A PRACTICAL APPROACH TO NETWORK VULNERABILITY ASSESSMENT

Staying one step ahead of the bad guys…

June 11, 2014

Gary Holtz, CISSP, C|EH, GSEC
Brian Voss, CISSP

©2014 Hewlett Packard Company
AGENDA

- Security Trends in 2014
  - Defining vulnerability, risk and threat
  - A Layered approach to Security – defense in depth
  - Identifying Vulnerabilities and related controls
  - Questions and Discussion
THE SEVEN MOST DANGEROUS NEW TECHNIQUES AND WHAT'S COMING NEXT

– Bad Guys Go Wireless & Mobile
  • RFID skimming in hotel or retail environments for card or other ID info
  • Attacks against mobile phones, tablets, and other untethered devices
  • Attackers using mobile devices as attack platforms are less conspicuous

– Air Gaps Are Dying - Innovative side channel attacks
  • If your security model depends solely on your system being air gapped, you will get pwned (USB keys, Pervasive Wireless, Smart Phone charging, eSound)

– Hacking the Internet of Things
  • Hackers reverse engineering embedded system (stripped down Linux based, http)
  • hacking with physical impact
  • In last 12 months, web cams and home router vulns
  • Up next? Thermostats, electronic locks, home automation

– Cyber Currency (Bitcoin)

– Point of Sale Malware: Data intercepted before encryption

– Harvesting Social Networks

– Discovery and Compromise of Industrial Control Systems
PREDATORY HACKING OF MOBILE DEVICES

- Communications Networks
  - Cellular
  - Wifi (WiPhising)
  - Bluetooth
  - NFC
- Malicious Apps
- Physical Access
  - USB (Juice Jacking)
  - SIM
  - Dock/Accessory Connector
  - Lock Screen
- Other
  - QR Code
  - RFID

Typing complex passwords on this???
HACKING THE INTERNET OF THINGS

• Hackers reverse engineering embedded system (stripped down Linux based, http)
• Hacking with physical impact
  – *Increasingly, if a hack doesn’t have kinetic impact… it seems far less interesting*
• In last 12 months, web cams and home router vulnerabilities
• Up next? Thermostats, electronic locks, home automation
HACKING EXPOSED: DAY OF DESTRUCTION
– Frying the Machine via Taking control of Advanced Configuration and Power Interface (ACPI) Embedded Controller
  • Most ACPI chips are not frequently updated by their manufacturers
  • Some laptops have open-source chip firmware and updater
  • Turn off the fans, Spike the CPU to 100%, Watch the temperature rise to boiling water level
– Rendering a PC worthless via ACPI Embedded Controller Firmware update
  • Social Engineer a victim to apply a patch
  • Patch updates the ACPI firmware and reboots the machine
  • Machine locks up during the update
  • Reboot renders the machine unbootable
HACKING TRAINS, PLANES AND AUTOMOBILES

• Hack in The Box Conf Amsterdam 2014: Remotely hacking airplanes (controversy about realism and applicability, but still…)
• DEF CON 2012: Talk on hacking trains in Spain
• DEC CON 2014: Charlie Miller & Chris Valasek on hacking cars
  • CAN’s and ECU’s
  • CAN injection
  • Steering, Brakes, Speed

https://www.youtube.com/watch?v=oqe6S6m73Zw
TOO CRITICAL TO FAIL: CYBER-ATTACKS ON ERP, CRM, SCM AND HR SYSTEMS

- UDP Packet sent to JDE with string of “SHUTDOWN” takes it down
- There are 15,000 ERP systems exposed on the Internet
- Scripts exist to exploit SAP/R3 – Script Kiddies can do attacks
- 2007 – Students hacked Peoplesoft to fix their grades
- 2012 – Anonymous released exploit to SAP systems
- 2013 – Malware targeting SAP systems was discovered in the wild
- Companies have “ERP Security Teams”, but their primary role is doing user admin activities.
- Rarely is anyone looking at protecting the technical layers of the environment
CRYPTO CURRENCY (BITCOIN)

– Cryptocurrency is an emerging technology. Bitcoin is the most pervasive at this point, but there are others as well such as Litecoin, Peercoin, Sexcoin and Dogecoin.

– Cryptocurrencies are specifications regarding the use of currency which seek to incorporate principles of cryptography to implement a distributed, decentralized and secure information economy.

