

LetsDefend: Http Basic Auth

The following writeup is for [HTTP Basic Auth](#) on LetsDefend, it involves investigating a pcap using Wireshark.

Scenario: We receive a log indicating a possible attack, can you gather information from the .pcap file?

How many HTTP GET requests are in pcap?

If you are using tshark, you can simply enter the following command that filters for HTTP GET requests and counts the number of lines (aka counts the number of GET requests):

```
tshark -n -r webserver.em0.pcap -Y 'http.request.method==GET' | wc -l  
5
```

Alternatively, just use Wireshark:

http.request.method==GET						
No.	Time	Source	Destination	Protocol	Length	Info
12	64.550254	192.168.63.20	1.1.1.5	HTTP	303	GET / HTTP/1.0
21	67.564082	192.168.63.20	1.1.1.5	HTTP	350	GET / HTTP/1.0
37	201.439138	192.168.63.50	1.1.1.5	HTTP	428	GET / HTTP/1.1
47	221.922660	192.168.63.20	1.1.1.5	HTTP	303	GET / HTTP/1.0
57	224.938759	192.168.63.20	1.1.1.5	HTTP	350	GET / HTTP/1.0

What is the server operating system?

If you follow the TCP or HTTP stream of any of these requests, you can see that the web serving is running on FreeBSD:

```
HTTP/1.1 401 Authorization Required  
Date: Thu, 20 Jan 2011 07:36:27 GMT  
Server: Apache/2.2.15 (FreeBSD) DAV/2 mod_ssl/2.2.15 OpenSSL/0.9.8n  
WWW-Authenticate: Basic realm="Restricted"  
Content-Length: 401  
Connection: close  
Content-Type: text/html; charset=iso-8859-1
```

What is the name and version of the web server software?

```
Server: Apache/2.2.15
```

What is the version of OpenSSL running on the server?

```
OpenSSL/0.9.8n
```

What is the client's user-agent information?

If you look at the packet details pane, you can see the User-Agent string in any of the HTTP requests:

Lynx/2.8.7rel.1 libwww-FM/2.14 SSL-MM/1.4.1 OpenSSL/0.9.8n

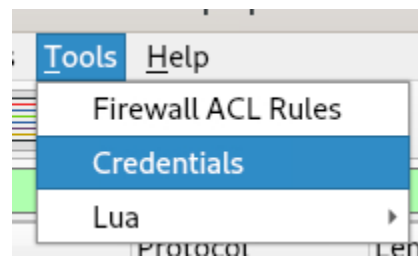
```
User-Agent: Lynx/2.8.7rel.1 libwww-FM/2.14 SSL-MM/1.4.1 OpenSSL/0.9.8n\r\n
```

What is the username used for Basic Authentication?

We can use the http.authbasic display filter to see basic authentication attempts:

```
Authorization: Basic d2ViYWRTaW46VzNiNERtMW4=\r\n
Credentials: webadmin:W3b4Dm1n
```

Alternatively, you can navigate to Tools > Credentials:



And here you will see the packet numbers associated with basic authentication:

Wireshark · Credentials · webser			
Packet N	Protocol	Username	Additional Info
21	HTTP ...	webadmin	
57	HTTP ...	webadmin	

The username is webadmin

What is the user password used for Basic Authentication?

The password is W3b4Dm1n