

# 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



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



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



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?



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 Subuntu1 (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

ssh hostkey e6:ad:1e:ee:15:53:7d:a6:ee:7c:aa:04:7a:ad:9a:9a

All Maps Videos Images More ▾ Search tools

About 30 results (0.85 seconds)

[gist:6789630 · GitHub](#)  
<https://gist.github.com/yedi/6789630> ▾  
Dec 24, 2015 - bash-3.2\$ ssh vagrant@192.168.111.222 .... debug1: Server host key:  
RSA e6:ad:1e:ee:15:53:7d:a6:ee:7c:aa:04:7a:ad:9a:9a. debug3: ...

[2.1.1.1.3. Using Eclipse to Develop With Makahiki on ...](#)  
[makahiki.readthedocs.org/en/.../installation-makahiki-vagrant-eclipse.ht...](http://makahiki.readthedocs.org/en/.../installation-makahiki-vagrant-eclipse.ht...) ▾  
Eclipse Add-ons: Web, XML, Java EE and OSGi Enterprise Development .... RSA key  
fingerprint is e6:ad:1e:ee:15:53:7d:a6:ee:7c:aa:04:7a:ad:9a:9a. ... In the Remote  
Systems sidebar, right-click "Ssh Terminals" and click "Launch Terminal."

[Conversando sobre Vagrant – Parte 02 - iMasters Blog ...](#)  
[https://www.ibm.com/...b719.../conversando\\_sobre\\_v...](https://www.ibm.com/...b719.../conversando_sobre_v...) ▾ Translate this page  
Jan 28, 2013 - host \$ ssh vagrant@localhost -p 2222 The authenticity of host ... RSA  
key fingerprint is e6:ad:1e:ee:15:53:7d:a6:ee:7c:aa:04:7a:ad:9a:9a.

# 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

# Real World Attack



## OWASP

The Open Web Application Security Project

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

Branch: master [vagrant](#) / [keys](#) /

New file Find file History

tmatilai Fix doc link [GH-3978] ... Latest commit 004ea50 on Jun 5, 2014

<a href="#">README.md</a>	Fix doc link [GH-3978]	2 years ago
<a href="#">vagrant</a>	Private key fix	3 years ago
<a href="#">vagrant.pub</a>	Change comment on public key to be more descriptive of its role	5 years ago



