Background

- HSBC
- DOD
- VA
- Masters in Computer Science
- Somerset Recon

- Avid CTF Competitor
Information Security Risks

HACKED
By:
ANONYMOUS
Health insurer Anthem hit by hackers, up to 80 million records exposed

The second largest health insurer in the US has been the victim of what could be the largest data breach in the healthcare sector to date.
Information Security Risks

Ukraine Blackout
Pentest Methodology/Process

- Pre-Engagement
  - NDA, Rules of Engagement, Contract, Documentation
- Information Gathering and Reconnaissance
- Enumeration
- Vulnerability Analysis
- Exploitation
- Post Exploitation
- Reporting
- Retest
Why Pentest?

- **Mitigate Risk**
- **Legal and Compliance**
  - PCI-DSS
  - HIPPA
  - GLBA
  - FISMA/NIST
- **Validate/Invalidate Security Controls**
- **Find and Mitigate Vulnerabilities**
- **Prevent compromise**
- **Make it more difficult for hackers**
Types of Pentests

- Whitebox
- Greybox
- Blackbox

- Internal Assessment
- External Assessment
Types of Pentests

- Network
- Web
- Mobile
- Device
- Wireless
- Red Team
Types of Pentests

- Nework

Diagram showing a network with Internet, Router, Firewall, External Assessment, and Internal Assessment.
Types of Pentests

- Network (Information Gathering)
Types of Pentests

- Network (Enumeration)

```plaintext
Starting Nmap 5.00 ( http://nmap.org ) at 2012-11-19 17:51 IST
Interesting ports on 192.168.1.1:
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Interesting ports on 192.168.1.2:
Not shown: 997 closed ports
PORT   STATE SERVICE
23/tcp open  telnet
53/tcp open  domain
80/tcp open  http

Nmap done: 2 IP addresses (2 hosts up) scanned in 0.51 seconds
```
Types of Pentests

- **Network (Vulnerability Analysis)**
Types of Pentests

- **Nework (Exploitation)**

```
RHOST => 192.168.40.132
PAYLOAD => windows/shell/bind_tcp
[*] Started bind handler
[*] Automatically detecting the target...
[*] Fingerprint: Windows 2003 - Service Pack 1 - lang:Unknown
[*] We could not detect the language pack, defaulting to English
[*] Selected Target: Windows 2003 SP1 English (NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (240 bytes) to 192.168.40.132
[*] Command shell session 1 opened (192.168.40.129:48910 -> 192.168.40.132:4444)

Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.
C:\WINDOWS\system32>
```
Types of Pentests

- Network (Post Exploitation)
Types of Pentests

Web (Information Gathering)
Types of Pentests

- **Web (Enumeration/Vulnerability Analysis)**
  - https://victim.com/?id=yoyo
  - https://victim.com/?id=yoyo><a
  - https://victim.com/?id='
  - https://victim.com/?id='%2b'
  - https://victim.com/?id='--
Types of Pentests

- Web (Enumeration/Vulnerability Analysis)
Types of Pentests

- Web (Exploitation)
Types of Pentests

❖ Mobile (Information Gathering)
Types of Pentests

- **Mobile** (Enumeration/Vulnerability Analysis)

---

A screenshot showing a terminal command and output. The command appears to be related to handling PKCS12 files, possibly for decrypting or examining certificates. The terminal output shows a series of hexadecimal values and strings, which are typical of cryptographic operations. The text around the screenshot is not clearly visible due to the overlay of images and text.
Types of Pentests

- Mobile (Exploitation)
Types of Pentests

- Device (Information Gathering)
Types of Pentests

- Device (Enumeration/Vulnerability Analysis)
Types of Pentests

- Device (Exploitation)

```bash
$ curl -k -X POST --data-binary @malicious_audio_file -H "Content-Type: audio/l16; rate=16000" "https://puppeteer.toytalk.com/v3/conversation/00000000000000000000?key=8d46bd11-1f20-4e2d-bae4-db64b4532edc&account=00000000000000000000"
```
Red Team (Information Gathering)
Types of Pentests

