

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>

File Extraction from HTTP Traffic

Tcpxtract

File Edit View Search Terminal Help

```
PentesterAcademy# apt-get install tcpxtract
```

```
Reading package lists... Done
```

```
Building dependency tree
```

```
Reading state information... Done
```

```
The following NEW packages will be installed:
```

```
tcpxtract
```

```
0 upgraded, 1 newly installed, 0 to remove and 88 not upgraded.
```

```
Need to get 16.7 kB of archives.
```

```
After this operation, 72.7 kB of additional disk space will be used.
```

```
Get:1 http://http.kali.org/kali/ kali/main tcpxtract amd64 1.0.1-8 [16.7 kB]
```

```
Fetch:16.7 kB in 3s (4,499 B/s)
```

```
Selecting previously unselected package tcpxtract.
```

```
(Reading database ... 280761 files and directories currently installed.)
```

```
Unpacking tcpxtract (from .../tcpxtract_1.0.1-8_amd64.deb) ...
```

```
Processing triggers for man-db ...
```

```
Setting up tcpxtract (1.0.1-8) ...
```

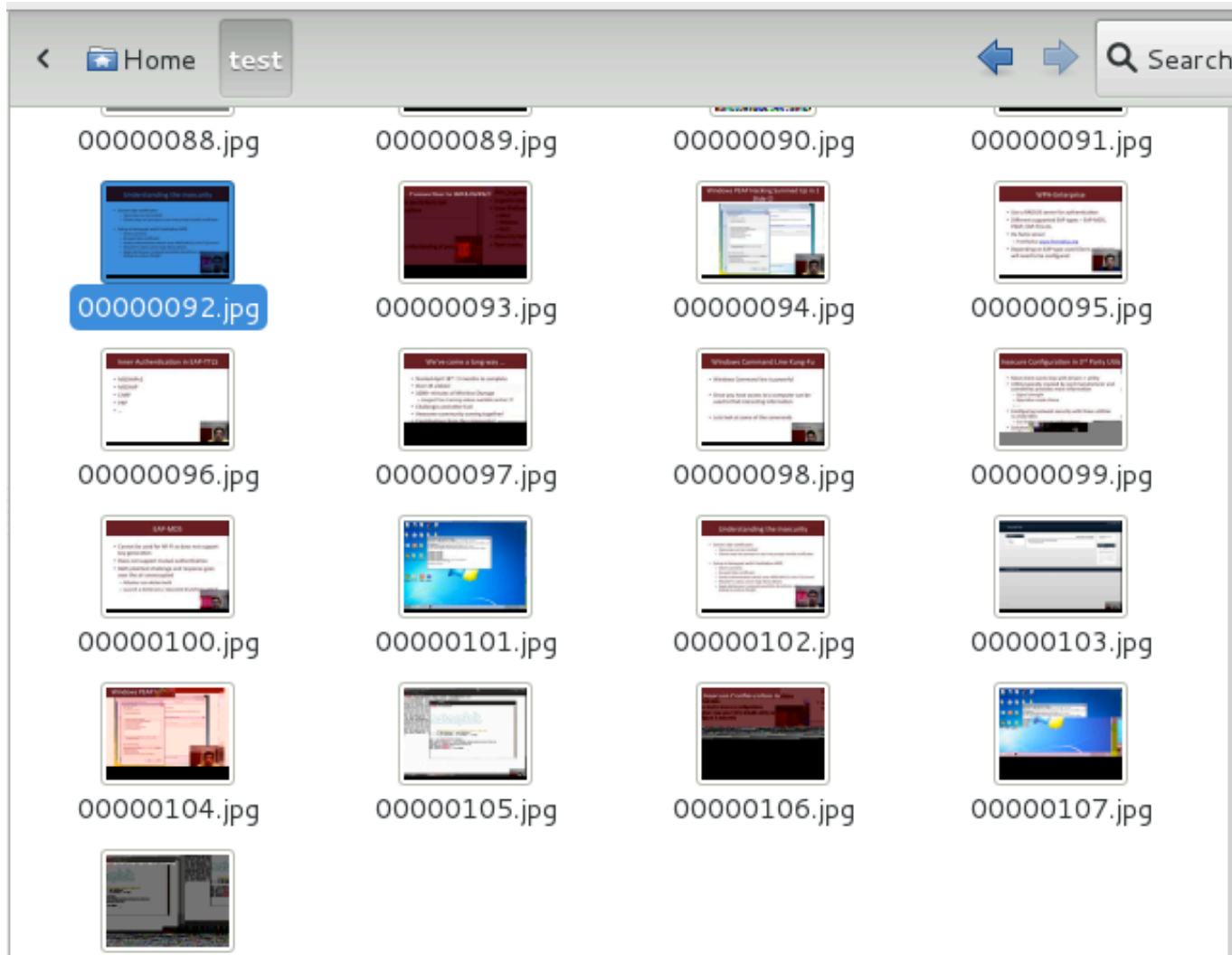
```
PentesterAcademy# █
```

Recovering Files

```
PentesterAcademy# tcpxtract -d eth0 -o test
```

```
Found file of type "html" in session [192.168.1.15:52966 -> 74.125.135.121:20480], exporting to test/00000000.html
Found file of type "html" in session [192.168.1.15:52966 -> 74.125.135.121:20480], exporting to test/00000001.html
Found file of type "html" in session [74.125.135.121:20480 -> 192.168.1.15:52966], exporting to test/00000002.html
Found file of type "html" in session [192.168.1.15:26855 -> 31.13.79.81:20480], exporting to test/00000003.html