– Highly volatile and sometimes misunderstood. People have made mistakes as well – losing their electronic wallet, disclosing their private key, spending the wrong amount.

– Recent shutdowns of Bitcoin exchanges like Mt. Gox because of being hacked add uncertainty to more wide use of cryptocurrency.
SOCIAL ENGINEERING: WHEN THE PHONE IS MORE DANGEROUS THAN MALWARE

– Vishing is a term for “voice phishing” – targeting a specific person and using the phone to access them.

– Humans are always the weakest link – friendly and helpful by nature.

– An effective Security Awareness program incorporates various types of social engineering (e.g. phishing emails), and if the person opens the attachment, or clicks the URL they will be immediately notified and are given instructions to change their behavior next time.

– Recent scams include attackers going through gated communities offering to “tune up” a person’s PC (and copying their hard drive before leaving.)

– Phoning vulnerable adults posing as grandkids needing help.
FUN WITH THE PROXMARK3

Welcome to the Proxmark III online store. We offer the fastest way to get started researching RFID and Near Field Communication systems using the powerful Proxmark III device.

- Pre-programmed thoroughly tested boards
- Read & emulate any RFID tag
- Orders ship within 2 business days

Get Yours Today!

Please see the FAQ and Terms of Sale. Additional information can be obtained by contacting sales@proxmark3.com. This website requires that javascript be enabled to function correctly.

<table>
<thead>
<tr>
<th>Product</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enclosed Proxmark III</td>
<td>$399</td>
</tr>
<tr>
<td>Naked Proxmark III</td>
<td>$229</td>
</tr>
<tr>
<td>Low Frequency Antenna</td>
<td>$59</td>
</tr>
<tr>
<td>High Frequency Antenna</td>
<td>$59</td>
</tr>
<tr>
<td>Tag Bundle</td>
<td>$12</td>
</tr>
</tbody>
</table>
SANS 20 CRITICAL SECURITY CONTROLS

Critical Control 1: Inventory of Authorized and Unauthorized Devices
Critical Control 2: Inventory of Authorized and Unauthorized Software
Critical Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
Critical Control 4: Continuous Vulnerability Assessment and Remediation
Critical Control 5: Malware Defenses
Critical Control 6: Application Software Security
Critical Control 7: Wireless Device Control
Critical Control 8: Data Recovery Capability
Critical Control 9: Security Skills Assessment and Appropriate Training to Fill Gaps
Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
Critical Control 11: Limitation and Control of Network Ports, Protocols, and Services
Critical Control 12: Controlled Use of Administrative Privileges
Critical Control 13: Boundary Defense
Critical Control 14: Maintenance, Monitoring, and Analysis of Audit Logs
Critical Control 15: Controlled Access Based on the Need to Know
Critical Control 16: Account Monitoring and Control
Critical Control 17: Data Loss Prevention
Critical Control 18: Incident Response and Management
Critical Control 19: Secure Network Engineering
Critical Control 20: Penetration Tests and Red Team Exercises

http://www.sans.org/critical-security-controls/
POINT OF SALE MALWARE

- Data intercepted before encryption
- Physical devices plugged in to capture data for later collection
- Infected software/firmware deployed from IT

HP has been hired by a retail company to take pictures of point of sale equipment at each retail location on a periodic basis for detection purposes (as an example).
HARVESTING SOCIAL NETWORKS

Too much information online today

- Professional information
- Personal information
- Family
- Hobbies
- Location
- Charity/volunteer
- Likes/dislikes

Aggregate information can by assembled for a detailed profile
COMPROMISE OF INDUSTRIAL CONTROL SYSTEMS

- Default credentials
- Less IT visibility
- Often connected to corporate network
- Physical destruction
- Stepping stone in the door
- New certification:
  
  Global Industrial Cyber Security Professional (GICSP)
  
  [http://www.giac.org/info/145227](http://www.giac.org/info/145227)
$7.2 million

The average cost of a data breach in 2012 for a company

{or $214 per breached record.}

-Datacastle
AGENDA

• Security Trends in 2014
  ➢ Defining vulnerability, risk and threat
• A Layered approach to Security – defense in depth
• Identifying Vulnerabilities and related controls
• Questions and Discussion
DEFINITIONS

• Vulnerability – a weakness in the environment that could be exploited

• Threat – Any event that can cause an undesirable outcome.

