



Raspberry Pi for the Infrastructure and hacker



OWASP
The Open Web Application Security Project

About Me



OWASP

The Open Web Application Security Project

Fred Donovan

Professor of Cyber Security Bellevue University

14 yrs Executive IT Consultant (US, APAC, EU)

Founder of Attack Logic, a U.S. based AppSec consultancy

InfoSec Researcher and Hacker

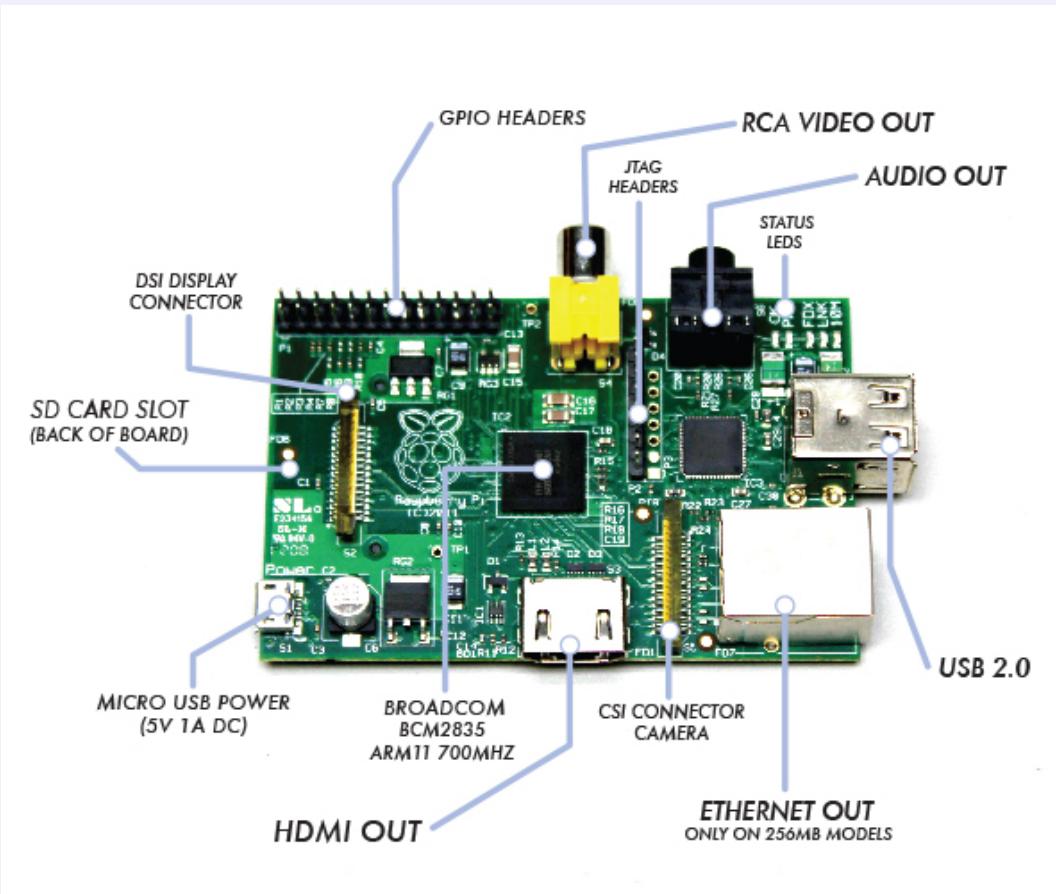
Likes Defense - Prefers Offense



OWASP

The Open Web Application Security Project

The ultra-small form-factor hardware





OWASP

The Open Web Application Security Project

Making it useful for a business



Kein
Schwein
ruft mich
an.



OWASP

The Open Web Application Security Project



Challenges: A kid can do it right?

No longer a lab curiosity

The “simplicity” goes out the door when you integrate mechanisms and algorithms

Minimizing CPU cycles

Business related implementations take considerable engineering skills



OWASP

The Open Web Application Security Project



Hardware modifications

Swap File Size

1.5 GB of SD space generating 2GB of RAM

Changing the CPU design

Converting the GPU to a RISC CPU



OWASP

The Open Web Application Security Project

Q-Box - An infrastructure monitoring device



126mm x 70mm x 28mm

170 grams

8 watts full load, 120v-240v

No fan or any moving parts

Operates 0°C–70°C

1GB NIC

802.11 b/g/n WiFi



OWASP

The Open Web Application Security Project



Q-Box - An infrastructure monitoring device

Nagios®



modsecurity
Open Source Web Application Firewall





OWASP

The Open Web Application Security Project



Significance of the Q-Box

Unprecedented ultra-small form factor

Extremely low power consumption

Built on open-source frameworks

Partitioned Virtual RAM

Converted to RISC CPU

Simultaneous infrastructure applications



OWASP

The Open Web Application Security Project



Q-Box - Other software modifications

Etherwake

TightVNC

SSH via Security Certificate

ClamAV

Nmap suite (Nmap, Zenmap, Ncat, Ndiff, and Nping).





OWASP

The Open Web Application Security Project



Unprecedented hardware modifications to an ultra-small form factor

Extremely low power consumption - 8 watts

Built on open-source frameworks

Partitioned Virtual RAM

Converted to RISC CPU

Simultaneous infrastructure applications



OWASP

The Open Web Application Security Project

H-Box - The hacker box



126mm x 70mm x 28mm

170 grams

8 watts full load, 120v-240v

No fan or any moving parts

Operates 0°C–70°C

1GB NIC

802.11 b/g/n WiFi

Bluetooth 3.0 Class 2



OWASP

The Open Web Application Security Project

H-Box - The hacker box

Aircrack-ng suite Anonymizer Universal asleap BED BeEF

bluebugger bluesnarfer btaudit Burp Suite cirt-fuzzer

Cisco-AuditingTool Cisco-exploiter DirBuster Ettercap

ettercap-gtk ettercap-plugins fasttrack fg-dump hping

ipcalc John the Ripper Laudanum mdcoll Metasploit Mimikatz

Nmap Oclhashcat Rainbowcrack Recon-ng Samaurai WTF SET

siege-ssl ssldump THC-Hydra Zed Attack Proxy





OWASP

The Open Web Application Security Project

H-Box – The hacker box

Internal Corporate Testing

Portable Hacking Box

Capabilities

Web Attacks

Network Attacks

WiFi

Bluetooth



Currently in use attached to Class-B network and utilizing the Wireless IP of the Laptop in which it is attached



OWASP

The Open Web Application Security Project

What's next??

Q-Hpot Honeypot Server

Capabilities

NOVA

HoneyD

ClamAV



Currently in use attached to Class-B network and utilizing the Wireless IP of the Laptop in which it is attached



OWASP

The Open Web Application Security Project



And next??

Super computations in a cluster.

$$\frac{1}{\pi} = \frac{\sqrt{10005}}{4270934400} \sum_{k=0}^{\infty} (-1)^k \frac{(6k)!}{(k!)^3 (3k)!} \frac{(13591409 + 545140134k)}{640320^{3k}}$$

U ed.



OWASP

The Open Web Application Security Project



DEMO





OWASP

The Open Web Application Security Project



Questions