SHODAN for Penetration Testers

- What is SHODAN?
- Basic Operations
- Penetration Testing
- Case Study 1: Cisco Devices
- Case Study 2: Default Passwords
- Case Study 3: Infrastructure Exploitation
- Other Examples
- The Future
- Conclusions
By pen testing, I mean…

- Black/gray/white box testing
- Ethical hacking
- Security auditing
- Vulnerability assessment
- Standards compliance
- Training
- All of the above
WHAT IS SHODAN?
What is SHODAN? (1)

- SHODAN (http://www.shodanhq.com/) is a computer search engine designed by web developer John Matherly (http://twitter.com/achillean)
- While SHODAN is a search engine, it is much different than content search engines like Google, Yahoo or Bing
What is SHODAN? (2)

- Typical search engines crawl for data on web pages and then index it for searching.
- SHODAN interrogates ports and grabs the resulting banners, then indexes the banners (rather than the web content) for searching.
What is SHODAN? (3)

- Rather than to locate specific content on a particular search term, SHODAN is designed to help the user find specific nodes (desktops, servers, routers, switches, etc.) with specific content in their banners.

- Optimizing search results requires some basic knowledge of banners.
SHODAN for Penetration Testers

BASIC OPERATIONS
Welcome to SHODAN, the first computer search engine

» Search the internet for servers, routers and more
» Find computers running certain software (HTTP, FTP, etc.)
» Filter hosts based on geographic location

» Learn more

Popular Searches 📰

cisco-ios last-modified
Finds Cisco-IOS results that do not require any authentication ;)

default password
Finds results with "default password" in the banner; the named defaults might work!

FTP anon successful
This search does not provide as many results as the other ftp search, but it looks like all the results that come back are successful anonymous logins

IIS 4.0 webservers
Almost all false positives removed by excluding other versions and http error codes

Contact

FOLLOW ME ON TWITTER

For direct inquiries:

jmatt@surtri.com

Presentations
SHODAN Search Provider Firefox Add-on

SHODAN Helper Firefox Add-on

SHODAN Computer Search Engine

Query

Country

Service

Hostname (full or partial)

Search

Popular Searches

cisco-ios last-modified
Finds Cisco-IOS results that do not require any authentication ;)

default password
Finds results with "default password" in the banner; the named defaults might work!

FTP anon successful
This search does not provide as many results as the other ftp search, but it looks like all the results that come back are successful anonymous logins

IIS 4.0 webservers
Basic Operations: Search

- Search terms are entered into a text box (seen below)
- Quotation marks can narrow a search
- Boolean operators + and – can be used to include and exclude query terms (+ is implicit default)
Basic Operations: Login

- Create and login using a SHODAN account; or
- Login using one of several other options (Google, Twitter, Yahoo, AOL, Facebook, OpenID)
- Login is *not* required, but *country* and *net* filters are not available unless you login
- Export requires you to be logged in
Login or Sign Up

Sign in using your account with

- Google
- Twitter
- Yahoo!
- AOL
- Facebook
- OpenID

Powered by RPX

Login using a SHODAN account

Username

Password

OR

Login

Don't have an account? Sign Up Now

Forgot your password? Reset your password now
Basic Operations: Filters

- **country**: filters results by two letter country code
- **hostname**: filters results by specified text in the hostname or domain
- **net**: filter results by a specific IP range or subnet
- **os**: search for specific operating systems
- **port**: narrow the search for specific services
Welcome to SHODAN, the first computer search engine

» Search the internet for servers, routers and more
» Find computers running certain software (HTTP, FTP, etc.)
» Filter hosts based on geographic location

» Learn more
Basic Operations: Country Filter

- Filtering by country can be accomplished by clicking on the country map (available from the drop down menu).
- Mouse over a country for the number of scanned hosts for a particular country.
Find all 'apache' servers in Switzerland
Find ‘apache’ servers running version 2.2.3

Top four countries matching your query

United States: 382,244
Germany: 64,188
France: 21,339
Canada: 19,037
Basic Operations: Hostname Filter

Search results can be filtered using any portion of a hostname or domain name.