\[
\text{Risk} = \text{Threat} \times \text{Vulnerability}
\]
RISK RELATED QUESTIONS

• What could happen (what is the threat)?
• If it happened, how bad could it be (impact of the threat)?
• How often could it happen (frequency annualized)?
• How reliable are the answers to the above questions (recognition of uncertainty)?
PRIORITIZING RISK

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Consequences</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Minor</td>
<td>Moderate</td>
<td>Major</td>
</tr>
<tr>
<td>Probable A</td>
<td></td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>Possible B</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Improbable C</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Key**
- **Green**: Low Risk
- **Yellow**: Medium Risk
- **Red**: High Risk

How much financial loss you are willing to accept from a single event?
AGENDA

• Security Trends in 2014
• Defining vulnerability, risk and threat
  ➢ A Layered approach to Security – defense in depth
• Identifying Vulnerabilities and related controls
• Questions and Discussion
LAYERED APPROACH – DEFENSE IN DEPTH

Not a New Concept
LAYERED APPROACH – DEFENSE IN DEPTH

The Human Factor
LAYERED NETWORK ARCHITECTURE

1. DMZ
   - WWW
   - Application Proxy

2. Middleware
   - Servers
   - Database

3. Private
   - Internet
   - Router

Internet

Router

Firewall

Application Proxy
ITS NOT JUST ABOUT WHO YOU ARE KEEPING OUT
BUT WHETHER THE RIGHT DATA IS LEAVING YOUR NETWORK

DLP – Data Loss Prevention
Exfiltration – data moving from within an environment out the perimeter and back to an attacker.

Prevention is IDEAL, but detection is a MUST. However detection without response has minimal value.
AGENDA

• Security Trends in 2014
• Defining vulnerability, risk and threat
• A Layered approach to Security – defense in depth
  ➢ Identifying Vulnerabilities and related controls
• Questions and Discussion
STRUCTURED METHODOLOGY FOR ATTACK

• Reconnaissance and discovery
• Fingerprinting and mapping the environment
• Identification of vulnerable components
• Planning your way in based on vulnerabilities.
• Penetrating the target – trial and error
• Gaining control (malware, rootkits, etc.)
SECURITY TOOLS

Network Vulnerability Tools

• OpenVAS
• Commercial Tools (Nessus, Qualys, Nexpose, etc.)

Port Scanning and Packet Crafting Tools

• Nmap/Zenmap
• Hping3

Host scanning

• Center for Internet Security Benchmarks
• Bastille

Web App Scanning Tools

• Nikto
• WebInspect
SECURITY TOOLS (CONT’D)

Penetration Testing and Exploitation Tools

- Metasploit
- CORE Impact

Pre-built toolkits – contain all of the above (LiveCD)

- Backtrack
- Kali (new replacement for Backtrack)

Internet Research for Public Information

- Google
- Hoovers
- LinkedIn
- Facebook
- Whois
- Arin
- Robots.txt (i.e. www.google.com/robots.txt)
INTRANET PCI SCAN

INTRANET WEB APP SCAN

Critical
High
Medium
Low
Info / None
# NETWORK SCAN EXECUTIVE SUMMARY

![Summary Table](image)

