



Certified Snort Professional VS-1148

Vskills Certifications

Vskills Brochure



Skills for a secure future

Certified Snort Professional

Certification Code VS-1148

Vskills certification for Snort Professional assesses the candidate as per the company's need for network security and assessment. The certification tests the candidates on various areas in installing and running Snort, building IDS, Plug-ins, logging, alerts, log analysis, rules, signatures, preprocessing Snortsnarf and other usage of Snort.

Why should one take this certification?

This Course is intended for professionals and graduates wanting to excel in their chosen areas. It is also well suited for those who are already working and would like to take certification for further career progression.

Earning Vskills Snort Professional Certification can help candidate differentiate in today's competitive job market, broaden their employment opportunities by displaying their advanced skills, and result in higher earning potential.

Who will benefit from taking this certification?

Job seekers looking to find employment in networking, security or IT departments of various companies, students generally wanting to improve their skill set and make their CV stronger and existing employees looking for a better role can prove their employers the value of their skills through this certification.

Test Details

- **Duration:** 60 minutes
- **No. of questions:** 50
- **Maximum marks:** 50, Passing marks: 25 (50%)

There is no negative marking in this module.

Fee Structure

Rs. 3,499/- (Excludes taxes)*

*Fees may change without prior notice, please refer <http://www.vskills.in> for updated fees

Companies that hire Vskills Snort Professional

Snort Professionals are in great demand. Companies specializing in network security or network management are constantly hiring skilled Snort Professionals. Various public and private companies also need Snort Professionals for their networking, security or IT departments.

Table of Contents

1. Installation and Optimization

- 1.1 Introduction
- 1.2 Installing Snort from Source
- 1.3 Installing Snort
- 1.4 Upgrading Snort
- 1.5 Monitoring Multiple Network Interfaces
- 1.6 Invisibly Tapping a Hub
- 1.7 Invisibly Sniffing Between Two Network Points
- 1.8 Invisibly Sniffing MB Ethernet
- 1.9 Sniffing Gigabit Ethernet
- 1.10 Tapping a Wireless Network
- 1.11 Positioning Your IDS Sensors
- 1.12 Capturing and Viewing Packets
- 1.13 Logging Packets That Snort Captures
- 1.14 Running Snort to Detect Intrusions
- 1.15 Reading a Saved Capture File
- 1.16 Running Snort as a Linux Daemon
- 1.17 Running Snort as a Windows Service
- 1.18 Capturing Without Putting the Interface into Promiscuous Mode
- 1.19 Reloading Snort Settings
- 1.20 Debugging Snort Rules
- 1.21 Building a Distributed IDS

2. Logging, Alerts, and Output Plug-ins

- 2.1 Introduction
- 2.2 Logging to a File Quickly
- 2.3 Logging Only Alerts
- 2.4 Logging to a CSV File
- 2.5 Logging to a Specific File
- 2.6 Logging to Multiple Locations
- 2.7 Logging in Binary
- 2.8 Viewing Traffic While Logging
- 2.9 Logging Application Data
- 2.10 Logging to the Windows Event Viewer
- 2.11 Logging Alerts to a Database
- 2.12 Installing and Configuring MySQL
- 2.13 Configuring MySQL for Snort
- 2.14 Using PostgreSQL with Snort and ACID
- 2.15 Logging in PCAP Format (TCPDump)
- 2.16 Logging to Email
- 2.17 Logging to a Pager or Cell Phone
- 2.18 Optimizing Logging
- 2.19 Reading Unified Logged Data

- 2.20 Generating Real-Time Alerts
- 2.21 Ignoring Some Alerts
- 2.22 Logging to System Logfiles
- 2.23 Fast Logging
- 2.24 Logging to a Unix Socket
- 2.25 Not Logging
- 2.26 Prioritizing Alerts
- 2.27 Capturing Traffic from a Specific TCP Session
- 2.28 Killing a Specific Session

3. Rules and Signatures

- 3.1 Introduction
- 3.2 How to Build Rules
- 3.3 Keeping the Rules Up to Date
- 3.4 Basic Rules You Shouldn't Leave Home Without
- 3.5 Dynamic Rules
- 3.6 Detecting Binary Content
- 3.7 Detecting Malware
- 3.8 Detecting Viruses
- 3.9 Detecting IM
- 3.10 Detecting PP
- 3.11 Detecting IDS Evasion
- 3.12 Countermeasures from Rules
- 3.13 Testing Rules
- 3.14 Optimizing Rules
- 3.15 Blocking Attacks in Real Time
- 3.16 Suppressing Rules
- 3.17 Thresholding Alerts
- 3.18 Excluding from Logging
- 3.19 Carrying Out Statistical Analysis

4. Preprocessing

- 4.1 Introduction
- 4.2 Detecting Stateless Attacks and Stream Reassembly
- 4.3 Detecting Fragmentation Attacks and Fragment Reassembly with Frag
- 4.4 Detecting and Normalizing HTTP Traffic
- 4.5 Decoding Application Traffic
- 4.6 Detecting Port Scans and Talkative Hosts
- 4.7 Getting Performance Metrics
- 4.8 Experimental Preprocessors
- 4.9 Writing Your Own Preprocessor

5. Administrative Tools

- 5.1 Introduction
- 5.2 Managing Snort Sensors
- 5.3 Installing and Configuring IDScenter

