Background

• Christian Espinosa | christian.espinosa@alpinesecurity.com
• Entrepreneur, Penetration Tester, Security Researcher, Incident Response, Survival Instructor for Bear Grylls
• Ed: BSGE, MBA
• Certs: CISSP, CCSP, CISA, CRISC, CPT, CSSA, CEPT, CEH, CREA, ECI, LPT
• Patents:
• Interests:
  • Ironman Triathlon, Mountaineering, Travel, Security, Things that Involve a Waiver
What is Decoding the Hack?
Objectives

• Improve awareness
• Understand the “state of affairs”
• Learn intelligence gathering methods
• Learn common hacking tactics, given several scenarios
Expectations

• General sample of hacking techniques – not inclusive
• Not a “right” way to do something
• May skip steps
• Ask questions any time
• Demos may have issues – like to run in realistic environment – some issues intentional
• You need written permission to perform penetration testing
• Balance of technical presentation
• Demo centric
Overview

• Context - Are we Winning?
• Hacking Methodology Overview
• Scenario 1 – Physical Access Attacks
• Scenario 2 – Client-Side Attacks
• Scenario 3 – Server-Side Attacks
Are We Winning?
Unfortunate Facts

• Most compromises are based on known problems that have known solutions
• 85+% of incidents managed by the US-CERT come down to the same 5 basic defenses
• Most attacks *should* have been blocked at the perimeter
• Very few attackers use “stealth” techniques
• Very few defenders have automated workflow
Time from Earliest Evidence of Compromise to Discovery of Compromise

205

median number of days that threat groups were present on a victim’s network before detection

↓ 24 days less than 2013

Longest Presence: 2,982 days

Source: Mandiant M-Trends 2015
How Compromises Are Being Detected

31% victims discovered the breach internally

69% victims notified by an external entity

Source: Mandiant M-Trends 2015
99.9% OF THE EXPLOITED VULNERABILITIES WERE COMPROMISED MORE THAN A YEAR AFTER THE CVE WAS PUBLISHED.
23% OF RECIPIENTS NOW OPEN PHISHING MESSAGES AND 11% CLICK ON ATTACHMENTS.

It Only Takes One
How Compromises Are Being Detected

53%

External Notification of Breach

47%

Internal Discovery of Breach

Median Time of Compromise to Discovery

<table>
<thead>
<tr>
<th>All Mandiant Investigations in 2015</th>
<th>External Notification</th>
<th>Internal Discovery</th>
</tr>
</thead>
<tbody>
<tr>
<td>146 days</td>
<td>320 days</td>
<td>56 days</td>
</tr>
</tbody>
</table>

Source: Mandiant M-Trends 2015
Threat Actions

Source: Verizon 2015 DBIR
Which should we do first?

Penetration Test

vs

Asset Inventory
Which should we do first?

(20) Penetration Test

vs

(1) Asset Inventory
Foundational Cyber Hygiene (FCH)

Prevents/stops 85-90% attacks...

- CSC 1: Inventory of Authorized and Unauthorized Devices
- CSC 2: Inventory of Authorized and Unauthorized Software
- CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
- CSC 4: Continuous Vulnerability Assessment and Remediation
- CSC 5: Controlled Use of Administrator Privileges
Know authorized & unauthorized devices
Know authorized & unauthorized software

You can’t defend what you don’t know
Methodology
Hacking Methodology | KISS

• Reconnaissance
  • Passive
  • Active
• Vulnerability Identification
• Initial Exploitation
• Expand Foothold
• Persistence

Objective Dependent
Overall Method - ORVE

• **Objective** – what are you trying to achieve? Who is the target?
  • Havoc, Chaos
  • DOS
  • Steal PII, Steal PHI
  • Hacktivism
  • Steal Credentials
  • Etc.

• **Recon**
  • Passive and Active
  • Supports Objective

• **Vulnerability ID**
  • Did our Recon yield a Vuln?
  • Prioritization of Vulns, based on Objective and likely success rate

• **Exploit**
  • Objective Dependent
Passive Recon - Whois

- Whois is a protocol used for querying databases that store registration information for Internet resources:
  - Domain names
  - IP Addresses
  - Etc.
- DNS

Registry Tech ID:
Tech Name: Blaine Word
Tech Organization: Ameren Services
Tech Street: 1901 Chouteau Ave, MC 280
Tech City: St. Louis,
Tech State/Province: MO
Tech Postal Code: 63103-3003
Tech Country: US
Tech Phone: +1.3145542230
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: bword@ameren.com
### Passive Recon - Google Hacking

