BREAKING AND ENTERING: HOW AND WHY DHS CONDUCTS PENETRATION TESTS

Robert Karas
National Cybersecurity Assessments and Technical Services (NCATS)
NCCIC | National Cybersecurity and Communications Integration Center

Penetration Tests

- Act as Adversary
- Common Paths to Success
  - Phishing – Click rate 12%
  - Credentials
    - Default
    - Re-Used
<table>
<thead>
<tr>
<th>Issue</th>
<th>Impact</th>
<th>Mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stakeholder believed they had 800 hosts, scan revealed over Flat</td>
<td>Flat network, person in region 1 can access all region 8</td>
<td>Segment network with router or firewall</td>
</tr>
<tr>
<td>discovered over 200 security cameras accessible with default</td>
<td>Physical security, theft, watching key strokes of users</td>
<td>Change default credentials and add network filters</td>
</tr>
<tr>
<td>credentials</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SQL Injection - successfully crafted and input a data string</td>
<td>Unauthorized user access was achieved from the</td>
<td>Sanitize all input provided by an untrusted</td>
</tr>
<tr>
<td>enumerated web application usernames and passwords, credentials to</td>
<td></td>
<td>Implement server-side controls of white-listed character sets. Encrypt data</td>
</tr>
<tr>
<td>log into web application and other devices</td>
<td></td>
<td>stored on the</td>
</tr>
<tr>
<td>Discovered WAP buried underneath paper/trash/debris and into the</td>
<td>Security controls implemented to connected to the bypassed. Anyone at</td>
<td>Monitor network for rogue devices, conduct walk-throughs to identify rogue</td>
</tr>
<tr>
<td>Local Area Network</td>
<td></td>
<td>devices</td>
</tr>
<tr>
<td>Phishing email sent to a limited number of employees. One forward to</td>
<td>All machines were potentially compromised or had to clean. IT resources</td>
<td>Train users to identify malicious email, technical controls.</td>
</tr>
<tr>
<td>the entire agency</td>
<td></td>
<td>allocated to mitigation and clean</td>
</tr>
<tr>
<td>Password reset function allowed the reset password to be any email</td>
<td>Anyone could reset an account and log into the</td>
<td>Ensure passwords can only be reset by the account owner and sent to the</td>
</tr>
<tr>
<td>address</td>
<td>This logic flaw impacted Confidentiality, Availability, Integrity</td>
<td>email address record for the account owner</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
What Happens Next?

<Initial Attack Vector> 
Local Account Hash Dump
Pivot to user computers

DHS
Domain Controller is accessed
DHS User Domain admin created

User
User
User
Admin

Domain Controller
SQL Server
Network Appliance
SQL QA
Why DHS offers these services

- Make informed, risk-based decisions
- Eliminate remote attack paths
- Promote data-driven decisions
#RSAC

## CYBER.DHS.GOV

**15-01 Critical Vulnerability Mitigation**

- 16-01- Security High Value Assets
- 16-01 - Threat to Network Infrastructure Devices
- 16-03 – 2016 Agency Cybersecurity Reporting Requirements
- 17-01 – Removal of Kaspersky Products

**18-01 – Enhance Email and Web Security**

## SERVICES

- Vulnerability Scanning
- Incident Response
- Automated Indicator Sharing
- Architecture Review
- Hunt
- Self Assessments
- Risk and Vulnerability Assessments
Questions?

NCATS_INFO@HQ.DHS.GOV