Find ‘apache’ servers in the .nist.gov domain

Find ‘iis-5.0’ servers in the .edu domain
Basic Operations: Net / OS Filters

- The net filter allows you to refine your searches by IP/CIDR notation.
- The OS filter allows you to refine searches by operating system.
Basic Operations: Port Filter

- SHODAN can filter your search results by port
- Current collection is limited to ports 21 (FTP), 22 (SSH), 23 (Telnet), and 80 (HTTP), while the overwhelming majority of collection is HTTP
- More ports/services coming (send requests to the developer via Twitter)
Basic Operations: Searches

- Popular searches are available on the main page
- Logged in users can save searches and share them with other users
Basic Operations: Export

- SHODAN lets you export up to 1,000 results per credit in XML format
- Credits can be purchased online
- Sample data export file is available

```
<shodan>
  <summary date="2010-03-16 23:23:19.921034" query="apache" total="6287987"/>
  <host country="US"
    hostnames="1stadvantagebailbond.com"
    ip="198.171.76.21"
    port="80"
    updated="16.03.2010">
    HTTP/1.0 200 OK
    Date: Tue, 16 Mar 2010 07:43:07 GMT
    Server: Apache/1.3.41 (Unix) FrontPage/5.0.2.2635 mod_ssl/2.8.31 OpenSSL/0.9.7m
    Last-Modified: Tue, 17 Nov 2009 17:40:25 GMT
    ETag: "19258d5-591-4b02e009"
    Accept-Ranges: bytes
    Content-Length: 1425
    Content-Type: text/html
  </host>
  ...
</shodan>
```
SHODAN for Penetration Testers

PENETRATION TESTING
Pen Testing: Ethics (1)

- Is it acceptable under any circumstances to view the configuration of a device that requires no authentication to view?
- What about viewing the configuration of a device using a default username and password?
- What about viewing the configuration of a device using a unique username and password?
- Changing the configuration of any device?
Pen Testing: Ethics (2)

- Default username and password
- Changing configurations
- No authentication
- Unique username and password
Pen Testing Applications

- Using SHODAN for penetration testing requires some basic knowledge of banners including HTTP status codes
- Banners advertise service and version
- Banners can be spoofed (unlikely?)
**Pen Testing: HTTP Status Codes**

<table>
<thead>
<tr>
<th>Status Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>200 OK</td>
<td>Request succeeded</td>
</tr>
<tr>
<td>401 Unauthorized</td>
<td>Request requires authentication</td>
</tr>
<tr>
<td>403 Forbidden</td>
<td>Request is denied regardless of authentication</td>
</tr>
</tbody>
</table>
Pen Testing: Assumptions

- “200 OK” banner results will load without any authentication (at least not initially)
- “401 Unauthorized” banners with `WWW-authenticate` indicate a username and password pop-up box (authentication is possible but not yet accomplished, as distinguished from “403 Forbidden”)
- Some banners advertise defaults
SHODAN for Penetration Testers

CASE STUDY: CISCO DEVICES
Case Study: Cisco Devices

Here is a typical “401 Unauthorized” banner when using the simple search term “cisco”:

HTTP/1.0 401 Unauthorized
Date: Tue, 01 Dec 2009 16:09:46 GMT
Www-authenticate: Basic realm="level_15 or view_access"
Connection: close
Accept-ranges: none
Server: cisco-IOS

Take note of the **Www-authenticate** line which indicates the requirement for a username and password.
Case Study: Cisco Devices

Now consider an example of a “200 OK” banner which does not include the `WWW-authenticate` line:

```
HTTP/1.0 200 OK
Transfer-encoding: chunked
Accept-ranges: none
Expires: Tue, 08 Jun 1993 06:55:45 GMT
Server: cisco-IOS
Last-modified: Tue, 08 Jun 1993 06:55:45 GMT
Connection: close
Cache-control: no-store, no-cache, must-revalidate
Date: Tue, 08 Jun 1993 06:55:45 GMT
Content-type: text/html
```
Case Study: Cisco Devices

A comparison of the two banners finds the second banner to include the *Last-modified* line which **does not** appear when *Www-authenticate* appears:

In fact, among “cisco” results these two lines are more than 99% mutually exclusive.
# Case Study: Cisco Results

<table>
<thead>
<tr>
<th>Search</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>cisco</td>
<td>251,742</td>
</tr>
<tr>
<td>cisco-ios</td>
<td>226,184</td>
</tr>
<tr>
<td>cisco www-authenticate</td>
<td>225,402</td>
</tr>
<tr>
<td>cisco last-modified</td>
<td>4,265</td>
</tr>
<tr>
<td>cisco last-modified www-authenticate</td>
<td>56</td>
</tr>
</tbody>
</table>
Case Study: Cisco Results

