

# Course Objectives

After completing this course, students will be able to:

* Summarize the CTE squad's responsibilities, objectives, and deliverables from each CPT stage
* Analyze threat information
* Develop a Threat Emulation Plan (TEP)
* Generate mitigative and preemptive recommendations for local defenders
* Develop mission reporting
* Conduct participative operations

## • Conduct reconnaissance

• Analyze network logs for offensive and defensive measures 

# Course Objectives (Continued)

Students will also be able to:

* Analyze network traffic and tunneling protocols for offensive and defensive measures
* Plan non-participative operations using commonly used tools, techniques and procedures (TTPs)

# Module 2: Threat Emulation (Objectives)

## • Conduct reconnaissance

* Generate mission reports from non-participative operations  Plan a non-participative operation using social engineering
* Plan a non-participative operation using Metasploit
* Analyze network logs for offensive and defensive measures
* Analyze network traffic and tunneling protocols for offensive and defensive measures
* Plan a non-participative operation using Python
* Develop fuzzing scripts
* Develop buffer overflow exploits

# Module 2 — Lesson 6: File Transfer (Objectives)

* Describe standard methods of transferring files
* Conduct file transfers with netcat
* Conduct uncommon methods of file transfers

## Transferring Files

What are some methods used to transfer files?

• Raw methods (socat, netcat and others)

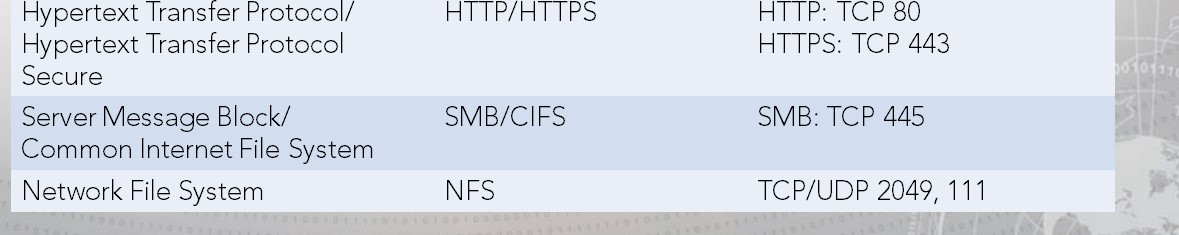
Common Name

Secure Copy Protocol/ SCP/SSH TCP 22

Secure Shell

File Transfer Protocol FTP TCP 20, 21

Trivial File Transfer Protocol TFTP TCP 69

Hypertext Transfer Protocol/ TCP 80

Hypertext Transfer Protocol TCP

## Transferring Files

Secure copy

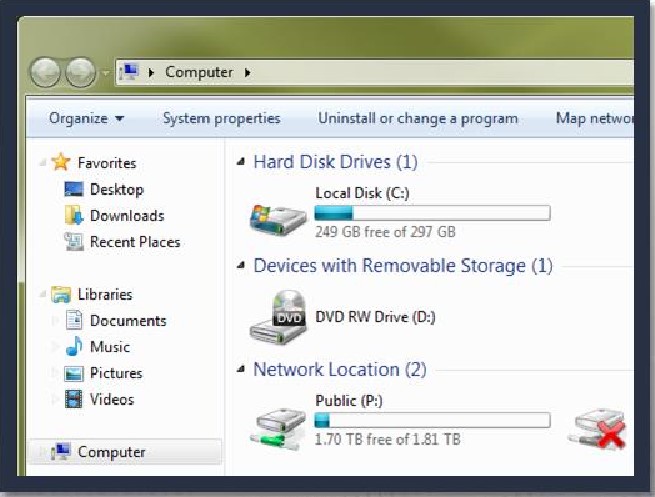
• scp [ [user@] src host: ] src file [ [user@] dst host: ] dst file



## Transferring Files

### Windows SMB

net use <drxve letter > : < sharename> / user: [domain] \ < username>



# Netcat

* Networking "Swiss Army knife"
* Can either initiate a TCP/UDP connection or bind to a port and listen for incoming connections

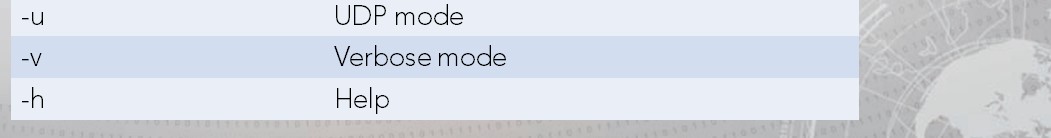
## Can be used for file transfers, banner grabbing, and port scanning

* Syntax varies depending on OS and Netcat version
* Netcat is not identical to ncat