<table>
<thead>
<tr>
<th>Operator</th>
<th>Purpose</th>
<th>Mixes with Other Operators?</th>
<th>Can be used Alone?</th>
<th>Web</th>
<th>Images</th>
<th>Groups</th>
<th>News</th>
</tr>
</thead>
<tbody>
<tr>
<td>intitle</td>
<td>Search page Title</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>allintitle</td>
<td>Search page title</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>inurl</td>
<td>Search URL</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
<td>not really</td>
</tr>
<tr>
<td>allinurl</td>
<td>Search URL</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>like intitle</td>
</tr>
<tr>
<td>filetype</td>
<td>specific files</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
<td>not really</td>
</tr>
<tr>
<td>allintext</td>
<td>Search text of page only</td>
<td>not really</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>site</td>
<td>Search specific site</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>not really</td>
</tr>
<tr>
<td>link</td>
<td>Search for links to pages</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>not really</td>
</tr>
<tr>
<td>inanchor</td>
<td>Search link anchor text</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
<td>not really</td>
</tr>
<tr>
<td>numrange</td>
<td>Locate number</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>not really</td>
</tr>
<tr>
<td>daterange</td>
<td>Search in date range</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
<td>not really</td>
<td>not really</td>
<td>not really</td>
</tr>
<tr>
<td>author</td>
<td>Group author search</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>not really</td>
</tr>
<tr>
<td>group</td>
<td>Group name search</td>
<td>not really</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>not really</td>
</tr>
<tr>
<td>insubject</td>
<td>Group subject search</td>
<td>yes</td>
<td>yes</td>
<td>like intitle</td>
<td>like intitle</td>
<td>yes</td>
<td>like intitle</td>
</tr>
<tr>
<td>msgid</td>
<td>Group msgid search</td>
<td>no</td>
<td>yes</td>
<td>not really</td>
<td>not really</td>
<td>yes</td>
<td>not really</td>
</tr>
</tbody>
</table>
Google Hacking Example

Google search query:

```
site:.mil filetype:pdf "secret"
```

Search results include:

- **SECRET**
  - https://www2.centcom.mil/.../EX%206...
  - United States Central Command

- **TOP SECRET - U.S. Coast Guard**
  - United States Coast Guard
  - U.S. DEPARTMENT OF HOMELAND SECURITY. U.S. COAST GUARD. C G - 4784A (R ev. 6-04). TOP SECRET DISCLOSURE RECORD. UNIT.

- **The Secret of Future Victories - US Army Combined Arms**
  - usacac.army.mil/.../06_92_SecretFutureVictories_Feb... United States Army
  - by IDA Log - 1992 - Related articles
  - Copy. S of 320 copies. AD--A250 718. IDA PAPER P-265 3. THE SECRET OF FUTURE VICTORIES. Paul F. Gormian. General, USA (Retired). DTIC. 05M.

- **THE ARMY SECURITY CLEARANCE: MYTH BUSTER**
  - www.ftmeade.army.mil/.../myth_busterv2.pdf
  - Fort George G. Meade
  - 3 Clearance Levels: Confidential, Secret and Top Secret -- Background Investigation: Evaluates a person's background to determine if they are eligible to hold a...

- **ISL 2014-01 - DSS**
  - www.dss.mil/.../ISL%202014-01%20-%20GSA...
  - Defense Security Service
  - Apr 14, 2014 - General Services Administration (GSA) Carriers for Overnight Delivery of SECRET and CONFIDENTIAL Classified Information. ISL 2006-02...
Google Hacking Database (GHDB)

Search the Google Hacking Database or browse GHDB categories

<table>
<thead>
<tr>
<th>Date</th>
<th>Title</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015-10-16</td>
<td>mail spool intitle:index.of</td>
<td>Sensitive Directories</td>
</tr>
<tr>
<td>2015-10-16</td>
<td>private parent intitle:index.of</td>
<td>Sensitive Directories</td>
</tr>
<tr>
<td>2015-10-16</td>
<td>inurl:users intitle:index.of</td>
<td>Sensitive Directories</td>
</tr>
<tr>
<td>2015-10-16</td>
<td>inurl:/my.logon.php3?</td>
<td>Pages containing login portals</td>
</tr>
<tr>
<td>2015-10-15</td>
<td>inurl:webvisu.htm ext:htm</td>
<td>Various Online Devices</td>
</tr>
</tbody>
</table>
Active Recon Scanning with Nmap