- This suggests that Cisco “200 OK” banners that include the *Last-modified* line do not require any authentication (at least not initially)

- The results on the previous slide suggest there are potentially 4,200+ Cisco devices that do not require authentication
Surely these HTML links will require some additional authentication…

Cisco Systems

Accessing Cisco 1812W "CT-1980028"

- Show diagnostic log - display the diagnostic log.
- Monitor the router - HTML access to the command line interface at level 0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
- Show tech-support - display information commonly needed by tech support.
- Extended Ping - Send extended ping commands.
- QoS Device Manager - Configure and monitor QoS through the web interface.
- VPN Device Manager (VDM) - Configure and monitor Virtual Private Networks (VPNs) through the web interface.

Help resources

1. CCO at www.cisco.com - Cisco Connection Online, including the Technical Assistance Center (TAC).
2. tac@cisco.com - e-mail the TAC.
3. 1-800-553-2447 or +1-408-526-7209 - phone the TAC.
4. cs-html@cisco.com - e-mail the HTML interface development group.
Nope. No authentication required for Level 15! No authentication required for configure commands.
No authentication required for Level 15 exec commands
show running-config

Building configuration...

Current configuration: 8995 bytes

version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption

hostname CT-1980028

boot-start-marker
boot-end-marker

logging buffered 51200 warnings

no aaa new-model

command completed.

show cdp neighbors

this[0] = "CN-CNC-VPNHub-1"
this[1] = "10.97.248.1"
this[2] = "Cisco 3745"
this[3] = "Tunnel0"
this[4] = "Tunnel0"
this[5] = "RS I"
this[6] = "CN-CNC-VPNHub-2"
this[7] = "10.65.8.1"
this[8] = "Cisco 3745"
this[9] = "Tunnel1"
this[10] = "Tunnel1"
this[11] = "RS I"

command completed.
## Cisco Aironet 350 Series Access Point

**Hostname**: ap-romeulandi-open

**21:57:35 Mon Dec 7 2009**

### Home: Summary Status

#### Association
- **Clients**: 0
- **Repeaters**: 0

#### Network Identity
- **IP Address**: 200.160.10.8
- **MAC Address**: 0040.9644.b738

#### Network Interfaces

<table>
<thead>
<tr>
<th>Interface</th>
<th>MAC Address</th>
<th>Transmission Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>FastEthernet</td>
<td>0040.9644.b738</td>
<td>100Mb/s</td>
</tr>
<tr>
<td>Radio0-802.11B</td>
<td>0040.9645.ed11</td>
<td>11.0Mb/s</td>
</tr>
</tbody>
</table>

### Event Log

<table>
<thead>
<tr>
<th>Time</th>
<th>Severity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dec 7 20:33:53.718</td>
<td>Warning</td>
<td>Packet to client 0021.c510.b576 reached max retries, removing the client</td>
</tr>
<tr>
<td>Dec 7 20:33:49.495</td>
<td>Information</td>
<td>Interface Dot11Radio0, Deauthenticate Station 0023.6c83.3f41 Reason: Sending station has left the BSS</td>
</tr>
</tbody>
</table>
Cisco Aironet 350 Series Access Point

Hostname: ap-romeulandi-open

Express Set-Up

Host Name: ap-romeulandi-open
MAC Address: 0040.9644.b738

Configuration Server Protocol:
- DHCP
- Static IP

IP Address: 200.160.10.8
IP Subnet Mask: 255.255.255.0
Default Gateway: 200.160.10.1

SNMP Community: registro
- Read-Only
- Read-Write

Radio 0-802.11B

Role in Radio Network:
- Access Point
- Repeater

Optimize Radio Network for:
- Throughput
- Range
- Custom

Aironet Extensions:
- Enable
- Disable
### Express Security Set-Up

#### SSID Configuration

1. **SSID**
   - [ ] Broadcast SSID in Beacon

2. **VLAN**
   - [ ] No VLAN
   - [ ] Enable VLAN ID: __________ (1-4094)
   - [ ] Native VLAN

3. **Security**
   - [ ] No Security
   - [ ] Static WEP Key
     - **Key 1** __________ 128 bit
   - [ ] EAP Authentication
     - **RADIUS Server:** __________ (Hostname or IP Address)
     - **RADIUS Server Secret:** 
   - [ ] WPA
     - **RADIUS Server:** __________ (Hostname or IP Address)
# Cisco Aironet 350 Series Access Point

