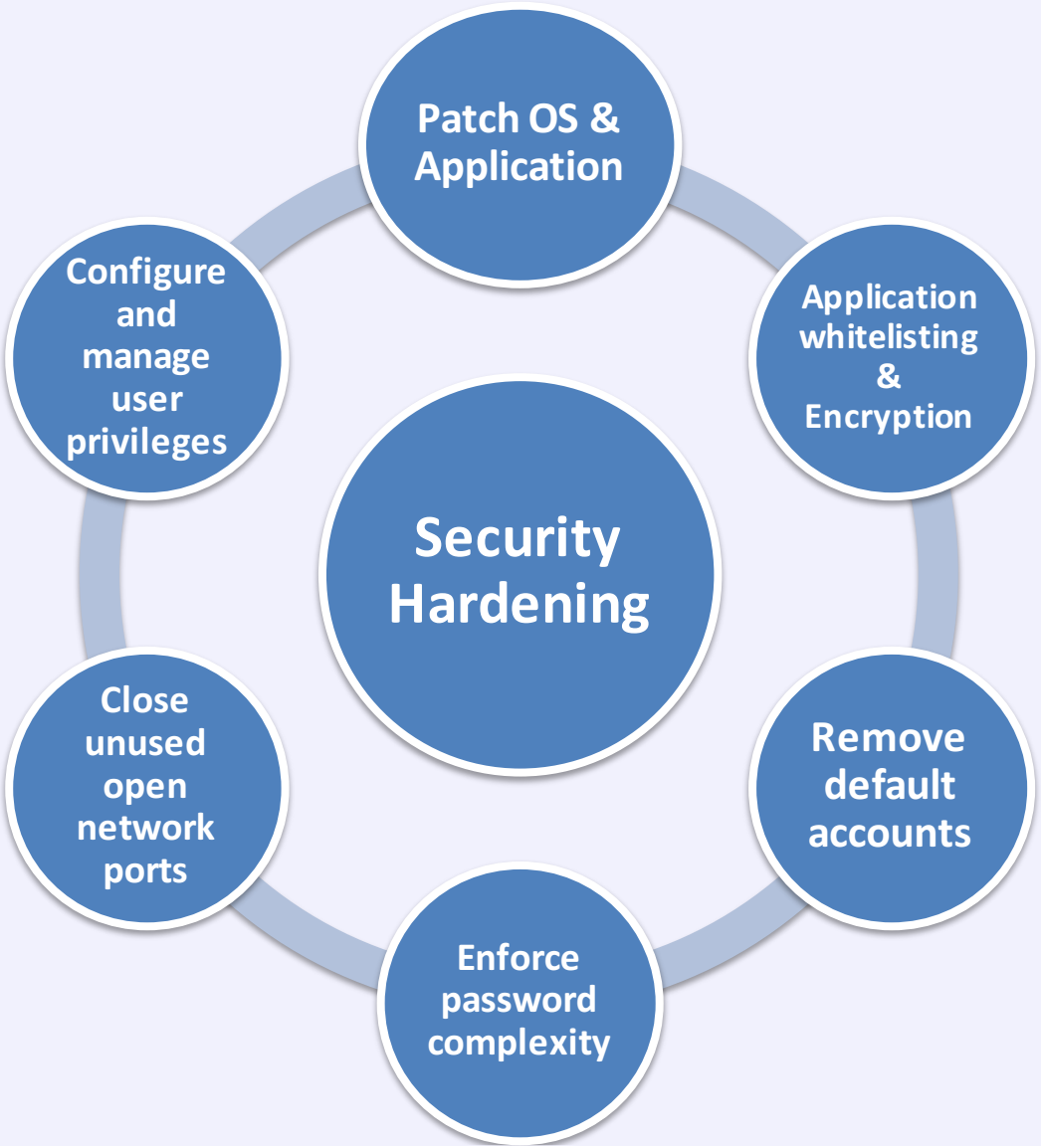
- Host Review & Hardening
  - Identifies system level insecure configuration & settings
  - Applies to operating system, network devices, databases and web servers

aura
INFORMATION SECURITY

POWERED
BY KORDIA

What is Host Review & Hardening?

OWASP
The Open Web Application Security Project



Security hardening standards

OWASP
The Open Web Application Security Project

- Center of Internet Security (CIS)
  - Audit & Hardening benchmarks for almost every OS, web server, database available free of charge

- OWASP Secure Configuration Guide (In Progress)
  - Hardening guide available for web servers, application servers, web frameworks, CMS

aura
INFORMATION SECURITY

POWERED
BY KORDIA

Security hardening standards

OWASP
The Open Web Application Security Project

- Microsoft's Baseline Server Hardening Guidelines
  - Security hardening for base server install

- NZISM & ASD Top 4
  - Governance minimum baseline acceptable controls for "system hygiene"

aura
INFORMATION SECURITY

POWERED
BY KORDIA

Audit Tools

OWASP
The Open Web Application Security Project

- Microsoft Baseline Security Analyzer (MBSA)
  - Looks at OS patch level, default OS accounts, anonymous access, SQL & IIS checks
- Just released - Microsoft Policy Analyser
  - Looks at group policy, local registry for security weaknesses

aura
INFORMATION SECURITY

POWERED
BY KORDIA

Audit Tools

OWASP
The Open Web Application Security Project

- Nessus Professional ($$$)
  - Paid tool. Lets you audit target machine against various industry benchmark or your own company baseline