## Common Options

-e <prog> Inbound execute program, often removed

Listen for inbound connections -p <port>



Local

port

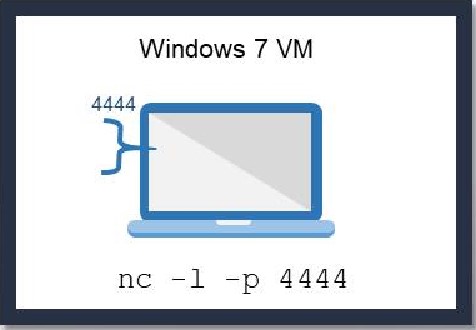
number

I

# Basic Netcat Usage

## Open a listening port on your Windows 7 VM

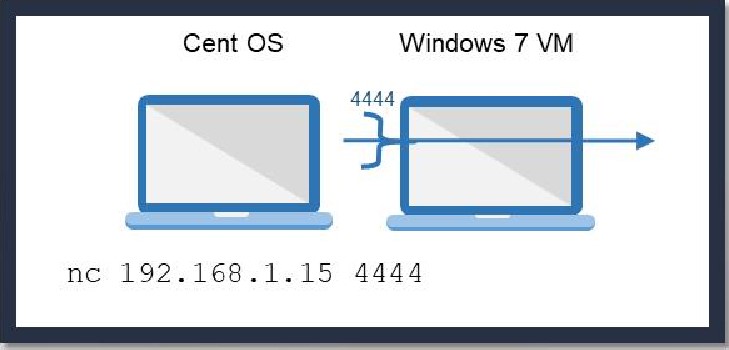
• Don't forget to check your syntax



How can we check to see if this port is listening?

# Basic Netcat Usage

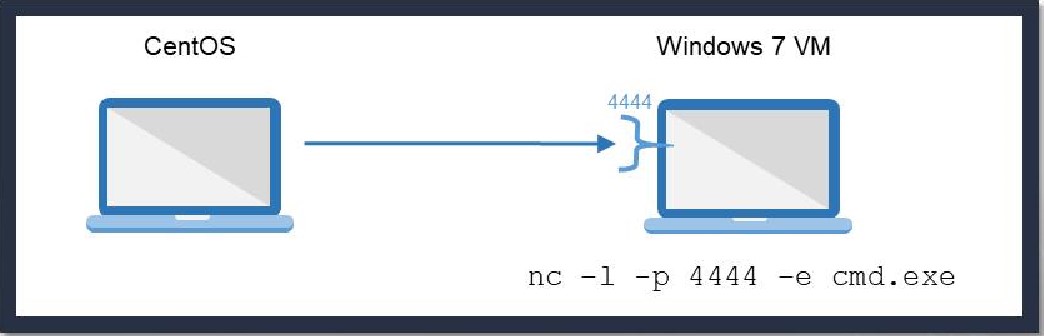
## Connect to Windows 7 VM from CentOS



Note: Use Ctrl+C to break out of the connection.

Using Netcat to Get a Remote Shell

Use the -e option to execute a program after connection.

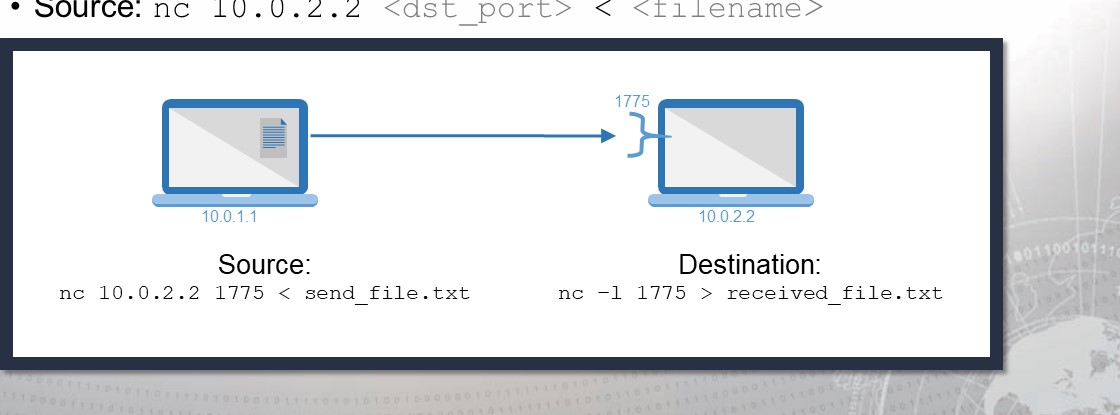


Ensure the nc version you are using has the —e option.