**Hostname**: ap-romeulandi-open

### Network Interfaces: Summary

<table>
<thead>
<tr>
<th>System Settings</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address (Static)</td>
<td>200.160.10.8</td>
</tr>
<tr>
<td>IP Subnet Mask</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>200.160.10.1</td>
</tr>
<tr>
<td>MAC Address</td>
<td>0040.9644.b738</td>
</tr>
</tbody>
</table>

### Interface Status

<table>
<thead>
<tr>
<th>Interface</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>FastEthernet</td>
<td>Enabled †</td>
</tr>
<tr>
<td>Radio0-802.11B</td>
<td>Enabled †</td>
</tr>
<tr>
<td>Hardware Status</td>
<td>Up †</td>
</tr>
<tr>
<td>Interface Resets</td>
<td>0</td>
</tr>
</tbody>
</table>

### Receive

<table>
<thead>
<tr>
<th>Description</th>
<th>Value 1</th>
<th>Value 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input Rate Timespan</td>
<td>5 minute</td>
<td>5 minute</td>
</tr>
<tr>
<td>Input Rate (bits/sec)</td>
<td>2000</td>
<td>1000</td>
</tr>
<tr>
<td>Input Rate (packets/sec)</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>Time Since Last Input</td>
<td>00:00:00</td>
<td>04:27:34</td>
</tr>
<tr>
<td>Total Packets Input</td>
<td>54958045</td>
<td>56487586</td>
</tr>
</tbody>
</table>
## Security Summary

### Administrators

<table>
<thead>
<tr>
<th>Username</th>
<th>Read-Only</th>
<th>Read-Write</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>

### Service Set Identifiers (SSIDs)

<table>
<thead>
<tr>
<th>SSID</th>
<th>VLAN</th>
<th>Radio</th>
<th>BSSID/Guest Mode</th>
<th>Open</th>
<th>Shared</th>
<th>Network EAP</th>
</tr>
</thead>
<tbody>
<tr>
<td>CGIBR</td>
<td></td>
<td>Radio0-802.11B</td>
<td>0040.9645.ed11 ✓</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Radio0-802.11B Encryption Settings

<table>
<thead>
<tr>
<th>Encryption Mode</th>
<th>WEP</th>
<th>Cipher</th>
<th>Key Rotation</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Server-Based Security

<table>
<thead>
<tr>
<th>Server Name/IP Address</th>
<th>Type</th>
<th>EAP</th>
<th>MAC</th>
<th>Admin</th>
<th>Accounting</th>
</tr>
</thead>
</table>
## Cisco Aironet 350 Series Access Point

**Hostname**: ap-romeulandi-open  
**Date**: 22:02:37 Mon Dec 7 2009

<table>
<thead>
<tr>
<th>Services</th>
<th>Value 1</th>
<th>Value 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telnet/SSH</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>CDP</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>Filters</td>
<td>Filter Defined</td>
<td></td>
</tr>
<tr>
<td>QoS</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>SNMP</td>
<td>Enabled</td>
<td></td>
</tr>
<tr>
<td>VLAN</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>Hot Standby</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>DNS</td>
<td>Enabled</td>
<td></td>
</tr>
<tr>
<td>HTTP</td>
<td>Enabled</td>
<td></td>
</tr>
<tr>
<td>STREAM</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>SNTP</td>
<td>Enabled</td>
<td></td>
</tr>
<tr>
<td>ARP Caching</td>
<td>Enabled</td>
<td></td>
</tr>
</tbody>
</table>
Catalyst 2960 Series Device Manager - STCM-sw1.cb3.bck

Uptime: 1 year, 32 weeks, 2 days, 19 hours, 28 minutes
Next refresh in 55 seconds

Move the pointer over the ports for more information.

Switch Information
- Host Name: STCM-sw1.cb3.bck
- Product ID: WS-C2960-24TT-L
- IP Address: 217.75.0.230
- MAC Address: 00:1E:BD:B8:18:80
- Version ID: V03
- Serial Number: F0C1149W02J
- Software: 12.2(35)SE5
- Contact:
- Location:

Switch Health
- Bandwidth Used: 0%
- Packet Error: 0%
- Fan: OK
- Temp: OK

Port Utilization

View Trends | View Port Statistics
### Catalyst 2960 Series Device Manager - STCM-sw1.cb3.bck

**Uptime:** 1 year, 32 weeks, 2 days, 19 hours, 28 minutes

Next refresh in 27 seconds

**View:** Status

Move the pointer over the ports for more information.

