Keeping Your Service Secure – Are You Doing Your Diligence?

ccNSO Meeting – ICANN51 - October 14, 2014
Merike Kaeo, CISO
Topics For Today

Trends in Attacks
Exploitation and Impacts
Community Responsibility
What You Can Do
Evolution of Attack Landscape

- Email propagation of malicious code
- "Stealth"/advanced scanning techniques
- Widespread attacks using NNTP to distribute attack
- Widespread attacks on DNS infrastructure
- Executable code attacks (against browsers)
- Automated widespread attacks
- GUI intruder tools
- Hijacking sessions
- Internet social engineering attacks
- Packet spoofing
- Automated probes/scans
- Widespread denial-of-service attacks
- Techniques to analyze code for vulnerabilities without source code
- DDoS attacks
- Increase in worms
- Sophisticated command & control
- Anti-forensic techniques
- Home users targeted
- Distributed attack tools
- Increase in wide-scale Trojan horse distribution
- Windows-based remote controllable Trojans (Back Orifice)

Intruder Knowledge

1990

ccNSO Meeting ICANN51
Credential Leakage is a Big Problem

Most often thru re-use of usernames and passwords
- How many registrants use usernames and passwords that they also use for their social media access?

Uncontrolled processes where new passwords are sent in cleartext emails to users
- This happens more often than you’d think

Exploiting vulnerabilities to get unauthorized access to systems where password files may be stored
Critical Vulnerabilities (last 6 months)

SSL/TLS
- Heartbleed followed by more bugs in June
- Be on lookout for more vulnerabilities

Scripts and Shells
- Bash shell issues [Shellshock] still need attention
- Resource for Proof of Concepts and Potential Targets
  https://github.com/mubix/shellshocker-pocs
Keeping Up With Vulnerabilities

Know Your Operating Systems and Application Versions
  - For TLS/SSL can use publicly available tests
    - https://www.ssllabs.com/ssltest/
Get On Mailing Lists For Vendor Security Announcements
Subscribe to National CERT Alert Lists
  - https://www.us-cert.gov/ncas/alerts/
Follow Security Industry Blogs
  - http://ccnso.icann.org/resources/cybercrime-resources.htm
## Determine Likelihood of Risk

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Definition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>Unlikely</td>
<td>Working tools or exploits are not readily available. Exploitation requires in-depth knowledge of the system and/or may require strong programming skills. User (or perhaps higher privilege) level access may be one of a number of pre-conditions.</td>
</tr>
<tr>
<td>Medium</td>
<td>Likely</td>
<td>Tools and exploits are available but need to be modified to work successfully. Exploitation requires basic knowledge of the system and may require some programming skills. User level access may be a pre-condition.</td>
</tr>
<tr>
<td>High</td>
<td>Certain</td>
<td>Tools and exploits are readily available on the Internet or other locations. Exploitation requires no specialized knowledge of the system and little or no programming skills. Anonymous users can exploit the issue.</td>
</tr>
</tbody>
</table>
## Assess Impact of Successful Exploitation

<table>
<thead>
<tr>
<th>Impact</th>
<th>Definition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Low</strong></td>
<td>Negligible</td>
<td>The risk will not substantively impede the achievement of business objectives, causing minimal damage to the organization’s reputation.</td>
</tr>
<tr>
<td><strong>Medium</strong></td>
<td>Moderate</td>
<td>The risk will cause some business objectives to be delayed or not be achieved, causing potential damage to the organization’s reputation. User level access with no disclosure of sensitive information.</td>
</tr>
<tr>
<td><strong>High</strong></td>
<td>Critical</td>
<td>The risk will cause damage to systems and the organization’s reputation. Administrator level access (for arbitrary code execution through privilege escalation for instance) or disclosure of sensitive information.</td>
</tr>
</tbody>
</table>
Review Credential Lifecycle Management

Creation
- Utilize password cracking tools to check strength of passwords
  - https://www.thc.org/thc-hydra/

Distribution
- Look to use cryptographical means for integrity and confidentiality

Storing
- Ensure credentials never stored in publicly accessible systems
- All credentials should be stored using cryptographic protections
- Pass The Hash Attacks
Review Credential Lifecycle Management

Renewal
- Tradeoff between too frequent vs how long a potential credential compromise can go undetected and cause harm

Revocation
- Remember to create a revocation certificate at the time when certificate created.

Recovery
- Scenarios where employee leaves company or forget password
What Are Basic Things Everyone Can Do

Control Physical and Logical Access to your Critical Servers
Credential Management
  - Don’t share credentials across systems
  - Look at entire lifecycle of how you handle credentials
    (creation, distribution, storing, renewal, revocation, recovery)
  - Test password strength
  - Encourage 2-factor authentication

Keep track of operating systems and application versions and apply security patches as they become available