

# Network Pentesting

Vivek Ramachandran

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

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

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

# Pentesting Windows Endpoints: Impersonation

# Get list of Tokens – as securitytube

```
meterpreter > list_tokens -u
[-] Warning: Not currently running as SYSTEM, not all tokens will be available
          Call rev2self if primary process token is SYSTEM

Delegation Tokens Available
=====
securitytube-PC\securitytube

Impersonation Tokens Available
=====
No tokens available

meterpreter > █
```

# Get list of Tokens – as SYSTEM

```
meterpreter > list_tokens -u
```

```
Delegation Tokens Available
```

```
=====
```

```
NT AUTHORITY\LOCAL SERVICE  
NT AUTHORITY\NETWORK SERVICE  
NT AUTHORITY\SYSTEM  
securitytube-PC\securitytube
```

```
Impersonation Tokens Available
```

```
=====
```

```
NT AUTHORITY\ANONYMOUS LOGON
```

```
meterpreter >
```

# Incognito

## Incognito Commands

=====

Command	Description
-----	-----
add_group_user	Attempt to add a user to a global group with all tokens
add_localgroup_user	Attempt to add a user to a local group with all tokens
add_user	Attempt to add a user with all tokens
impersonate_token	Impersonate specified token
list_tokens	List tokens available under current user context
snarf_hashes	Snarf challenge/response hashes for every token

—

# Pentester Academy

PentesterAcademy

a SecurityTube.net initiative



TOPICS PRICING WHY SUBSCRIBE [MEMBER ACCESS](#)



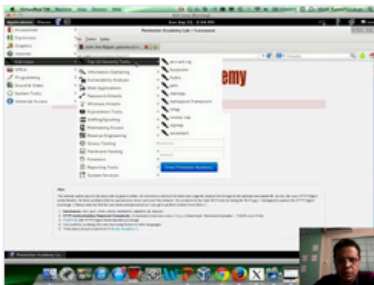
## Revolutionizing Infosec Training

Highly Technical, Hands-on, Affordable

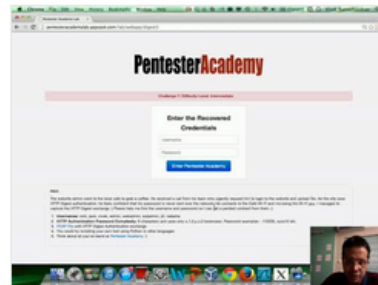
[Start Learning Today!](#)

## Latest Videos

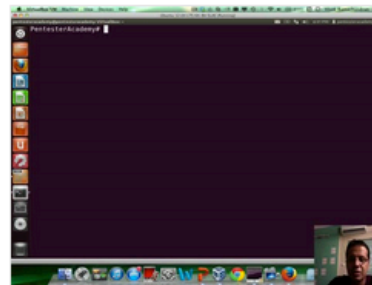
New content added weekly!



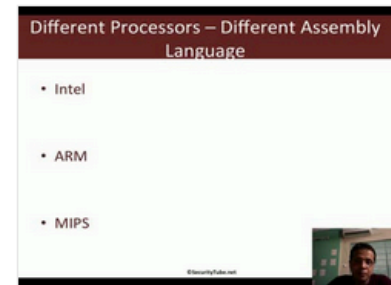
Challenge 7: Cracking Digest Authentication Solution in WAP Challenges



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