- CIS-CAT Benchmark Assessment Tool ($$$$$)
  - Paid tool. Lets you audit target machine against CIS security benchmarks.

aura
INFORMATION SECURITY

POWERED
BY KORDIA

Benefits

OWASP
The Open Web Application Security Project

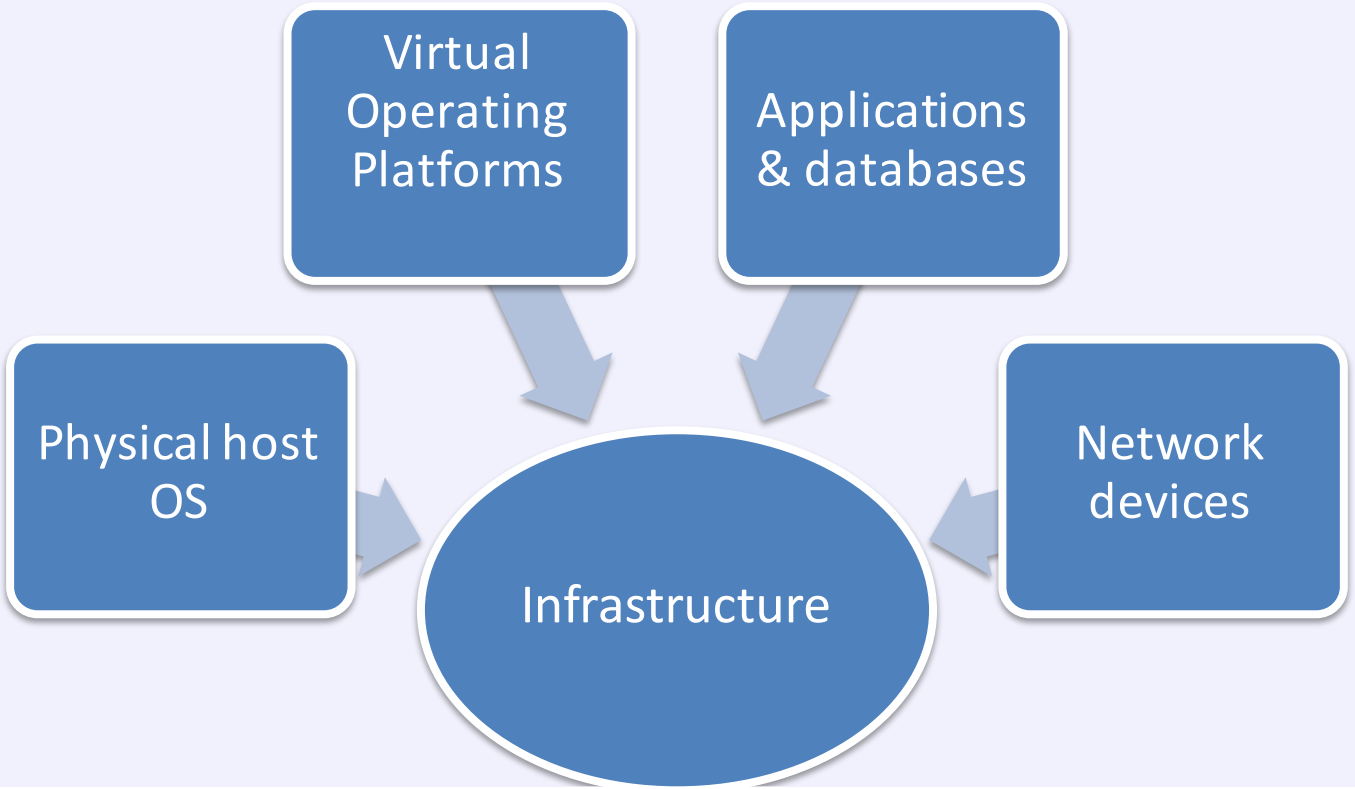
- **Benefits**
  - Detect and fix issues at early stage
  - Bring all systems to known security hardened state
  - Minimize insiders threat
  - Achieve IT audit compliance requirement

aura
INFORMATION SECURITY

POWERED
BY KORDIA

Challenges

In an *InformationWeek* survey of CISOs, "enforcing security policies" was ranked as No. 2 "biggest security challenge"



Challenges

OWASP
The Open Web Application Security Project

1. Asset & Application platform visibility
2. Communication issues – Introduces an opportunity for an attacker to look for exploit

aura
INFORMATION SECURITY

POWERED
BY KORDIA

Approach

OWASP
The Open Web Application Security Project

Discovery

- To overcome visibility, develop an asset inventory
- Categorize external and internal asset
- Establish process to discover new assets (or changes in assets)

aura
INFORMATION SECURITY

POWERED
BY KORDIA

Approach

OWASP
The Open Web Application Security Project

Hardening

- Determine set of secure configuration for your organisation
  - Security requirement of a software development company differs from financial institute
- Develop a baseline security standard for each platform

aura
INFORMATION SECURITY

POWERED
BY KORDIA

Approach

OWASP
The Open Web Application Security Project

Hardening – Continued

- Aim to bring each platform in known security state
- Stay aligned with industry security standard

- Document deviations, exceptions from the baseline

aura
INFORMATION SECURITY

POWERED
BY KORDIA

Approach

OWASP
The Open Web Application Security Project

- **Optimize hardening**
  - Develop process to harden server before deployment of any critical data
  - Educate people of the hardening process

- Powershell cmdlets in Windows & Shell script in Linux could make life easier

aura
INFORMATION SECURITY

POWERED
BY KORDIA

email: nilesh@aurainfosec.com