Web Apps
Dripping With Honey

OWASP Denver and Boulder too!!
April 2020

HARSH TRUTH #1
Bypassing defenses is often very easy

HARSH TRUTH #2
INTLEAK IS REAL

SOC Analyst

Company (redacted)

$30,000 - $45,000 a year
ARCSIGHT, SPLUNK, LOGRHYTHM, QRADAR, ANTIVIRUS, FIREWALLS AND SOURCEFIRE AND SIMILAR TOOLS PREFERRED. Company has open positions for...
Desirable proficiencies:

- Experience migrating from Checkpoint to Palo Alto
- Network Access Control (Forescout preferred)
- RADIUS
- F5
- Secure Routing & Switching
- Cisco AnyConnect & Umbrella
Sales folks want sales

It really is this easy!

A 90-day demo! Heck yeah, we can make that happen!
HARSH TRUTH #4

It’s easier than ever to leverage tech on a PoC
Jeff McJunkin to the rescue

Also, BHIS/AC
HARSH TRUTH #5

PoC will be... harsh
SCENE
DELETED
(use your imagination)

Recap:
1. Easy to find your defenses.
2. Easy to get your defenses.
3. Easy to setup an abuse lab.

HARSH TRUTH #6
Defenses we all use are *broken*. But there is another way.

Hi, I’m Mick!

- Managing Partner of InfoSec Innovations
- Teach SANS 504 & 555
- IANS Faculty
- @BetterSafetyNet
What we’re going to cover

• Honeypots are dead easy
• Used appropriately, honeypots can be used with existing infrastructure.
• Attackers trip over honeypots
  • They slow attackers down
  • Make for easier detection
  • Make for quicker detection

GOOD TRUTH #1
Attackers expect “normal”

GOOD TRUTH #2
Attackers are predictable

1. Recon
2. Probing
3. Exploitation
4. Post-Exploitation
GOOD TRUTH #3

Honeypots are dead easy...
Any interaction is suspect

GOOD TRUTH #4
Web architectures are easy to “honey”

“classic” N-tier architecture

Presentation
Application
Data store

Web services

Service
Service
Service

Honeypots are dead easy...
Honeypots confuse

Confuse recon
PortSpoof

How to run portspoof

Sudo portspoof *** get options here
Honeypots misdirect

Misdirect probes
Robots.txt

Honey Robot.txt
User-agent: *
Disallow: /api/
Disallow: /bo/
Disallow: /uploader.jsp
Disallow: /admin/
Disallow: /editor.jsp

Honey Upload
User-agent: *
Disallow: /api/
Disallow: /bo/
Disallow: /uploader.jsp
Disallow: /admin/
Disallow: /editor.jsp

Batch process uploader
Choose File  No file chosen
Strictly for use by REDACTED
Process
Honey User Logon

User-agent: *
Disallow: /api/
Disallow: /bo/
Disallow: /uploader.jsp
Disallow: /admin/
Disallow: /editor.jsp
Sign in

Username or Email Address

Password

Login

DO YOU WANT THREAT INTEL?

BECAUSE THAT'S HOW YOU GET THREAT INTEL
Honeypots are dead easy...

Honeypots lie
Lie to the exploit

Web Services
<xs:element name="actionCSRImpersonateCustomer">
  <annotation>
    <documentation>
      Allow Phone rep (CSR) to become user. Internal use only.
    </documentation>
  </annotation>
</xs:element>

<xs:element name="CBCStreamAuthenticator">
  <annotation>
    <documentation>
      Crypto stream generator. Used for creating user tokens.
    </documentation>
  </annotation>
</xs:element>
Honeypots buy time

Honeypot data
DESCRIBE CC_Info;

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Null</th>
<th>Key</th>
<th>Default</th>
<th>Extra</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cust_ID</td>
<td>int(10) unsigned</td>
<td>NO</td>
<td>PRI</td>
<td>NULL</td>
<td>auto_increment</td>
</tr>
<tr>
<td>CC_Num</td>
<td>varchar(16)</td>
<td>NO</td>
<td>UNI</td>
<td>NULL</td>
<td></td>
</tr>
<tr>
<td>Card_Name</td>
<td>varchar(75)</td>
<td>NO</td>
<td></td>
<td>NULL</td>
<td></td>
</tr>
<tr>
<td>Expires</td>
<td>date</td>
<td>NO</td>
<td></td>
<td>NULL</td>
<td></td>
</tr>
<tr>
<td>CSC</td>
<td>int(3)</td>
<td>NO</td>
<td></td>
<td>NULL</td>
<td></td>
</tr>
<tr>
<td>active_user</td>
<td>tinyint(1) unsigned</td>
<td>NO</td>
<td>MUL</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

DESCRIBE Potential_Explore_Sites;

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Null</th>
<th>Key</th>
<th>Default</th>
<th>Extra</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site_ID</td>
<td>int(10) unsigned</td>
<td>NO</td>
<td>PRI</td>
<td>NULL</td>
<td>auto_increment</td>
</tr>
<tr>
<td>LAT</td>
<td>int(6)</td>
<td>NO</td>
<td>UNI</td>
<td>NULL</td>
<td></td>
</tr>
<tr>
<td>LONG</td>
<td>int(6)</td>
<td>NO</td>
<td></td>
<td>NULL</td>
<td></td>
</tr>
<tr>
<td>Purch_Max</td>
<td>int(9)</td>
<td>NO</td>
<td></td>
<td>NULL</td>
<td></td>
</tr>
<tr>
<td>Purch_Date</td>
<td>date</td>
<td>YES</td>
<td></td>
<td>NULL</td>
<td></td>
</tr>
</tbody>
</table>
Honeypots are dead easy...

You’re already ready!
Shout out to:
Michael Hogue-Rennie
<link rel='stylesheet' id='contentking-stylesheet-css' href='https://www.loggly.com/wp-content/plugins/contentking/assets/css/contentking.css' />
<link rel='stylesheet' id='et_monarch-css-css' href='https://www.loggly.com/wp-content/themes/et_monarch/css/et_monarch.css' />
<link rel='stylesheet' id='loggly-style-css' href='https://www.loggly.com/wp-content/uploads/2016/01/loggly-style.css' />
<link rel='stylesheet' id='tablepress-default-css' href='https://www.loggly.com/wp-content/plugins/tablepress/css/tablepress.css' />
<script type='text/javascript' src='https://www.loggly.com/wp-includes/js/jquery.min.js'></script>
<script type='text/javascript' src='https://www.loggly.com/wp-includes/js/jquery-ui.min.js'></script>

404’s as honeypots!
1. Pictures
2. CSS
3. JavaScript files
4. XML Schemas

RECAP

• Honeypots are dead easy
• Overlay honeypots are best.
• Advantages of honeypots
  • They slow attackers down
  • Make for easier detection
  • Make for quicker detection
Conventional Wisdom isn’t wise

• Have to be a pen tester when I “grow up”
• Have to do all the things before I do “active defense”

Thank you!

• My wife
• SANS
• You!
Oh $&@+!!
I finished too early!
MORE HONEY AWESOME!

Honeypots hurt
Honeypots hurt*
(consult your lawyers)

Honeypot zipbomb
User-agent: *
Disallow: /api/
Disallow: /backups/
Disallow: /uploader.jsp
Disallow: /admin/
Disallow: /editor.jsp

Honeypot PDF
MSFVenom

<xsl:element name="QuoteGeneratorPDF">
  <annotation>
    <documentation>
      Generate Quote PDF. If no quote ID is given, send all PDFs associated with current user
    </documentation>
  </annotation>
</xsl:element>