#### Setting up the SSH Tunnel

This process enables you to connect from local host to a remote host residing on a different network



#### **Creating SSH Connection**

Host Name = Router's IP Address seen by local host. Port = 22 (SSH)

Saved Sessions = name as you please



#### Configuring Port<-->IP Mapping

Connection>SSH> select "Enable compression"

🕵 PuTTY Configuratio	n	
Category:		
🖃 Teminal		Options controlling SSH connections
···· Keyboard ···· Bell		Data to send to the server
Features		Remote command:
⊡ ·· Window Appearance Behaviour		Protocol options
		Enable compression     Preferred SSH protocol version:
⊡ Connection	=	○ 1 only ○ 1 ○ 2 ○ 2 only
Proxy		Encryption options
Telnet		Encryption cipher selection policy: AES (SSH-2 only)
SSH		Blowfish 3DES
Kex Auth TTY		wam below here Arcfour (SSH-2 only) DES
X11		Enable legacy use of single-DES in SSH-2
Tunnels Bugs	-	
About		Open Cancel

#### Connection>SSH> Tunnels>

Pully Configuration	on			
Category: Category: 	•	Options Port forwarding Local ports a Remote ports Forwarded ports: L33232 192: L33050 192: Add paw forward	controlling SSH p ccept connections do the same (SS : 168.1.232:3389 168.1.50:3389	ort forwarding s from other hosts H-2 only) Remove
Connection Data Proxy Telnet Rlogin SSH Kex Kex	III	Add new forward Source port Destination	ied port: 33050 192.168.1.50:3 Remote IPv4	Add 3389 O Dynamic O IPv6
TTY X11 Tunnels Bugs Serial	*		Open	Cancel

Note: the source port can be any number that does not create conflict with other source ports. Hence, make it a unique source port for each device and do not use any of the common TCP/UDP ports.

The following is a good convention for Source Port numbering.

```
Ex:
Source port: 33050 (33|050 = 33(1st 2 digits of RTP TCP socket, 3389 | 050(192.168.1.50))
Destination: 192.168.1.50:3389 (3389 = TCP socket for Remote Desktop Protocol))
```

Press Add



Note: You can add multiple mapping as long as the remote device is in the same remote network.



Load the tunnel you just created. It will log you on to the B1 server

📴 128.29.29.253 - PuTTY	
Thank you	
Note:	
Anything you store in the home directory on this machine is backed up	
nightly. If you accidentally delete something, give me a call and I can	
restore it for you in a couple of minutes. There are some limitations:	
2. Backups are only stored for the previous week and this week. These are not	
archives.	
3. Only the home partition on this machine (b1) is backed up. I recommend not	
storing vital information on the test machines for extended lengths of	
time.	
Jason (x37755)	
=== This machine is for official MITRE business only. ===	
To determine whether a file is a text file, executable, or some other type	=
of file, use	
file filename	
Dru Zappejedigtar cal	
[krbe@b1 ~1\$	
[krhee@b1 ~]\$	

## Setting up a RDP session

It should read:

Localhost:SourcePort# (must match the source port from PuTTY settings)

Computer: DISA\_Probe\_XP:33050

Your computer name must match the host name!

🔁 Remote Desktop Connection	RuTTY Configuration	
Remote Desktop Connection         Remote Desktop Connection         Computer:         Image: Desktop Connection         User name:         None specified         You will be asked for credentials when you connect.         Connect       Encel         Help       Options >>	PuTTY Configuration       X         Category:       Options controlling SSH port forwarding         - Keyboard       Port forwarding         - Realures       Options controlling SSH port forwarding         - Window       Category:         - Window       Remote ports accept connections from other hosts         - Repearance       Remote ports do the same (SSH-2 only)         Forwarded ports:       Remove         L23012       192.168.1.12:23         L33050       192.168.1.503389         - Colours       Add new forwarded port:         - Data       Source port	
	Image: Second control of the second control of th	

## Configuring the Hostname (Windows)

By Default, the host name should be "localhost". If you want it to be something different follow this instructions. Note: This is not required unless seeing "localhost" on the remote desktop connection really bothers you.

To have the desired name show for logging into RTP, you must change the host name of the local host name. Look for Host file under following directory:





Set local host = 127.0.0.1 If you want the name to match on the RDP window: The host file should match the login name:

📔 C:\Wi	indows\Sys	tem32\drivers\etc\l	hosts - Notepad++					
<u>File</u>	lit <u>S</u> earch	View Encoding	<u>Language</u> Settin	s Macro	Run Plugins <u>W</u> indow ?			Х
			hhiadia	h	2   12   <del>2</del>   <del>5</del>   1   <b>12</b>   0   1		. 🔻 🗷 🗔 🖖	
😑 chang	ge.log 📙	protected.html 📔	Recommend.txt 📙 ho	sts				
1	# Copyr	ight (c) 1993	3-2009 Microsof	t Corp.				
2	#							
3	# This	is a sample H	HOSTS file used	by Micro	soft TCP/IP for Windows.			
4	#							
5	# This	file contains	s the mappings	of IP add	iresses to host names. Each	L		
6	# entry	should be ke	ept on an indiv	idual lin	e. The IP address should			
7	# be pl	aced in the :	first column fo	llowed by	the corresponding host na	me.		
8	# The I	P address and	d the host name	should b	e separated by at least on	e		
10	# space							
11	# Addit	ionally com	ments (such as	these) ma	w he inserted on individua	1		
12	# lines	or following	n the machine r	ame denot	ed by a '#' symbol.	-		
13	#		g one maonine .	and action				
14	# For e	xample:						
15	#	-						
16	#	102.54.94.97	rhino.acme	.com	# source server			
17	#	38.25.63.10	x.acme.com	L	# x client host			
18								
19	# local	host name rea	solution is har	dled with	in DNS itself.			
20	# 127	.0.0.1	localhost					
21	# ::1		localhost			· · · · · ·		
22								
23	localho	st name resol	lution is hand	ed within	DNS itself.			
24	127	.0.0.1	Purple12					
25	127	.0.0.1	DISA_Probe_XP					
20								
27								
20								
Normal t	ext file		length : 949 line	s : 28	Ln:1 Col:1 Sel:0	Dos\Windows	ANSI	INS



# Windows --> CentOS (Cross Platform RDP)

Set Remote Desktop configs as follows:

On the Remote device (In this case CentOS Linux distro), configure as follows.

Preferences 🔸 🐱	Accessibility
File Edit View Termin 🔊 Administration 🔸 🕎	More Preferences
[Ixia@mm143307-pc ~] bash: ifconfig: comm [Ixia@mm143307-pc ~] ethl Link encap: About GNOME	About Me Desktop Background
inet addr:1	File Management · 🗐 ixia@mm143307-pc:~
UP BROADCAS	Fonts <u>File Edit View Terminal Tabs H</u> elp
RX packets: Dog Out ixia TX packets: OUL is ion of the second	Keyboard THIS SYSTEM IS FOR USE BY TELCHEMY PERSONNEL WITH SECURE SYSTEM ACCESS AUTHORITY ONLY. USE IS MONITORED BY TELCHEMY ITS.
Interrupt:58 Memory:Test0000-Te	Menus & loolbars Remote Desktop Preferences X
lo Link encap:Local Loopback inet addr:127.0.0.1 Mask:255.6 inet6 addr: ::1/128 Scope:Host UP LOOPBACK RUNNING MTU:16436 RX packets:1422 errors:0 dropp TX packets:1422 errors:0 dropp collisions:0 txqueulen:0 RX bytes:2270556 (2.1 MiB) TX	Mouse       Password:       Sharing         Network Proxy       Last login: Mon J Sun Microsystems -bash-3.005 su ro Password:       Allow other users to view your desktop         Remote Desktop       # ping 172.30.151 172.30.151       Image: Allow other users to control your desktop         your remote desktop access preferences       72.30.151
vmnetl Link encap:Ethernet HWaddr 00: inet addr:172.16.48.1 Bcast:17	Screen Resolution 172.30.151.71 1s Security # Screensaver 5 # Management of the security of
Screenshot- ixia@mm143307- pc:~.png	Sound # dvqwin Theme dvqwin: not found # exit Password:
	Volume Control     -bash-3.00\$ dvqwi       [1] 935       -bash-3.00\$         Windows         Bash-3.00\$         Windows         Yes          Yes

### Using VNC (Sharing View of current Session)

Allows remote party to share the view of the current login session



# Using NoMachine (Logging Into a Remote Machine)

Logging directly onto a remote machine. Use NoMachine Application as follows

Fill in login credentials of the remote system you are logging into. Session: notation for yourself. Description for the login.

III NX	_	. 🗆 🗙
NDM	ACHINE	
Login	ixia	
Password	******	
Session	Telchemy	-
	🔲 Login as a guest user	
Configure	Login <u>C</u> los	e

Host = Destination IP

Port = 22 (SSH)

Desktop = select OS						
🛄 NX - Telchemy 📃 🗆 🗙						
NOMACHINE						
General Advanced Services Environment About						
Server						
Host 172.30.151.68 Port 22						
Remember my password Key						
Desktop						
Unix GNOME Settings						
MODEM ISDN ADSL WAN LAN						
Display-						
Available area						
Use custom settings Settings						
Spread over multiple monitors						
Delete Save Dk Cancel						

Leave as default						
🔟 NX - Telchemy 📃 🔲 🗙						
NOMACHINE						
General Advanced Services Environment About						
Network						
Disable encryption of all traffic						
Disable ZLIB stream compression						
Connect through a HTTP proxy						
System						
Grab the keyboard when the client has focus						
Disable DirectDraw for screen rendering						
Disable deferred screen updates						
Cache:						
In memory 16 Mb 🔽 On disk 64 Mb 💌						
Remove all cache files						
Delete Save Dk Dancel						

#### Leave as default

📶 NX - Telchemy 📃	
NOMACHINE	
General Advanced Services Environment Ab	out
User NX directory	$\neg$
C:\Documents and Settings\Administrator\.nx	
Remove old session files	
System NX directory	
C:\Program Files\NX Client for Windows	
- Font server	
Use font server	
Host Port 7100	
Select NX fonts	
Default 8, MS Shell DI Fixed 8, Courier	
Delete Save Dk Cance	