

SPtrace: Simulate port/protocol trace.

DESCRIPTION: The SPtrace command simulates ftp, ssh, telnet, smtp, http, pop, imap trace.

USAGE: ./SPtrace <port> <expect_file> <response_file>

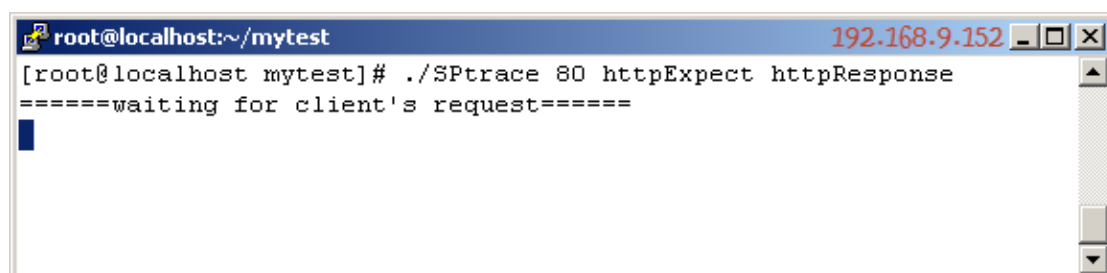
<port>: default port for specific protocol. e.g: 21 for 'ftp'. (Make sure this port is not already in use, or you need to stop this port first and don't forget to restore the change afterwards.)

<expect_file>: this file lists the expected requests, which are used to compare with the requests from client to decide whether to send out the responses in <response_file>.

<response_file>: this file lists the simulated responses for expected requests.

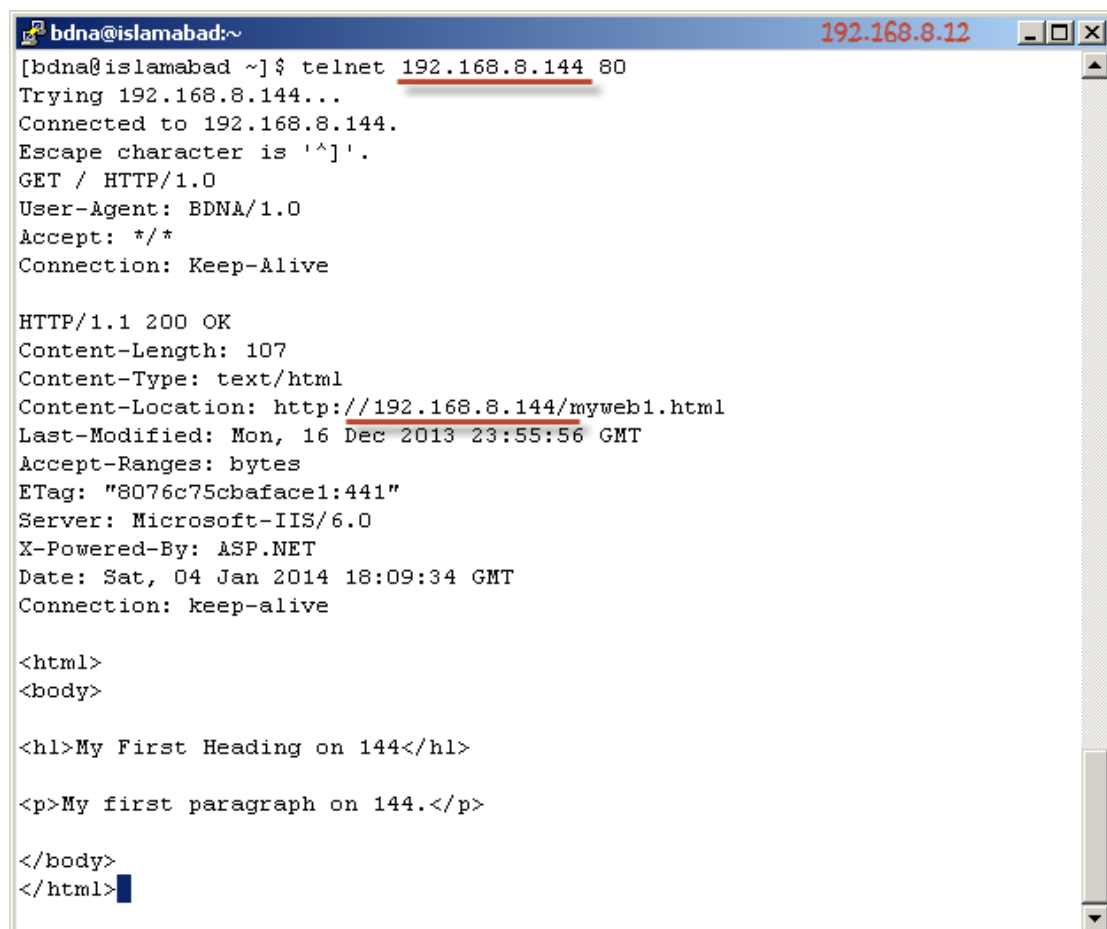
Note: the simulated **responses** are corresponding to the expected **requests** line by line.

