Web Application Pentesting

Vivek Ramachandran

SWSE, SMFE, SPSE, SISE, SLAE, SGDE Course Instructor

Certifications: http://www.securitytube-training.com

Pentester Academy: http://www.PentesterAcademy.com

HTTP Digest Authentication (RFC 2617)

RFC 2617 – Security Enhanced

- Adds Client Nonce
  - Mitigate chosen Plain-text attacks
- Adds "QOP" – Quality of Protection
  - auth for Authentication
  - auth-int for Authentication and Integrity
    - Rarely used and not well supported

HTTP Digest Authentication with QOP=auth

The first time the client requests the document, no Authorization header is sent, so the server responds with:

```
HTTP/1.1 401 Unauthorized
WWW-Authenticate: Digest
        realm="testrealm@host.com",
        qop="auth,auth-int",
        nonce="dcd98b7102dd2f0e8b11d0f600bfb0c093",
        opaque="5ccc069c403ebaf9f0171e9517f40e41"
```

The client may prompt the user for the username and password, after which it will respond with a new request, including the following Authorization header:

```
Authorization: Digest username="Mufasa",
        realm="testrealm@host.com",
        nonce="dcd98b7102dd2f0e8b11d0f600bfb0c093",
        uri="/dir/index.html",
        qop=auth,
        nc=00000001,
        cnonce="0a4f113b",
        response="6629fae49393a05397450978507c4ef1",
        opaque="5ccc069c403ebaf9f0171e9517f40e41"
```

Source: http://tools.ietf.org/html/rfc2617

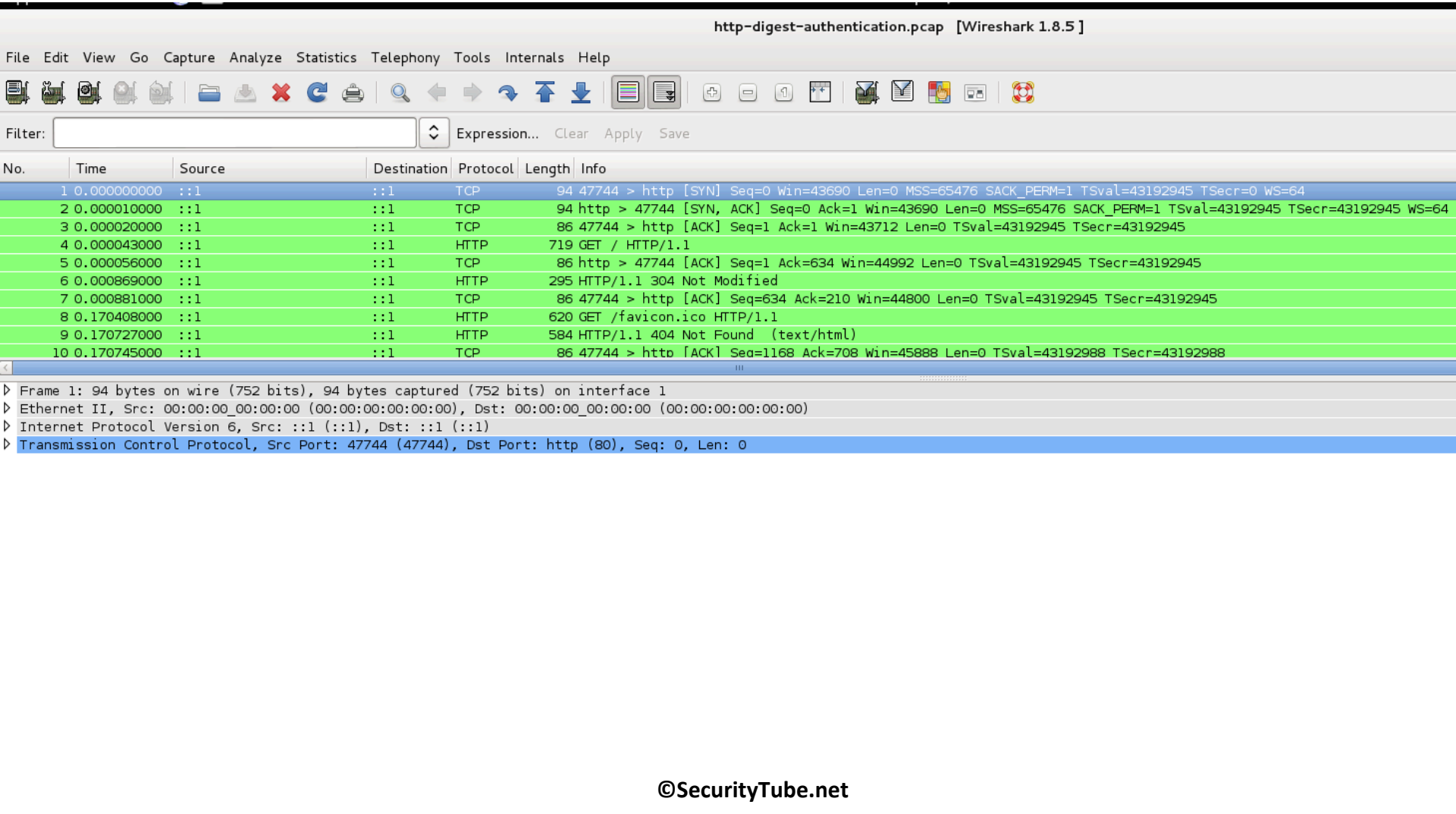
Response Calculation (RFC 2617)