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**

# 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

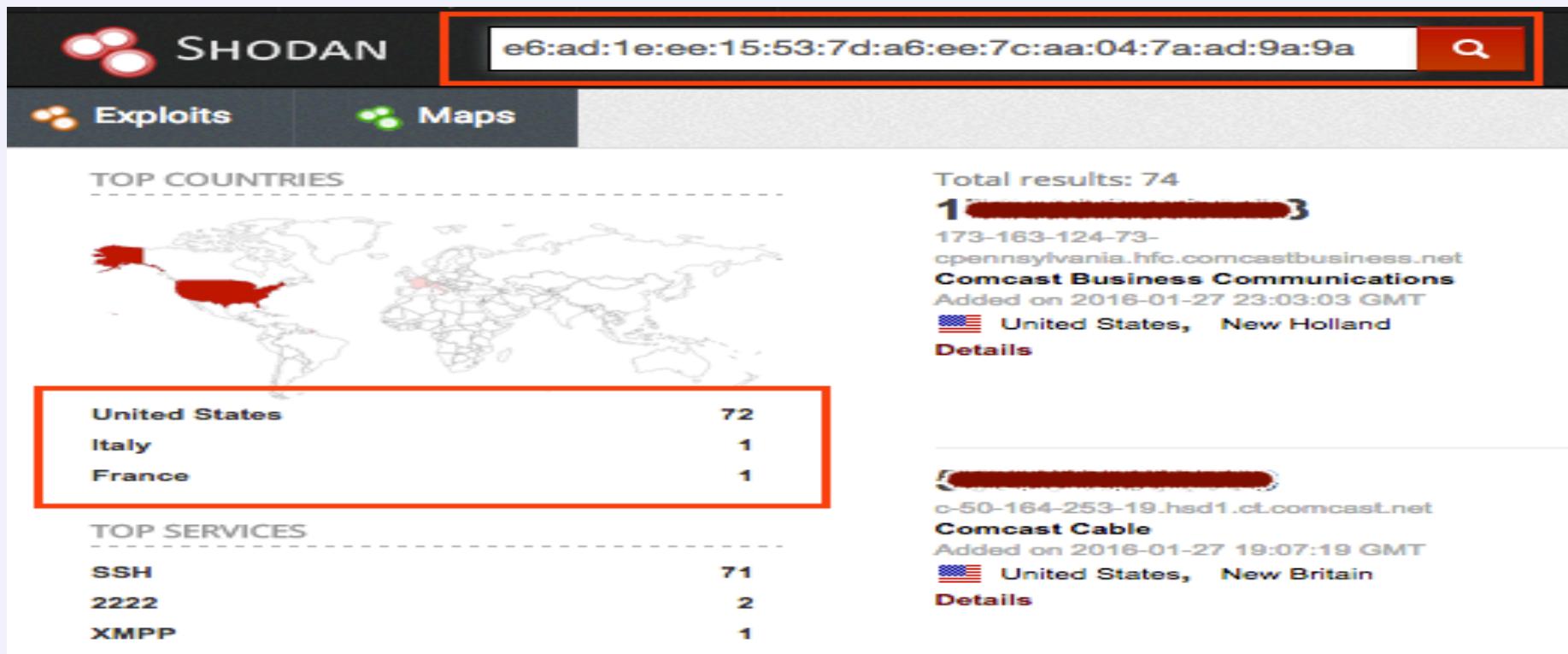
# Statistics



# OWASP

The Open Web Application Security Project

- Search ssh-hostkey on shodan.io



A screenshot of the Shodan search interface. The search bar contains the hex string "e6:ad:1e:ee:15:53:7d:a6:ee:7c:aa:04:7a:ad:9a:9a". The results page shows a world map with red dots indicating found hosts. Below the map is a table of top countries:

Country	Count
United States	72
Italy	1
France	1

Below the table is a section for top services:

Service	Count
SSH	71
2222	2
XMPP	1

The main search results area displays the following entry:

Total results: 74

1 [REDACTED] 3  
173-163-124-73-  
cpennsylvania.hfc.comcastbusiness.net  
**Comcast Business Communications**  
Added on 2016-01-27 23:03:03 GMT  
United States, New Holland  
[Details](#)

Below this result is another entry:

5 [REDACTED]  
c-50-164-253-19.hsd1.ct.comcast.net  
**Comcast Cable**  
Added on 2016-01-27 19:07:19 GMT  
United States, New Britain  
[Details](#)

- 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 **3<sup>rd</sup>** and **10<sup>th</sup>** critical security control