### Port Settings

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
<th>Enable</th>
<th>Speed</th>
<th>Duplex</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fa0/18</td>
<td>SWS Spam firewall</td>
<td>✔</td>
<td>Auto</td>
<td>Auto</td>
</tr>
<tr>
<td>Fa0/19</td>
<td>IomegaNAS</td>
<td>✔</td>
<td>Auto</td>
<td>Auto</td>
</tr>
<tr>
<td>Fa0/20</td>
<td>Fix-IT DRAC port</td>
<td>✔</td>
<td>Auto</td>
<td>Auto</td>
</tr>
<tr>
<td>Fa0/21</td>
<td>Fix-IT Webfarm</td>
<td>✔</td>
<td>Auto</td>
<td>Auto</td>
</tr>
<tr>
<td>Fa0/22</td>
<td>Lynxtec Hosted ser</td>
<td>✔</td>
<td>Auto</td>
<td>Auto</td>
</tr>
<tr>
<td>Fa0/23</td>
<td>ESP Server</td>
<td>✔</td>
<td>Auto</td>
<td>Auto</td>
</tr>
<tr>
<td>Fa0/24</td>
<td>SWS Spam firewall</td>
<td>✔</td>
<td>Auto</td>
<td>Auto</td>
</tr>
<tr>
<td>G10/1</td>
<td>Uplink to SW12</td>
<td>✔</td>
<td>Auto</td>
<td>Auto</td>
</tr>
</tbody>
</table>

---

Submit  Cancel
### Port Status

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
<th>Status</th>
<th>VLAN</th>
<th>Speed</th>
<th>Duplex</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fa0/1</td>
<td>APC Managed PDU</td>
<td></td>
<td>55</td>
<td>100</td>
<td>full</td>
</tr>
<tr>
<td>Fa0/2</td>
<td>Brillo Connection</td>
<td></td>
<td>1</td>
<td>100</td>
<td>full</td>
</tr>
<tr>
<td>Fa0/3</td>
<td>Sanquay Temp Firew</td>
<td></td>
<td>55</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fa0/4</td>
<td></td>
<td></td>
<td>171</td>
<td>100</td>
<td>full</td>
</tr>
<tr>
<td>Fa0/5</td>
<td>Kirby - WF</td>
<td></td>
<td>104</td>
<td>10</td>
<td>full</td>
</tr>
<tr>
<td>Fa0/6</td>
<td></td>
<td></td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fa0/7</td>
<td></td>
<td></td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fa0/8</td>
<td></td>
<td></td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fa0/9</td>
<td></td>
<td></td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fa0/10</td>
<td></td>
<td></td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fa0/11</td>
<td>Sqnquay-CMR</td>
<td></td>
<td>801</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fa0/12</td>
<td>AcomGUY Hosted ser</td>
<td></td>
<td>55</td>
<td>100</td>
<td>full</td>
</tr>
<tr>
<td>Fa0/13</td>
<td></td>
<td></td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fa0/14</td>
<td>Jacc.IT - PWCC WF</td>
<td></td>
<td>40</td>
<td>100</td>
<td>full</td>
</tr>
<tr>
<td>Fa0/15</td>
<td>ProjectMCT-PWCC WF</td>
<td></td>
<td>40</td>
<td>100</td>
<td>full</td>
</tr>
</tbody>
</table>
The username and password are used to log into the router.

### Basic Configuration

<table>
<thead>
<tr>
<th>Username</th>
<th>Login Password</th>
<th>Password is Encrypted</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Secret Password

The enable secret password provides access to the routers command line.

- **Current Password:** <none>
- **Enter New Password:**
- **Re-Enter New Password:**

### Configuration Details

- **Hostname:** DHYHPG
- **Domain Name:**

---

**Model Type:** Cisco 1841  
**IOS Version:** 12.4(18b)
<table>
<thead>
<tr>
<th>Interface</th>
<th>FastEthernet0/1</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>192.168.1.1</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Subnet Bits</td>
<td>24</td>
</tr>
</tbody>
</table>

You can edit the LAN address shown below. Use the new IP address to reconnect to your router from the browser.
Cisco SDM Express lets you configure one WAN connection. To configure a WAN connection, choose an interface, click Add Connection, and enter the connection parameters.