EXAMPLES: ./SPtrace 80 httpExpect httpResponse

A terminal window titled 'root@localhost:~/mytest' with an IP address of 192.168.9.152. The command './SPtrace 80 httpExpect httpResponse' has been executed, resulting in the output '====waiting for client's request====' followed by a cursor.

```
root@localhost:~/mytest 192.168.9.152
[root@localhost mytest]# ./SPtrace 80 httpExpect httpResponse
====waiting for client's request====
```

Real trace on 192.168.8.144:

A terminal window titled 'bdna@islamabad:~' with an IP address of 192.168.8.12. It shows a telnet session to 192.168.8.144 on port 80. The output includes the client's GET request, the server's HTTP 200 OK response with various headers, and the beginning of an HTML document.

```
bdna@islamabad:~ 192.168.8.12
[bdna@islamabad ~]$ telnet 192.168.8.144 80
Trying 192.168.8.144...
Connected to 192.168.8.144.
Escape character is '^]'.
GET / HTTP/1.0
User-Agent: BDNA/1.0
Accept: */*
Connection: Keep-Alive

HTTP/1.1 200 OK
Content-Length: 107
Content-Type: text/html
Content-Location: http://192.168.8.144/myweb1.html
Last-Modified: Mon, 16 Dec 2013 23:55:56 GMT
Accept-Ranges: bytes
ETag: "8076c75cbaface1:441"
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Date: Sat, 04 Jan 2014 18:09:34 GMT
Connection: keep-alive

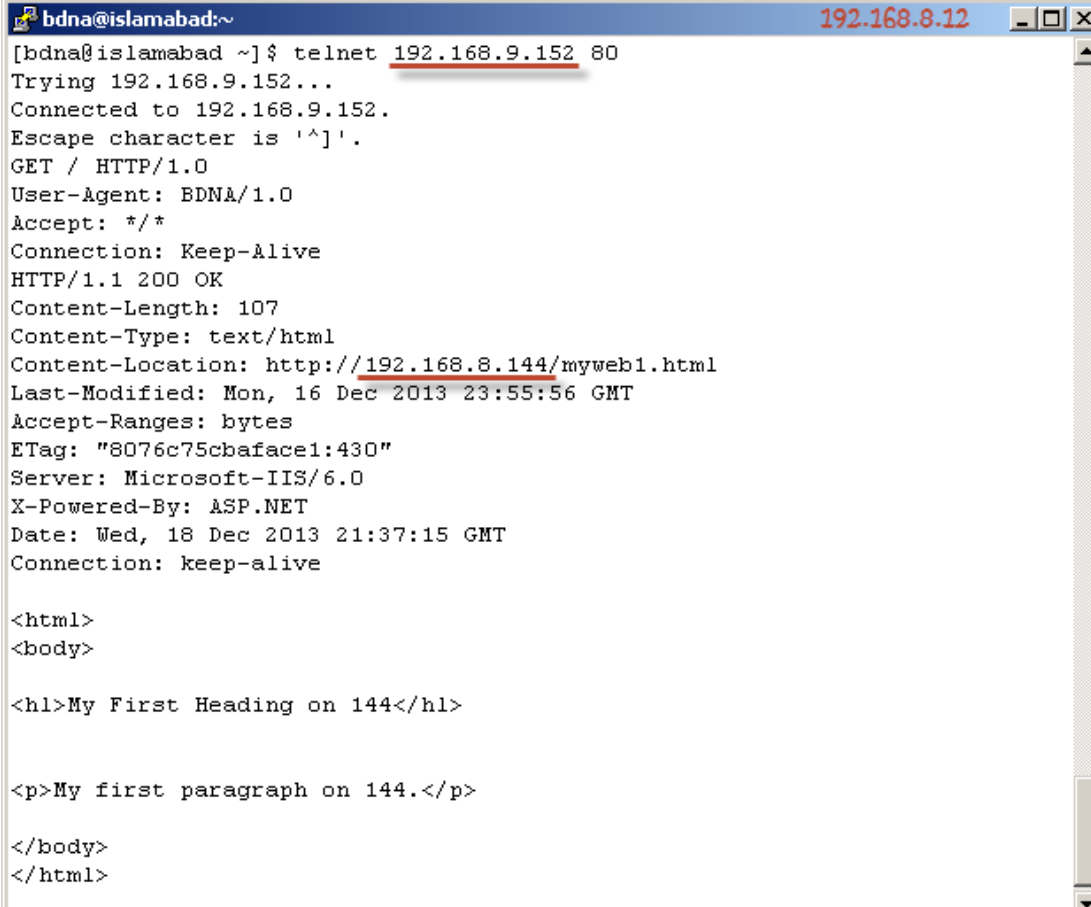
<html>
<body>

<h1>My First Heading on 144</h1>

<p>My first paragraph on 144.</p>

</body>
</html>
```