- **Read Team (Exploitation)**
Types of Pentests

- Read Team (Post Exploitation)
Types of Pentests

- Wireless

```bash
[02:34:54] Tested 627489 keys (got 55118 IVs)

<table>
<thead>
<tr>
<th>KB</th>
<th>depth</th>
<th>byte(vote)</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>0/1</td>
<td>FC(78080)</td>
</tr>
<tr>
<td>1</td>
<td>0/1</td>
<td>81(72960)</td>
</tr>
<tr>
<td>2</td>
<td>0/2</td>
<td>A2(66560)</td>
</tr>
<tr>
<td>3</td>
<td>0/1</td>
<td>C8(79616)</td>
</tr>
<tr>
<td>4</td>
<td>0/2</td>
<td>9B(65280)</td>
</tr>
<tr>
<td>5</td>
<td>0/1</td>
<td>B3(76288)</td>
</tr>
<tr>
<td>6</td>
<td>0/1</td>
<td>2E(72192)</td>
</tr>
<tr>
<td>7</td>
<td>0/1</td>
<td>1A(72784)</td>
</tr>
<tr>
<td>8</td>
<td>0/2</td>
<td>4A(68352)</td>
</tr>
<tr>
<td>9</td>
<td>0/1</td>
<td>14(68688)</td>
</tr>
<tr>
<td>10</td>
<td>0/1</td>
<td>58(67328)</td>
</tr>
<tr>
<td>11</td>
<td>1/1</td>
<td>16(66048)</td>
</tr>
<tr>
<td>12</td>
<td>1/2</td>
<td>AE(64444)</td>
</tr>
</tbody>
</table>

KEY FOUND! [ FC:81:A2:C8:9B:B3:2E:1A:00:14:C9:8F:AA ]
Decrypted correctly: 100%
```

(root@debian:koosha)
## Types of Pentests

- **Wireless**

<table>
<thead>
<tr>
<th>Opcode_AttHandle</th>
<th>AttValue</th>
<th>CRC</th>
<th>RSSI (dBm)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x52 0x0012</td>
<td>FF FF FF FF FF FF FF FF FF FF FF FF 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A</td>
<td>0x846ECF</td>
<td>-55</td>
</tr>
<tr>
<td>0x52 0x0012</td>
<td>02 01 11 02 BE 00 00 4A 2C 3A 57 BC 08 55 4C 34 40 E2 01 00</td>
<td>0xFF0751</td>
<td>-56</td>
</tr>
<tr>
<td>0x52 0x0012</td>
<td>02 02 04 06 FE 01 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00</td>
<td>0x207A9E</td>
<td>-63</td>
</tr>
</tbody>
</table>

```
188
189
fff5a5a5a5a5a5a5a5a5a5a5a5a5a5a5a5a84f7652b8d
190 PASSWORD: 123456
```
What are the most common passwords?
What are the most common passwords?

- 123456
- password
- 12345678
- qwerty
- 12345
- 123456789
Pentest Tips and Tricks

- Antivirus Bypass
- IDS/IPS/WAF Bypass
- NAC/WiFi/Proxy
Pentest Tips and Tricks

- **Automation**
  - Nessus
  - Nexpose
  - Web Inspect
  - IBM Appscan
  - NTO Spider
  - Acunetix
  - Burp Suite Pro
Pentest Tips and Tricks

- Manual Pentest
- Automated Scan
- Try not to burn yourself with the soldering iron
Pentest Tips and Tricks

- Client-Side Exploitation
- Scope Social Engineering
- Screenshots
  - Take them immediately
- Be careful when performing authenticated attacks or scans
- Eliminate false positives
- Document mitigations
Pentest Tips and Tricks

Social Engineering

- Nobody can resist pizza
- Emergency
- Helpdesk
- Leveraging relationships
- CallerID Spoofing
- Spring Break 2016
Pentest Tips and Tricks

- **Reporting**
  - Vulnerability description
  - Vulnerability risk ratings
  - Steps to reproduce
  - Screenshots
  - Impact
  - Mitigations
Making Hackers Lives More Difficult

- Updated Software
- Segregated Networks (VLANS/Firewall rules)
- Hardened OS configurations
- Microsoft Enhanced Mitigation Experience Toolkit (EMET)
- Secure Software Development Lifecycles
- Browser Hardening (NoScript, Scriptno, Adblock Plus, Java and flash are uninstalled)
- Application Whitelisting
- Firmware/chip protections
- Hardware debugging is disabled
Get More Value Out Of Pentest

- **Give more information to the testers**
  - Network diagrams
  - External and internal network access
  - 2 of every types of account
  - Directory listings
  - Sourcecode
  - Web services documentation
  - Development build of mobile application and production build

- **Look for signs of highly skilled testers**
  - Nessus or Nexpose is not the only tool in their arsenal
  - Manual testing
  - Testers have additional skills/experience (exploit development, reverse engineering, software development, network, systems administration, virtualization, wireless protocols, software defined radio, CTF, etc.)
Get More Value Out Of Pentest

- **Pentest on non production systems**
  - Development
  - QA
  - Pre-production

- **Provide technical assistance to testers if needed**
  - System goes down
  - Account gets locked out or expires
  - Answer questions (e.g. Should user X be able to get to data Y? Is anyone using this service?)
  - Embedded device fails
Get More Value Out Of Pentest

❖ How much do pentests cost?
  ▪ $125-$400 per hour per tester

❖ Typical engagements
  ▪ Web: 4-6 days
  ▪ Network: 4-10 days
  ▪ Mobile: 5-10 days
  ▪ Device/IoT: 7-15
  ▪ Red Team: 4-10

❖ Be careful of vulnerability scans that charge by IP address
Questions???