### Interface List

<table>
<thead>
<tr>
<th>Interface</th>
<th>IP</th>
<th>Type</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>FastEthernet0/0</td>
<td>220.231.101.130/30</td>
<td>10/100Ethernet</td>
<td>Up</td>
</tr>
</tbody>
</table>
When a router has not learned a route to a destination network, it can use a configured default route. The default route specifies the next stop for traffic to unknown networks, called the next hop. You can specify a router interface, or an IP address as the next hop.

- **Enable default route**

Select a router interface or the IP address of a remote host as the next hop.

- Interface: FastEthernet0/0
- IP Address: 220.231.101.129
Security Settings

- **Disable services that involve security risks**
  This disables active services such as Finger, PAD, CDP etc. which may make your router vulnerable to security attacks.

- **Enable services for enhanced security on the router/network**
  This enables Logging and other services, which will enhance the security on the router.

- **Encrypt passwords**
  This encrypts all passwords on your router by enabling password encryption services.

Router Clock Settings

You can synchronize your router's date/time settings with the local PC clock. The router clock is used during negotiation of some of the security options.

- Synchronize with my local PC clock
SHODAN for Penetration Testers

CASE STUDY: DEFAULT PASSWORDS
Case Study: Default Passwords (1)

- The ‘default password’ search locates servers that have those words in the banner

- This doesn’t suggest that these results will be using the defaults, but since they’re advertising the defaults they would potentially be the lowest hanging fruit
Case Study: Default Passwords (2)

An example of a ‘default password’ result:

HTTP/1.0 401
Date: Sat, 21 Dec 1996 12:00:00 GMT
WWW-authenticate: Basic realm="Default password:1234"
Server: PrintSir WEBPORT 1.1

The server line indicates this is likely to be a print server; also note the “401” and WWW-authenticate which indicates the likelihood of a username and password pop-up box.
Case Study: Default Passwords (3)

- This does not suggest that this device is using the default password, but it does mean that it is a possibility
- While no username is listed, a null username or “admin” is always a good guess
- And did it work?
A username and password are being requested by http://220.130.40.86. The site says: "Default password: 1234"

User Name: 

Password: 

OK Cancel
<table>
<thead>
<tr>
<th>Feature</th>
<th>Value</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Printers (LP)</td>
<td>PSCC789E</td>
<td>Enable</td>
</tr>
<tr>
<td>IPP Printers (IP)</td>
<td>EPSON680</td>
<td>Enable</td>
</tr>
<tr>
<td>LPR Printers (L)</td>
<td>PS1206P</td>
<td>Enable</td>
</tr>
<tr>
<td>AppleTalk Printers (AP)</td>
<td>2.6.21</td>
<td>Enable</td>
</tr>
<tr>
<td>NetWare Printers (NW)</td>
<td>00:00:B4:CC:78:9E</td>
<td>Enable</td>
</tr>
<tr>
<td>SMB Port Number</td>
<td>No</td>
<td>Enable</td>
</tr>
<tr>
<td>LPT Port Number</td>
<td>1</td>
<td>Enable</td>
</tr>
<tr>
<td>NetBEUI Port Number</td>
<td>No</td>
<td>Disable</td>
</tr>
</tbody>
</table>
SHODAN for Penetration Testers

CASE STUDY: INFRASTRUCTURE EXPLOITATION

How to PWN an ISP
Cisco Systems

Accessing Cisco WS-C3750G-12S

Telnet - to the router.
Show interfaces - display the status of the interfaces.
Show diagnostic log - display the diagnostic log.
Monitor the router - HTML access to the command line interface at level 0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15.
Connectivity test - ping the nameserver.

Show tech-support - display information commonly needed by tech support.
Extended Ping - Send extended ping commands.

Web Console - Manage the Switch through the web interface.