Transferring Files With Netcat

Forward transfer

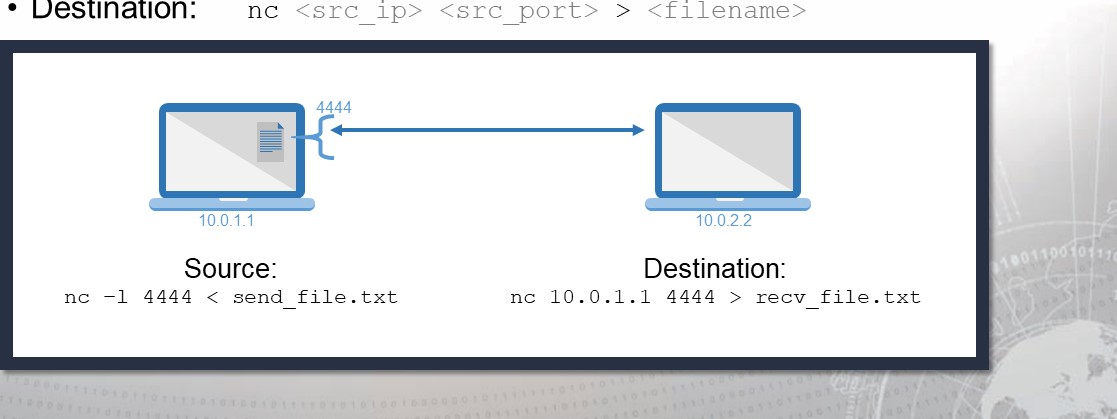
* Receiver sets up listener; sender calls forward
* Destination: nc -1 <dst port > < filename>

• Source: nc 10 . 0 .2 .2 <dst port > < filename>

Transferring Files With Netcat

Reverse transfer

* Sender sets up listener; receiver calls back
* Source: nc -1 <src port > < <filename>

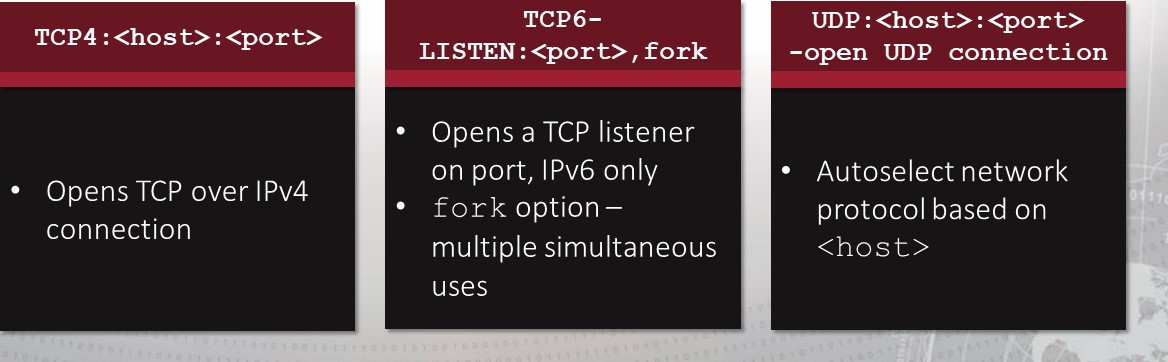


•

Destination:

## Socat

* Socat accepts two bidirectional byte streams and transfers data between them.
* Typical Examples:



## Transferring Files via Terminal

Sometimes all you have is a console window

* For example, telnet; shell from exploitation

Paste can copy text, but what about binaries?

* Need to encode as text, then paste and decode



* uuencode/uudecode—common on UNIX
* Interpreters on target—Perl, Python, Bash, GCC
* For example, perl has uudecode built in

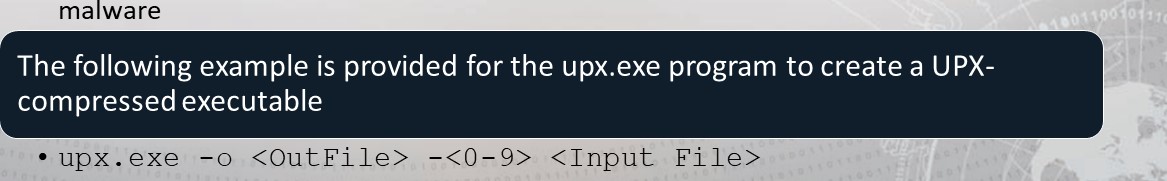
Packers



* Smaller-sized executable
* Different file hash



* Most antivirus software detects the presence of UPX packing and flags it as possible



Exercise: File Transfers

Objectives

After completing this exercise, students will be able to:

* Describe standard methods of transferring files
* Conduct file transfers with netcat
* Conduct uncommon methods of file transfers

Duration

This exercise will take approximately 2.5 hours to complete.

Exercise: File Transfers

|  |  |
| --- | --- |
|  | IP Address |

Note:

|  |  |
| --- | --- |
| Kali | 1@.10.1.6€ |
| Ubuntu | 10.10.1.7e |
| Windows 10 | 10.10.1.2e |
| Windows 7 | 10.10.1. 30 |

## Debrief

General Questions

* How did you feel about this section?
* Were there any areas in particular where you had difficulty?
* Do you understand how this relates to the work you will be doing?

# Summary

* One of an attacker's primary goals upon gaining entry to a targeted network is to establish a foothold and further the scope of the attack
* Tunneling and redirection permit an attacker to form channels of communication that would otherwise be impossible given existing infrastructure and setup
* Network defenders must understand these tools, tactics and procedures to gain a tactical advantage against attackers and prevent loss of critical data



|  |
| --- |
| End of Module 2, Lesson  6 |