Simulated trace on 192.168.9.152:



```
[bdna@islamabad ~]$ telnet 192.168.9.152 80
Trying 192.168.9.152...
Connected to 192.168.9.152.
Escape character is '^]'.
GET / HTTP/1.0
User-Agent: BDNA/1.0
Accept: */*
Connection: Keep-Alive
HTTP/1.1 200 OK
Content-Length: 107
Content-Type: text/html
Content-Location: http://192.168.8.144/myweb1.html
Last-Modified: Mon, 16 Dec 2013 23:55:56 GMT
Accept-Ranges: bytes
ETag: "8076c75cbaface1:430"
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Date: Wed, 18 Dec 2013 21:37:15 GMT
Connection: keep-alive

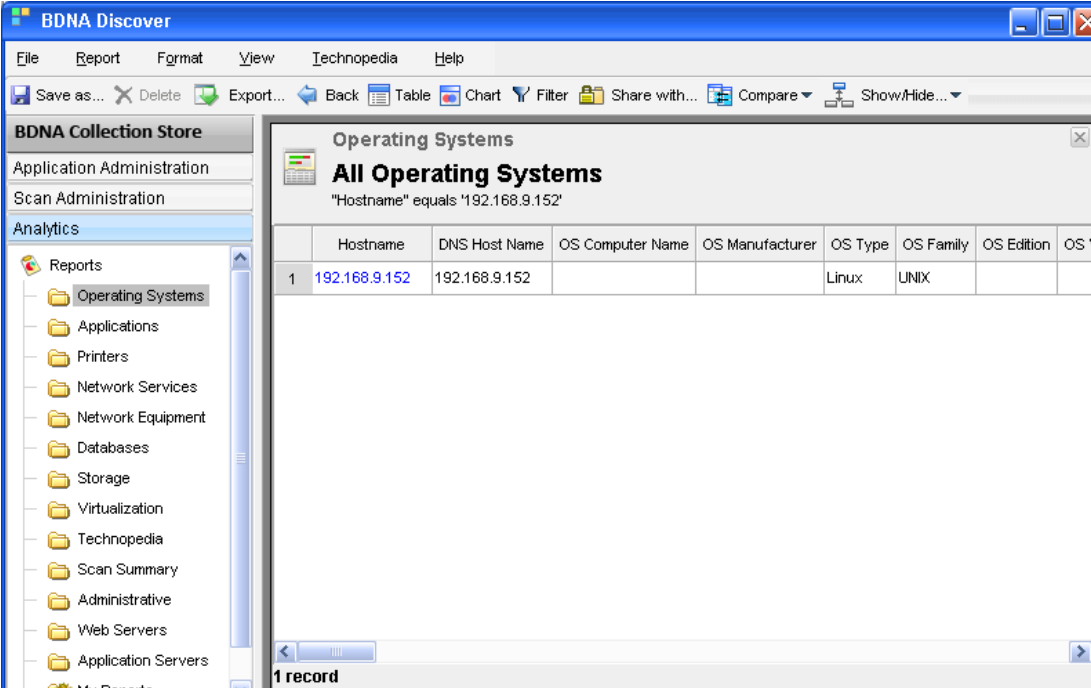
<html>
<body>

<h1>My First Heading on 144</h1>

<p>My first paragraph on 144.</p>

</body>
</html>
```

