

Letters to Santa--a real world attack

Part 3, More Reconnaissance

In the last section you should have found that the Letters to Santa site and the development site are both at the same IP address. The dev site is in scope!

```
C:\Users\John>nslookup 12s.northpolechristmastown.com
Server: UnKnown
Address: 10.128.128.128

Non-authoritative answer:
Name: 12s.northpolechristmastown.com
Address: 35.185.84.51

C:\Users\John>nslookup dev.northpolechristmastown.com
Server: UnKnown
Address: 10.128.128.128

Non-authoritative answer:
Name: dev.northpolechristmastown.com
Address: 35.185.84.51
```

<sidebar>

In case you are wondering how two web sites can be on the same IP address, HTTP and HTTPS allow the browser to specify the web site name in the request. Since IPv4 addresses are in short supply most ISPs put many sites on the same IP address. In fact, many modern web servers will not respond if the IP address is put into the browser address (or URL) bar instead of the domain name of the site. The browser puts the domain name of the web server in the HOST field of the HTTP request header. It is easy to see the HOST field in an unencrypted (HTTP) request header.

```
Wireshark · Follow TCP Stream (tcp.stream eq 10) · wireshark_eth0_20180327155652_ICbA87
GET / HTTP/1.1
Host: dev.northpolechristmastown.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
```

No.	Time	Source	Destination	Protocol	Length	Info
25	3.382451892	192.168.2.138	35.185.84.51	TCP	74	55472 → 80
26	3.411892676	35.185.84.51	192.168.2.138	TCP	60	80 → 55472
27	3.412013617	192.168.2.138	35.185.84.51	TCP	54	55472 → 80
28	3.412665332	192.168.2.138	35.185.84.51	HTTP	384	GET / HTTP/1.1
29	3.413085785	35.185.84.51	192.168.2.138	TCP	60	80 → 55472
30	3.444870482	35.185.84.51	192.168.2.138	HTTP	453	HTTP/1.1 303 See other

▶ Frame 28: 384 bytes on wire (3072 bits), 384 bytes captured (3072 bits) on interface 0
 ▶ Ethernet II, Src: Vmware_96:54:94 (00:0c:29:96:54:94), Dst: Vmware_fb:1c:5c (00:50:56:fb:1c:5c)
 ▶ Internet Protocol Version 4, Src: 192.168.2.138, Dst: 35.185.84.51
 ▶ Transmission Control Protocol, Src Port: 55472, Dst Port: 80, Seq: 1, Ack: 1, Len: 338
 ▼ Hypertext Transfer Protocol
 ▶ GET / HTTP/1.1\r\n
 Host: dev.northpolechristmastown.com\r\n
 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0\r\n
 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
 Accept-Language: en-US,en;q=0.5\r\n
 Accept-Encoding: gzip, deflate\r\n
 Connection: keep-alive\r\n
 Upgrade-Insecure-Requests: 1\r\n
 \r\n

In an encrypted (HTTPS) request the name of the site is given, in clear text, in the Server Name Indication (SNI) when the TLS session is started. This allows the server to determine which site is being requested and present the matching certificate to the browser. More information is available [here](#) and [here](#).



No.	Time	Source	Destination	Protocol	Length	Info
13	2.786984780	192.168.2.140	35.185.84.51	TCP	54	45286 → 443 [ACK] S
14	2.787259956	192.168.2.140	35.185.84.51	TLSv1.2	201	Client Hello
15	2.787852040	35.185.84.51	192.168.2.140	TCP	60	443 → 45286 [ACK] S

Secure Sockets Layer	
	TLSv1.2 Record Layer: Handshake Protocol: Client Hello
	Content Type: Handshake (22)
	Version: TLS 1.0 (0x0301)
	Length: 202
	Handshake Protocol: Client Hello
	Handshake Type: Client Hello (1)
	Length: 198
	Version: TLS 1.2 (0x0303)
	Random: 35a0f05335ceb9e46427ddb6e2ab8ec0c05f7f96a5a611b8...
	GMT Unix Time: Jul 6, 1998 11:42:11.000000000 EDT
	Random Bytes: 35ceb9e46427ddb6e2ab8ec0c05f7f96a5a611b885897990...
	Session ID Length: 0
	Cipher Suites Length: 30
	Cipher Suites (15 suites)
	Compression Methods Length: 1
	Compression Methods (1 method)
	Extensions Length: 127
	Extension: server_name (len=35)
	Type: server_name (0)
	Length: 35
	Server Name Indication extension
	Server Name list length: 33
	Server Name Type: host_name (0)
	Server Name length: 30
	Server Name: 12s.northpolechristmastown.com
	Extension: extended_master_secret (len=0)

</sidebar>

Examine the <http://dev.northpolechristmastown.com> site, and its source code. Remember the links about vulnerabilities you saw in Part 1, and Sparkle Redberry's last two hints (especially the link she gives you.)

Questions, part 3

- 1) What would be a promising attack to try in the next stage?
- 2) What evidence do you have to support this decision?