Hash1 = MD5(Username:Realm:Password)

Hash2 = MD5(method:URI)

Response = MD5(Hash1:Nonce:NonceCount:Client-Nonce:QOP:Hash2)

Wireshark – Digest Authentication



Digest Authentication

```
GET / HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:22.0) Gecko/20100101 Firefox/22.0 Iceweasel/22.0
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
If-Modified-Since: Tue, 23 Jul 2013 12:26:26 GMT
If-None-Match: "486ae-b1-4e22ce6d50080"
Authorization: Digest username="vivek", realm="Pentester-Academy", nonce="cmMXCA/nBAA=7002cad884ece9b87dd63d4a0aa7f3b1cf9f731b", uri="/",
algorithm=MD5, response="9444743d2960f562e0145a53cc4e2390", qop=auth, nc=00000001, cnonce="c6470d4d075843c9"

HTTP/1.1 304 Not Modified
Date: Mon, 23 Sep 2013 15:54:32 GMT
Server: Apache/2.2.22 (Debian)
Connection: Keep-Alive
Keep-Alive: timeout=5, max=100
ETag: "486ae-b1-4e22ce6d50080"
Vary: Accept-Encoding
```

Response Calculation (RFC 2617)

Hash1 = MD5(Username:Realm:Password)

```
PentesterAcademy# python
Python 2.7.3 (default, Jan  2 2013, 13:56:14)
[GCC 4.7.2] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>>
>>> import hashlib
>>>
>>> hash1 = hashlib.md5("vivek:Pentester-Academy:pentesteracademy").hexdigest()
>>>
>>> hash1
'4260744fc3c98fd3223426fc152374a4'
>>>
>>>
```

Use Python 2.7.x

Response Calculation (RFC 2617)

Hash2 = MD5(method:URI)

```
>>>
>>>
>>> hash2 = hashlib.md5("GET:/").hexdigest()
>>>
>>> hash2
'71998c64aea37ae77020c49c00f73fa8'
>>>
>>>
```

Response Calculation (RFC 2617)

Response = MD5(Hash1:Nonce:NonceCount:Client-Nonce:QOP:Hash2)

```
>>>
>>> nonce = "cmMXCA/nBAA=7002cad884ece9b87dd63d4a0aa7f3b1cf9f731b"
>>>
>>> nonceCount = "00000001"
>>>
>>> clientNonce = "c6470d4d075843c9"
>>>
>>> qop = "auth"
>>>
>>> response_string = hash1 + ':' + nonce + ':' + nonceCount + ':' + clientNonce + ':' + qop + ':' + hash2
>>>
>>> response = hashlib.md5(response_string).hexdigest()
>>>
>>> response
'9444743d2960f562e0145a53cc4e2390'
>>>
```



```
Authorization: Digest username="vivek", realm="Pentester-Academy", nonce="cmMXCA/nBAA=7002cad884ece9b87dd63d4a0aa7f3b1cf9f731b", uri="/",
algorithm=MD5, response="9444743d2960f562e0145a53cc4e2390", qop=auth, nc=00000001, cnonce="c6470d4d075843c9"
```

Pentester Academy

PentesterAcademy | a SecurityTube.net initiative

TOPICS PRICING WHY SUBSCRIBE MEMBER ACCESS

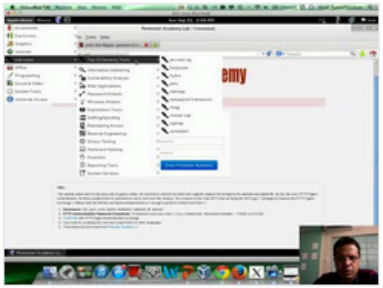
Revolutionizing Infosec Training

Highly Technical, Hands-on, Affordable

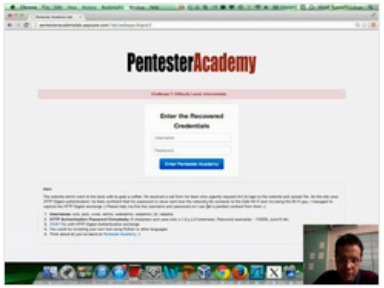
Start Learning Today!

Latest Videos

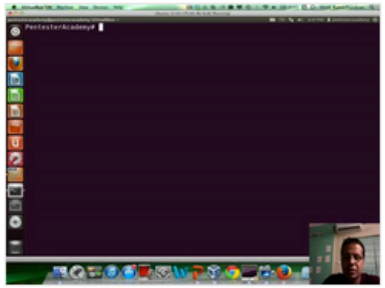
New content added weekly!



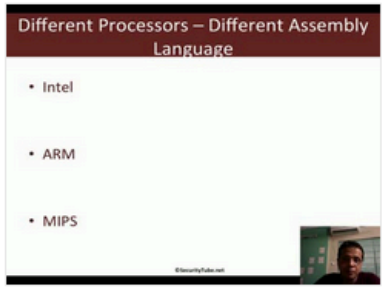
Challenge 7: Cracking Digest Authentication Solution in WAP Challenges



Challenge 7: Cracking Digest Authentication in WAP Challenges



Module 1: GDB Test Solution in x86_64 Assembly Language and Shellcoding on Linux



Module 1: CPU Information in x86_64 Assembly Language and Shellcoding on Linux