Found file of type "html" in session [192.168.1.15:26855 -> 31.13.79.81:20480], exporting to test/00000004.html
Found file of type "html" in session [31.13.79.81:20480 -> 192.168.1.15:26855], exporting to test/00000005.html
Found file of type "gif" in session [74.125.236.37:20480 -> 192.168.1.15:38529], exporting to test/00000006.gif
Found file of type "html" in session [74.125.236.164:20480 -> 192.168.1.15:52128], exporting to test/00000007.html
Found file of type "gif" in session [74.125.236.37:20480 -> 192.168.1.15:38529], exporting to test/00000008.gif
Found file of type "gif" in session [216.59.38.124:20480 -> 192.168.1.15:9431], exporting to test/00000009.gif
Found file of type "html" in session [192.168.1.15:52966 -> 74.125.135.121:20480], exporting to test/00000010.html
Found file of type "html" in session [192.168.1.15:52966 -> 74.125.135.121:20480], exporting to test/00000011.html
Found file of type "html" in session [74.125.135.121:20480 -> 192.168.1.15:52966], exporting to test/00000012.html
Found file of type "html" in session [192.168.1.15:26855 -> 31.13.79.81:20480], exporting to test/00000013.html
```

Recovering Files



Pentester Academy

PentesterAcademy

a SecurityTube.net initiative



TOPICS

PRICING

WHY SUBSCRIBE

MEMBER ACCESS



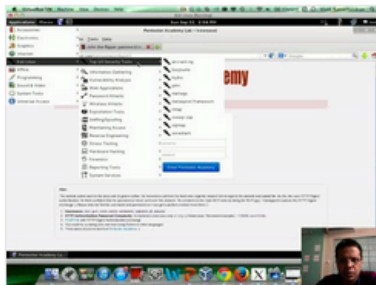
Revolutionizing Infosec Training

Highly Technical, Hands-on, Affordable

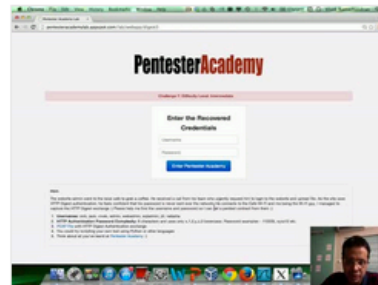
Start Learning Today!

Latest Videos

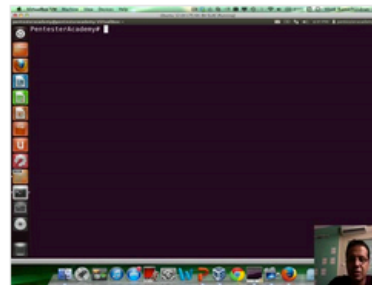
New content added weekly!



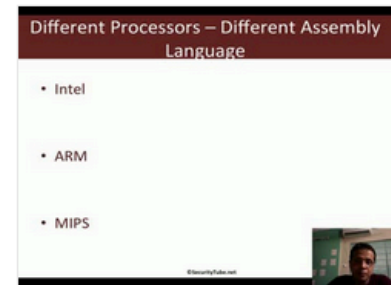
Challenge 7: Cracking Digest Authentication Solution in WAP Challenges



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