<table>
<thead>
<tr>
<th>Severity</th>
<th>Plugin Id</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td></td>
<td></td>
</tr>
<tr>
<td>High</td>
<td>00470</td>
<td>Apache HTTP Server Byte Range DoS</td>
</tr>
<tr>
<td>High</td>
<td>30320</td>
<td>PCI DSS Compliance</td>
</tr>
<tr>
<td>Medium</td>
<td>17744</td>
<td>OpenSSH &lt;= 2.3.0 Allow Top Forwarding Port Bouncing</td>
</tr>
<tr>
<td>Medium</td>
<td>51192</td>
<td>SSL Certificate Cannot Be Trusted</td>
</tr>
<tr>
<td>Medium</td>
<td>68010</td>
<td>CGI Generic Cross-Site Request Forgery Detection (potential)</td>
</tr>
<tr>
<td>Medium</td>
<td>07082</td>
<td>SSL Self-Signed Certificate</td>
</tr>
<tr>
<td>Medium</td>
<td>11714</td>
<td>Nonexistent Page (404) Physical Path Disclosure</td>
</tr>
<tr>
<td>Medium</td>
<td>17704</td>
<td>OpenSSH S/KEY Authentication Account Enumeration</td>
</tr>
<tr>
<td>Medium</td>
<td>33021</td>
<td>.svn/entries Disclosed via Web Server</td>
</tr>
<tr>
<td>Medium</td>
<td>40411</td>
<td>SSL Certificate with Wrong Hostname</td>
</tr>
<tr>
<td>Medium</td>
<td>68030</td>
<td>Web Server Allows Password Autocomplete (PCI-DSS variant)</td>
</tr>
<tr>
<td>Medium</td>
<td>11213</td>
<td>HTTP TRACE/TRACK Methods Allowed</td>
</tr>
<tr>
<td>Medium</td>
<td>11904</td>
<td>SGDynamo sgdynamo.exe HTNAME Parameter Path Disclosure</td>
</tr>
<tr>
<td>Medium</td>
<td>17705</td>
<td>OPIE w/ OpenSSH Account Enumeration</td>
</tr>
<tr>
<td>Medium</td>
<td>42573</td>
<td>SSL Medium Strength Cipher Suites Supported</td>
</tr>
<tr>
<td>Medium</td>
<td>07792</td>
<td>Apache HTTP Server httpOnly Cookie Information Disclosure</td>
</tr>
<tr>
<td>Medium</td>
<td>17703</td>
<td>OpenSSH &lt; 5.9 Multiple DoS</td>
</tr>
<tr>
<td>Medium</td>
<td>68200</td>
<td>PCI DSS compliance: Insecure Communication Has Been Detected</td>
</tr>
<tr>
<td>Low</td>
<td>20194</td>
<td>Web Server Uses Plain Text Authentication Forms</td>
</tr>
<tr>
<td>Low</td>
<td>42980</td>
<td>SSL / TLS Renegotiation Handshakes MITM Plain Text Data Injection</td>
</tr>
<tr>
<td>Low</td>
<td>59491</td>
<td>SSL / TLS Renegotiation DoS</td>
</tr>
<tr>
<td>Low</td>
<td>53841</td>
<td>Portable OpenSSH ssh-keysign ssh-remote-helper Utility File Descriptor Leak Local Information Disclosure</td>
</tr>
<tr>
<td>Low</td>
<td>47830</td>
<td>CGI Generic Injectable Parameter</td>
</tr>
<tr>
<td>Info</td>
<td>10107</td>
<td>HTTP Server Type and Version</td>
</tr>
</tbody>
</table>
## NETWORK SCAN DETAIL SUMMARY

### Results Details

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
</table>

### Synopsis

Nessus has determined that this host is NOT COMPLIANT with the PCI DSS requirements.

### Description

The remote web server is vulnerable to cross-site scripting (XSS) attacks, implements old SSL2.0 cryptography, runs obsolete software, or is affected by dangerous vulnerabilities (CVSS base score >= 4).

### See Also

- [http://www.pcisecuritystandards.org/](http://www.pcisecuritystandards.org/)
HP WEBINSPECT SUMMARY

Vulnerabilities By Threat Class (Top 12)

- Information Leakage: 114
- Insufficient Authentication: 6
- Predictable Resource Location: 3
- Cross-site Scripting: 1
- Insufficient Authorization: 1

Vulnerability By Severity

- Critical: 1
- High: 1
- Medium: 29
- Low: 101
- Informational: 34
- Best Practice: 6

Session Extensions (Top 12)

- ASPX: 65
- JS: 53
- CSS: 42
- HTML: 15
- TTF: 3
- AXD: 3
- TXT: 2
- .woff: 1
- SCHEMA: 1
- HTM: 1

Site Structure

- Comments: 280
- Cookies: 25
- Emails: 82
- Forms: 78
- Scripts: 87

www.hp.com/go/webinspect
Interesting Physical Security Finds
STOPPED AT THE DOOR (NO BADGE)

Unwelcome Visitor
“I NEVER THOUGHT I’D THANK THE PERSON WHO BROKE INTO MY COMPANY”

Interior Lockset on exterior door
PHYSICAL SECURITY – PROPERTY

Exposed cables in cable tray under outdoor walkway
AGENDA

• Security Trends in 2014
• Defining vulnerability, risk and threat
• A Layered approach to Security – defense in depth
• Identifying Vulnerabilities and related controls

Questions and Discussion
THANK YOU