- 5.4 Installing and Configuring SnortCenter
- 5.5 Installing and Configuring Snortsnarf
- 5.6 Running Snortsnarf Automatically
- 5.7 Installing and Configuring ACID
- 5.8 Securing ACID
- 5.9 Installing and Configuring Swatch
- 5.10 Installing and Configuring Barnyard
- 5.11 Administering Snort with IDS Policy Manager
- 5.12 Integrating Snort with Webmin
- 5.13 Administering Snort with HenWen
- 5.14 Newbies Playing with Snort Using EagleX

6. Log Analysis

- 6.1 Introduction
- 6.2 Generating Statistical Output from Snort Logs
- 6.3 Generating Statistical Output from Snort Databases
- 6.4 Performing Real-Time Data Analysis
- 6.5 Generating Text-Based Log Analysis
- 6.6 Creating HTML Log Analysis Output
- 6.7 Tools for Testing Signatures
- 6.8 Analyzing and Graphing Logs
- 6.9 Analyzing Sniffed (Pcap) Traffic
- 6.10 Writing Output Plug-ins

7. Other Uses

- 7.1 Introduction
- 7.2 Monitoring Network Performance
- 7.3 Logging Application Traffic
- 7.4 Recognizing HTTP Traffic on Unusual Ports
- 7.5 Creating a Reactive IDS
- 7.6 Monitoring a Network Using Policy-Based IDS
- 7.7 Port Knocking
- 7.8 Obfuscating IP Addresses
- 7.9 Passive OS Fingerprinting
- 7.10 Working with Honeypots and Honeynets
- 7.11 Performing Forensics Using Snort
- 7.12 Snort and Investigations
- 7.13 Snort as Legal Evidence in the U.S.
- 7.14 Snort as Evidence in the U.K.
- 7.15 Snort as a Virus Detection Tool
- 7.16 Staying Legal

Sample Questions

1. What type of alert is logged by Snort by default?

- A. All
- B. Full
- C. Complete
- D. None of the above

2. What does the class type refers to as a part of a Snort rule?

- A. Where to look for connection
- B. Priority helper
- C. Unique number
- D. None of the above

3. Which of the following is the comment section in a Snort rule?

- A. Class type
- B. Direction
- C. Message
- D. None of the above

4. What is the name of default Snort rule updater?

- A. Oinkmaster
- B. Updater
- C. Snortupdater
- D. None of the above

5. Which of the following may indicate malware infection in network?

- A. DNS queries to gator.com
- B. HTTP to yahoo.com
- C. HTTP to google.com
- D. None of the above

Answers: 1 (B), 2 (B), 3 (C), 4 (A), 5 (A)

Certifications

➤ Accounting, Banking and Finance

- Certified AML-KYC Compliance Officer
- Certified Business Accountant
- Certified Commercial Banker
- Certified Foreign Exchange Professional
- Certified GAAP Accounting Standards Professional
- Certified Financial Risk Management Professional
- Certified Merger and Acquisition Analyst
- Certified Tally 9.0 Professional
- Certified Treasury Market Professional
- Certified Wealth Manager

➤ Big Data

- Certified Hadoop and Mapreduce Professional

➤ Cloud Computing

- Certified Cloud Computing Professional

➤ Design

- Certified Interior Designer

➤ Digital Media

- Certified Social Media Marketing Professional
- Certified Inbound Marketing Professional
- Certified Digital Marketing Master

➤ Foreign Trade

- Certified Export Import (Foreign Trade) Professional

➤ Health, Nutrition and Well Being

- Certified Fitness Instructor

➤ Hospitality

- Certified Restaurant Team Member (Hospitality)

➤ Human Resources

- Certified HR Compensation Manager
- Certified HR Staffing Manager
- Certified Human Resources Manager
- Certified Performance Appraisal Manager

➤ Office Skills

- Certified Data Entry Operator
- Certified Office Administrator

➤ Project Management

- Certified Project Management Professional

➤ Real Estate

- Certified Real Estate Consultant

➤ Marketing

- Certified Marketing Manager

➤ Quality

- Certified Six Sigma Green Belt Professional
- Certified Six Sigma Black Belt Professional
- Certified TQM Professional

➤ Logistics & Supply Chain Management

- Certified International Logistics Professional
- Certified Logistics & SCM Professional
- Certified Purchase Manager
- Certified Supply Chain Management Professional

➤ Legal

- Certified IPR & Legal Manager
- Certified Labour Law Analyst
- Certified Business Law Analyst
- Certified Corporate Law Analyst

➤ Information Technology

- Certified ASP.NET Programmer
- Certified Basic Network Support Professional
- Certified Business Intelligence Professional
- Certified Core Java Developer
- Certified E-commerce Professional
- Certified IT Support Professional
- Certified PHP Professional
- Certified Selenium Professional
- Certified SEO Professional
- Certified Software Quality Assurance Professional

➤ Mobile Application Development

- Certified Android Apps Developer
- Certified iPhone Apps Developer

➤ Security

- Certified Ethical Hacking and Security Professional
- Certified Network Security Professional

➤ Management

- Certified Corporate Governance Professional
- Certified Corporate Social Responsibility Professional

➤ Life Skills

- Certified Business Communication Specialist
- Certified Public Relations Officer

➤ Media

- Certified Advertising Manager
- Certified Advertising Sales Professional

➤ Sales, BPO

- Certified Sales Manager
- Certified Telesales Executive

& many more job related certifications

Contact us at :

Vskills

011-473 44 723 or info@vskills.in

www.vskills.com