Raspberry Pi for the Infrastructure and hacker

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
The ultra-small form-factor hardware
Making it useful for a business

Kein Schwein ruft mich an.
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
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
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
Q-Box – An infrastructure monitoring device
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
Q-Box – Other software modifications

Etherwake
TightVNC
SSH via Security Certificate
ClamAV
Nmap suite (Nmap, Zenmap, Ncat, Ndiff, and Nping).
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
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
H-Box – The hacker box
Aircrack-ng suite Anonymizer Universal asleep 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 sslscan THC-Hydra Zed Attack Proxy
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
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
And next??
Super computations in a cluster.

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