SANS NetWars FAQ

-1) What do I need to play?

The day before the round starts, registered players will receive an email with download instructions.  There will be a link to an ISO 9660 CD-ROM image that can be burned to disk or virtualized and booted from.  VMware player is a free option for PCs available at <http://www.vmware.com/>.  Once you download the image, you can technically begin to hack, reverse-engineer, or otherwise find out how the image connects to the rest of the game.  Scoring actually starts 12:01 AM Pacific of the Round Start Date (Round 2.0 is scheduled from 12:01 AM August 17, 2009 to 11:59 PM August 23, 2009 Pacific Time).

Due to the high number of players, and the variety of email servers, you may not receive your download instructions sometime the 24 hours before the game starts.  If you have not received instructions by 12:01 AM on the start date, please feel free to send to an email to [netwars@sans.org](mailto:netwars@sans.org) requesting help.

0) Why is the game not working?

Each round is designed to play for about one week, you might be trying outside the schedule.  If a round is scheduled, and you are using a fresh ISO image for that round, you need to find out how the image is connecting to the game and break-in to that access.

If DNS seems to be failing, try using this IPv4 address (it shouldn't change this week) 65.173.218.209.  Anything else, please email the exact error message to netwars@sans.org and we'll see what we can do to help.

1) Am I limited to what tools I can use?

No, there are no tools that are banned.  Additional tools such as the latest firefox browser can be used on the downloaded image can be added with the appbrowser; you must have root privileges, though.  ;) Past the tunnel, there is limited space to force you to be creative in your tool selection.

2) My tool didn't exploit XXXX, why not?

Exploits fail for a variety of reasons, try them again, try adjusting settings, or maybe the vulnerability simply doesn't exist.  There are many tools in the game already, I suggesting finding them--they are in the game to help you play.

3) Why do I have to use Linux?

It is simply too logistically complicated to support Windows as a client desktop.  If you'd like to use an external operating system, then theoretically you could find the key and export it to something you are more comfortable with (try the dropbearconvert command in the image).  You can also create tunnels with the Linux image and use an external tool through the tunnel.

4) Why is FreeBSD a target?

FreeBSD was necessary to create a challenging environment but at least slightly familiar with MacOS X and Linux experienced users.  You may want to have a look at http://www.freebsd.org or <http://www.fresports.org> for examples of commands and tools.  Also don't forget to look at

/var/ports when you get into the game. Example command to add a package:

pkg\_add /var/ports/packages/whatever-2.5.tbz

If you do not have root access, you may try using the tarball or running your copy of the tool:

cd /home/backup; tar -xvjf /var/ports/packages/whatever-2.5.tbz

But remember, you will run out of space if you do not make wise choices, and only one target has all of the pre-compiled packages.

5) Why is there a Windows XP target?

Ok, now you are being silly--because it is a very likely target!

6) I am not used to this terminal, where do I start?

Useful things to type on various machines in the game:

ls -la

dir

pwd

cd %appdata%/..&cd

id

uname -a

set

winver

ipconfig

ifconfig

netstat -a|more

cat /etc/passwd

7) How do I find custom vulnerabilities in the game?

Look around, see what you can communicate with. What kinds of errors can you cause? If you don't know where to start, try looking at the websites with a text HTTP browser, view the source code and try bad data to see what it tells you about the website.

8) Why doesn't nmap work?

Nmap does work, but you must run it correctly.  Try using simple scans, then try difference command line options such as:

nmap -A 192.168.10.0/24

9) How do I make an HTTP request in the game?

You could use any external browser with a tunnel, google for ssh tunnels or find an in-game hint on how to do this.  Also, some machines have text browsers on them.  Ones you may want to try:

wget http://192.168.10.40/

fetch http://192.168.10.47/

GET http://192.168.10.51/

POST http://192.168.10.52/

echo "GET /" | nc 192.168.10.53 80 > 53\_index.html

a) Can I get a hint?

If you have a technical problem with the game play, email netwars@sans.org with QUESTION in the subject and we'll answer as soon as we can within reason.  IRC and jabber (XMMP) channel instructions will be included in the download instructions for interactive help.  There are also hints sprinkled throughout the game in various files (usually in user’s home directories) -- you will need to break into different accounts and machines to find them.

b) Is there a non-twitter scoreboard?

There is a live in-game scoreboard at TCP port 8888 on 192.168.10.110.

c) What are the rules (somebody keeps killing my processes or prevents me from doing what I want)?

That's the offensive and defensive nature of the game.  You need to be able to take preventive precautions in case somebody kills your process or connection.  If somebody figures out how to counter your attack on their process, then you better find a new attack or prevent them from preventing your attack . . .  The rules are simply that hosts 192.168.10.0/24, 192.168.11.0/24, 192.168.12.0/24, and 192.168.9.0/24 are fair game for attacking (anything inside our game on that network is fine (and once you download the ISO you can attack your copy of the ISO all you want).

d) Why am I not getting points?

Points are scored by placing a token in the “root” or banner of a service:

user::username

The “username” value must be 4-12 alphanumeric characters.  For example, when I test the game, I use “jimshew” as my username.  You can place this token hidden or in plain view on a default HTTP page, in the banner on an FTP server, or in a username field in an SQL table.

There will be a list of bonus points that will ask questions about the environment for various bonus points mid-game.  These tasks must be received to [netwars@sans.org](mailto:netwars@sans.org) with the Subject of BONUS ITEMS before the end of the round to be counted.  A sneak peek of three questions, from simple to hard:

* Enter the password of the “sales” account:
* Enter the salt used for md5 hashing in mysql server used by the HTTP sites on 192.168.10.51-55 (re-read this carefully):
* Enter the shortest length of keystrokes to go from the “tc” account to the “root” account on the ISO image:

e) What’s the NetWars status?

NetWars Round 2.0 will run August 17th, 12:01 AM through August 23rd, 11:59 PM Pacific Time.  You can follow <http://twitter.com/sansnetwars/> but to give you an idea, Round 2.0 centers around:

* 4 Target networks (even WEP!)
* 8 Target Appliance/devices (routers, VOIP, etc.)
* 24 Target hosts
* Various new and classic Server and Client vulnerabilities
* Even more BONUS challenges (to be released August 20th)

f) Can we play in teams?

NetWars is designed to be played by individuals.  There is nothing preventing people from helping each other out, but points will be awarded based on the token keys placed.  Each player should still have their own registration and their own image (excessive external connections with the same account have \*interesting\* results).