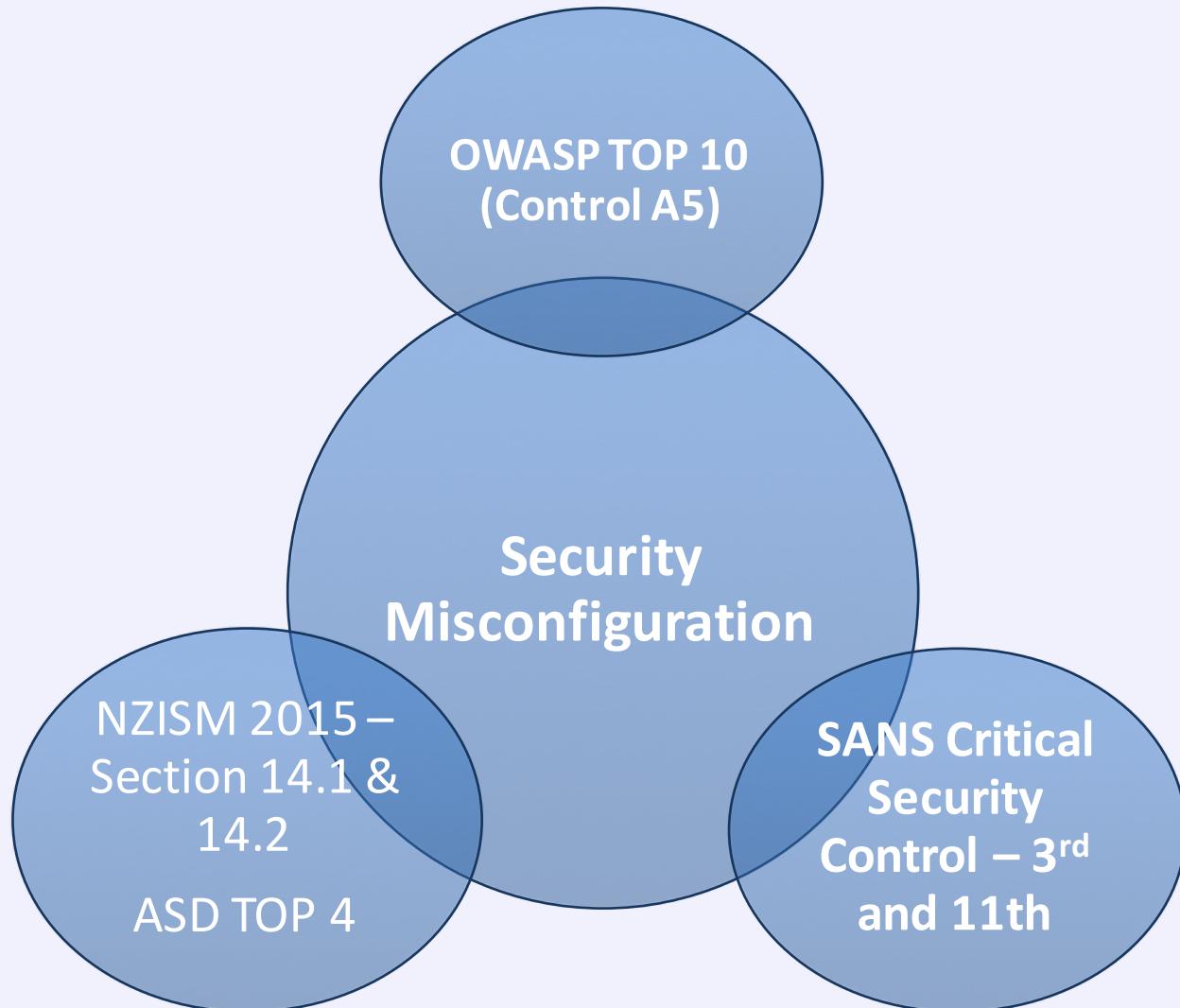
POWERED  
BY KORDIA

# 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



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

# 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"

# 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



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.



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

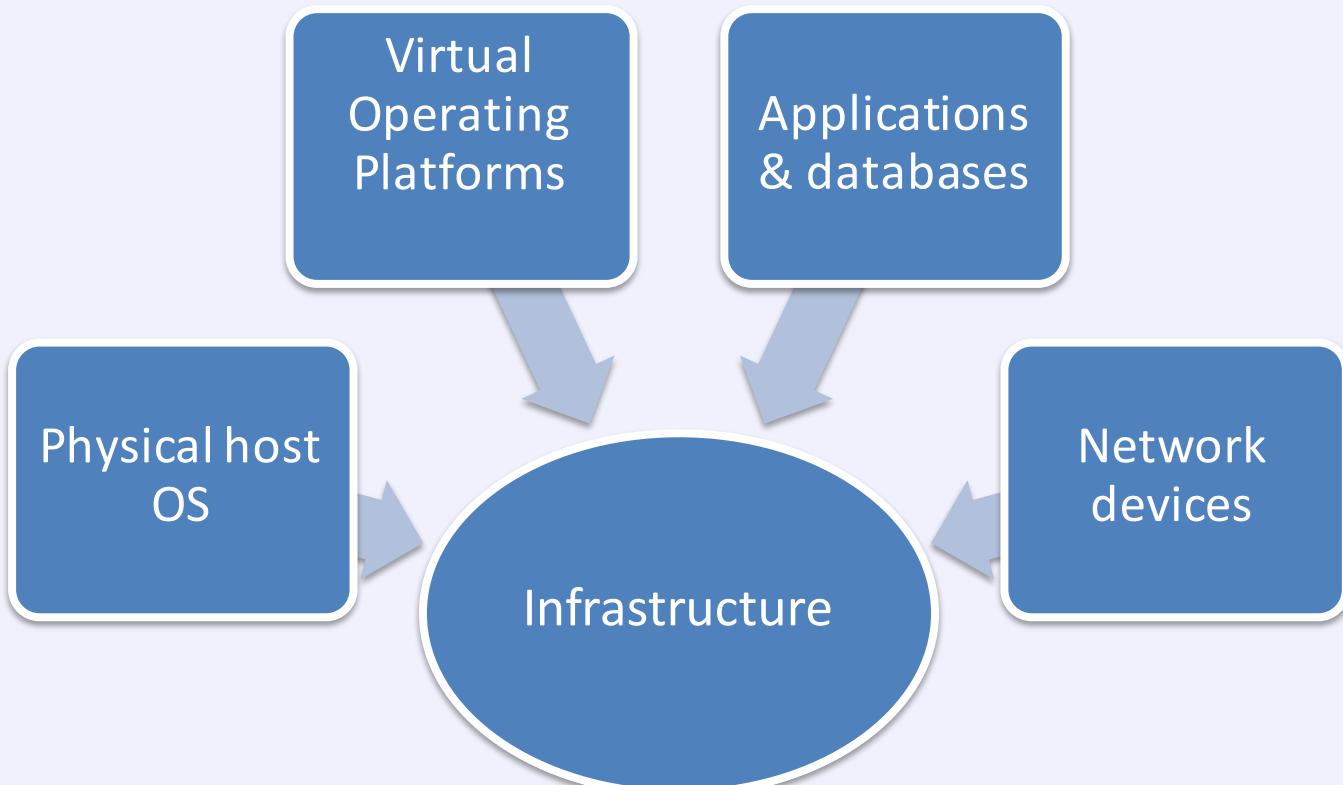


# OWASP

The Open Web Application Security Project

## Challenges

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





# OWASP

The Open Web Application Security Project

## Challenges

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

# 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)

# 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



## Hardening – Continued

- Aim to bring each platform in known security state
- Stay aligned with industry security standard
- Document deviations, exceptions from the baseline

# 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



# OWASP

The Open Web Application Security Project

# Questions?



email: nilesh@aurainfosec.com