Help resources

1. CCO at www.cisco.com - Cisco Connection Online, including the Technical Assistance Center (TAC).
2. tac@cisco.com - e-mail the TAC.
3. 1-800-553-2447 or +1-408-526-7209 - phone the TAC.
4. cs-html@cisco.com - e-mail the HTML interface development group.
Output

Command base-URL was: /level/15/exec/-
Complete URL was: /level/15/exec/-/show/ip/route/CR
Command was: show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is                     to network 0.0.0.0

        is variably subnetted, 10 subnets, 3 masks

D    EX               [170/28416] via          2w5d, Vlan401
         [170/28416] via          2w5d, Vlan400
D                        [90/3072] via          2w5d, Vlan401
         [90/3072] via          2w5d, Vlan400
D    EX               [170/4226816] via         3w5d, Vlan401
         [170/4226816] via         3w5d, Vlan400
D    EX               [170/3115776] via         3w5d, Vlan401
         [170/3115776] via         3w5d, Vlan400
D    EX               [170/2178816] via      02:01:41, Vlan401
         [170/2178816] via      02:01:41, Vlan400
D    EX               [170/3072] via          2w5d, Vlan401
         [170/3072] via          2w5d, Vlan400
Command base-URL was: /level/15/exec/-
Complete URL was: /level/15/exec/-/show/running-config/CR
Command was: show running-config

Building configuration...

Current configuration : 10374 bytes
  
  ! Last configuration change at 06:40:37 EST Tue Apr 6 2010 by
  ! NVRAM config last updated at 06:40:48 EST Tue Apr 6 2010 by
  
  version 12.2
  no service pad
  service timestamps debug datetime msec
  service timestamps log datetime msec
  no service password-encryption
  !
  hostname
  !
  boot-start-marker
  boot-end-marker
  !
  username     privilege 15 secret 5
  username     privilege 2 secret 5
  aaa new-model
  !
  !
Command base-URL was: /level/15/exec/-
Complete URL was:/level/15/exec/-/show/cdp/neighbors/CR
Command was: show cdp neighbors

Capability Codes:  R - Router,  T - Trans Bridge,  B - Source Route Bridge
             S - Switch,  H - Host,  I - IGMP,  r - Repeater,  P - Phone

<table>
<thead>
<tr>
<th>Device ID</th>
<th>Local Intrfce</th>
<th>Holdtme</th>
<th>Capability</th>
<th>Platform</th>
<th>Port ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gig 1/0/11</td>
<td>173</td>
<td>R S I</td>
<td></td>
<td>CISCO7606 Gig 1/6</td>
<td></td>
</tr>
<tr>
<td>Gig 1/0/12</td>
<td>143</td>
<td>R S I</td>
<td></td>
<td>WS-C3750 Gig 1/0/12</td>
<td></td>
</tr>
<tr>
<td>Gig 1/0/2</td>
<td>155</td>
<td>S I</td>
<td></td>
<td>WS-C3750- Gig 1/0/1</td>
<td></td>
</tr>
<tr>
<td>Gig 1/0/10</td>
<td>167</td>
<td>S I</td>
<td></td>
<td>WS-C3560E Gig 0/25</td>
<td></td>
</tr>
<tr>
<td>Gig 1/0/9</td>
<td>131</td>
<td>R S I</td>
<td></td>
<td>WS-C3750- Gig 1/0/1</td>
<td></td>
</tr>
</tbody>
</table>

Command completed.
Case Study:  How to PWN an ISP

- Two Cisco 3750 infrastructure switches with direct access to Cisco 7606 Router
- VLAN IDs for internal ISP network, hotels, condos, apartments, convention center, public backbone...
- SNMP server IP address and community strings
SHODAN for Penetration Testers

OTHER EXAMPLES
Some general observations…
javascript:SnapshotWin()
client.html
system.html
security.html
network.html
wireless.html
ddns.html
accesslist.html
audiovideo.html
cameracontrol.html
mailftp.html
motion.html
application.html
syslog.html
parafile.html
maintain.html
SHODAN for Penetration Testers

THE FUTURE
The Future

- API in the works for program integration
- Summary report for export option
- Software fingerprints
- Collection of HTTPS
SHODAN for Penetration Testers

CONCLUSIONS
Conclusions

- SHODAN aggregates a significant amount of information that isn’t already widely available in an easy to understand format
- Allows for passive vulnerability analysis

**Bottom line:** SHODAN is a potential game-changer for pen testers that will help shape the path for future vulnerability assessments
Authors and add-ons

- John Matherly (http://twitter.com/achillean)
- Gianni Amato (SHODAN Helper)
- sagar38 (SHODAN Search Provider)
SHODAN for Penetration Testers

QUESTIONS