- Nmap – standard for open source scanning tool
Active Recon – Burp Suite

**Contents**

<table>
<thead>
<tr>
<th>Host</th>
<th>Method</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://10.1.1.19">http://10.1.1.19</a></td>
<td>GET</td>
<td>/</td>
</tr>
<tr>
<td><a href="http://10.1.1.19">http://10.1.1.19</a></td>
<td>GET</td>
<td>/all.php</td>
</tr>
<tr>
<td><a href="http://10.1.1.19">http://10.1.1.19</a></td>
<td>GET</td>
<td>/cat.php</td>
</tr>
</tbody>
</table>

**Issues**

- Cross-site scripting (reflected)
- SQL injection
- Unencrypted communications
- Cookie without HttpOnly flag set
- Path-relative style sheet import
- Frameable response (potential Clickjacking)

**Cross-site scripting (reflected)**

**Issue:** Cross-site scripting (reflected)

**Severity:** High

**Confidence:** Certain

**Host:** http://10.1.1.19

**Path:** /cat.php

**Issue detail**

The value of the id request parameter is copied into the HTML document as plain text between tags. The payload `u7x98<script>alert(1)</script>jubha` was submitted in the id parameter. This input was echoed as `u7x98<script>alert(1)</script>jubha` in the application's response.
Scenario->
Physical Access Attack
Physical Access Attack - ORVE

• Objectives
  • Plant a backdoor to use for persistent access
  • Steal credentials and PII

• Recon (Observation)
  • Walk through of facility showed users leave computers unlocked when they walk away from desks
  • Desktop computers are under tables, use USB Keyboards, run Windows 10
  • Users leave desks unattended, desks are located between entry and bathroom
  • Ethernet jacks next to power outlets in entry way and on way to bathroom

• Vulnerability
  • Unlocked systems
  • Unattended computers

• Exploits
  • Use HID on unlocked system for backdoor
  • Use hardware USB key logger to steal credentials and PII
Scenario Use Cases

- Admiral’s Club
- Hotel Kiosk
- Partner Facility
- Office Building
- Retail Store
- Airport
- Etc.
Key Loggers

- Software
- Hardware
HID Exploit Demo Steps

- Generate Script with Payload
- Encode Script
- Save to Micro SD via USB
- Move Micro SD to HID
- Test. Test again.
- Place HID in Target (unlocked computer)
- Let Script Run
- Remove HID
- Objective Complete
Key Logger Demo Steps

• Find a target computer
• Insert key logger
• Come back later to pick it up
• Use key sequence to change key logger into USB
• View keystrokes
Scenario->
Client Side Attack
Client-Side Attack - ORVE

• Objectives
  • Steal user credentials
  • Deliver payload to internal system

• Recon
  • Users can access Facebook and LinkedIn from work (Observation, SE)
  • Determine email address of users (Discover Script)
  • Systems appear to be running Windows 7 and IE 8 (Observation)
  • Users use corporate laptops and free wifi at café during lunch (Observation)

• Vulnerability
  • Win7 / IE 8?
  • Café Wireless

• Exploits
  • Use MITM to confirm Win 7 / IE 8
  • Use Phishing for Delivery
  • (1) Use SET to steal Credentials (Facebook example)
  • (2) Use MS11-003 to deliver payload
Facebook Credential Stealing Demo Steps

• Use SET Credential Harvester to Clone the Facebook Page
• Set up Post back page to listen for stolen credentials
• Start apache2
• Test
• Tail –f /var/www/html/harvester-file
• Use GoPhish to send phishing email (Facebook Tag) to victim – Ivan Drago’s email on Windows 10 machine
Browser Exploit Demo Steps

• Use MITM - Ettercap to Figure out / Confirm User Agent
• Wireshark to capture User Agent
• GoPhish for LinkedIn Invite
• Send to Gordon Alpine’s email account
• Use Metasploit to exploit MS11-003
• Take Over Windows 7 Machine with Meterpreter Reverse Shell or desired payload
Scenario->
Server Side Attack
Server-Side Attack - ORVE

• Objectives
  • Steal PII from target
  • Plant back door on target system

• Recon
  • Web server (nmap)

• Vulnerability
  • SQL Injection (Burp)
  • XSS (Burp)

• Exploits
  • Use SQLi to extract admin password hash
  • Use SQLi to upload shell
  • Use shell to extract information
SQLi Attack Demo Steps

- Nmap against target
- Burp against target
- Manual parameter tampering
- Column # determination with UNION
  - UNION SELECT 1,2,3,.....
- Info Retrieval
  - UNION SELECT 1,(info),3,4
- Retrieve admin password hash
- Crack password
- Login
- Upload shell

```php
<?php
    system($_GET['cmd']);
?>
```
Contact Info

Christian Espinosa
christian.espinosa@alpinesecurity.com
www.alpinesecurity.com