Level 1 scan against 192.168.9.152 before simulating http trace on that host **Types** it as LINUX.



BDNA Discover

File Report Format View Technopedia Help

Save as... Delete Export... Back Table Chart Filter Share with... Compare Show/Hide...

BDNA Collection Store

- Application Administration
- Scan Administration
- Analytics
 - Reports
 - Operating Systems**
 - Applications
 - Printers
 - Network Services
 - Network Equipment
 - Databases
 - Storage
 - Virtualization
 - Technopedia
 - Scan Summary
 - Administrative
 - Web Servers
 - Application Servers
 - My Reports

Operating Systems

All Operating Systems

"Hostname" equals '192.168.9.152'

	Hostname	DNS Host Name	OS Computer Name	OS Manufacturer	OS Type	OS Family	OS Edition	OS \
1	192.168.9.152	192.168.9.152			Linux	UNIX		

1 record

工作表 查询构建器					
SELECT * FROM inv_final_host_traces;					
查询结果 x					
SQL 已提取 50 行, 用时 0.047 秒					
NET	IP	HOST	WINNING_METHOD	WINNING_OSTYPE	
1 9152	192.168.9.152	192.168.9.152	Nmap 5.21	Linux	

Level 1 scan against 192.168.9.152 after simulating http trace on that host **Types** it as Windows

BDNA Discover							
File Report Format View Technopedia Help							
Save as... Delete Export... Back Table Chart Filter Share with... Compare Show/Hide...							
BDNA Collection Store							
Application Administration							
Scan Administration							
Analytics							
Reports							
Operating Systems							
Applications							
Printers							
Network Services							
Network Equipment							
Databases							
Storage							
Virtualization							
Technopedia							
Scan Summary							
Operating Systems							
All Operating Systems							
	Hostname	DNS Host Name	OS Computer Name	OS Manufacturer	OS Type	OS Family	OS Edition
1	192.168.9.152	192.168.9.152		Microsoft Corporation	Windows	Windows	
1 record							

工作表 查询构建器					
SELECT * FROM inv_final_host_traces;					
查询结果 x					
SQL 提取的所有行: 1, 用时 0 秒					
NET	IP	HOST	WINNING_METHOD	WINNING_O...	
1 9152	192.168.9.152	192.168.9.152	httpPortTrace	Windows	

httpExpect & httpResponse

ftpExpect & ftpResponse

If the first expected request equals to 'null', the first response will be sent out as long as the client get connected, even though, the client did not send request at that moment.



```

root@localhost:~/mytest
220 Microsoft FTP Service
221 Goodbye

2 simulated response

~
~
"ftptrace" 4L, 41C

```