SANS SKILLS QUEST

BY NETWARS - CORE EDITION

Inside the Challenges

RANGE FACTS	DETAILS
Sections/Chapters	**31 and growing**
Total challenges	**Over 200 and growing**
Total points available	**4000+**
Difficulty mix	**56% Beginner | 37% Intermediate | 6% Advanced | 1% Extreme**
Deployment	Browser-based; 6 and 12-month subscriptions available
Reporting	Score dashboard highlights individual achievements and overall progress.

What Each Section Teaches & Measures

SECTION	CORE SKILLS ASSESSED	TYPICAL ROLES
Linux Labyrinth	Shell navigation, process & network basics	Jr SOC, SysAdmin
ELK SIEM Log Analysis	Threat-hunt in Elastic, event-ID triage, host ↔ network pivots	SOC Tier 1-2, Threat Hunter
Linux Binary Analysis	/proc forensics, open-file & socket discovery, malware triage	DFIR, Malware Analyst
Galileo's Enigma	Encoding, password attacks, SSH/FTP enum	Blue/Red Hybrid
Come Watson – CTI	OSINT fundamentals, actor profiling	CTI Analyst

CYBER RANGE

SANS SKILLS QUEST

BY **NETWARS** - CORE EDITION

SECTION	CORE SKILLS ASSESSED	TYPICAL ROLES
Grace's Debugger Platform	Windows debugging, credential-theft detection	DFIR, Win IR
PowerShell Assault	PS recon & automation, web requests, CSV parsing	Blue Team, Win Admin
Filament Foolery	Web enumeration, TLS cert review, Python scripting	AppSec, DevSecOps
Terminal Treasure Hoard	Packet filters, regex, fuzzing, GPG, privilege escalation	Red/Blue Senior
Seven Deadly Crypto Sins	Real-world crypto errors (ECB, reuse, entropy)	App Pentest, Crypto Eng
Feistel's ECB School	Block-cipher internals, padding-oracle exploits	Crypto Research
Zeek	Network forensics via Zeek scripting & logs	NDR Engineer, DFIR
The Elf C0de	Python logic, type casting, control flow puzzles	DevSecOps
Cloud Command Lines	AWS/Azure CLI, IMDS abuse, creds handling	Cloud Engineer
Packet Analysis 101/201	PCAP triage, exfil detection, TShark, WPA/WEP	SOC Tier 1-3
SegFault Society	Log slicing, memory-corruption indicators	App Security
Ada Lovelace – Assembly	x64 shellcode, syscall crafting	Exploit Dev
Sort-O-Matic / Get Big	Bash sort/uniq, log mining at scale	Data Ops
Cabal Tracker	Graph-query CTI, link analysis	Threat Intel
Cloud Storage	S3 enum, pickle deserialization RCE	Cloud Security
Employee Search	People OSINT, QR-code analysis	HR Security
Webmail	Phishing-kit reverse engineering	Email Analyst
Admin Tools	Admin shares, RDP security, tool misuse	SysAdmin

CYBER RANGE

SANS SKILLS QUEST

BY NETWARS - CORE EDITION

SECTION	CORE SKILLS ASSESSED	TYPICAL ROLES
Domain Registrar	DNS/WHOIS tamper detection	DNS Ops
Depot – Marshal or aMaze	Deserialization & fuzzing RCE	AppSec, Red Team
WAFfle Time!	WAF bypass, HTTP smuggling	Web Pentest
Infiltrating Ancient Ruins	Advanced search-string OSINT	Red Team
Get a Job	Social-eng résumé bait	Sec-Awareness
USB HIDden	USB packet crafting, HID injection	DFIR
Sort-O-Matic	Quick log sorting (awk/uniq)	SOC Tier 1
Get Big	Regex on large data sets	Data Engineer

Mapped SANS Courses:
SEC301/401 (fundamentals), SEC503/504 (blue-team and IR), SEC560/575/760 (red-team), FOR500/508/572 (forensics), SEC488 (cloud), SEC660/663 (exploit & crypto), FOR578 (CTI), plus others per section.

Why Customers Choose Skills Quest – Core Edition

- ✓ **Role coverage** – challenges map to SOC Tier 1-3, Threat Hunt, DFIR, AppSec, Cloud, and Red Team tracks.
- ✓ **Immediate ROI** – validates the skills you've mastered and the capabilities you can immediately apply on the job. It also provides SANS course recommendations to accelerate your career growth and strengthen your organization's defenses.
- ✓ **Safe, repeatable labs** – browser-delivered; practice safely in an isolated, cloud-based environment — no software installation required.
- ✓ **Objective metrics** – executives receive dwell-time, success-rate, and discipline-heat-map dashboards.
- ✓ **Flexible delivery** – self-paced (6 or 12 month access)

Ready to see SANS Skills Quest by NetWars in action?

Contact sales@sans.org to arrange a live demo or pilot license for your team.

SANS