Blue Team Level 1 Certification (Standard)
1 Topic
Soft Skills
7 Topics
Security Controls
5 Topics | 1 Quiz
Networking 101
6 Topics | 1 Quiz
Section Introduction, Networking 101
Network Fundamentals
The OSI Model
Network Devices
Network Tools
Ports and Services
Activity) End of Section Review, Networking 101
Management Principles
4 Topics | 1 Quiz
PHISHING ANALYSIS DOMAIN
PA1) Introduction to Emails and Phishing
7 Topics | 1 Quiz
PA2) Types of Phishing Emails
10 Topics | 2 Quizzes
PA3) Tactics and Techniques Used
12 Topics | 2 Quizzes
PA4) Investigating a Phishing Email
8 Topics | 2 Quizzes
PA5) Analysing URLs, Attachments, and Artifacts
8 Topics | 1 Quiz
PA6) Taking Defensive Actions
12 Topics | 1 Quiz
PA7) Report Writing
7 Topics | 1 Quiz
PA8) Phishing Response Challenge
3 Topics | 1 Quiz
THREAT INTELLIGENCE DOMAIN
TI1) Introduction to Threat Intelligence
7 Topics
TI2) Threat Actors & APTs
6 Topics | 2 Quizzes
TI3) Operational Threat Intelligence
7 Topics | 1 Quiz
TI4) Tactical Threat Intelligence
7 Topics | 2 Quizzes
TI5) Strategic Threat Intelligence
5 Topics | 1 Quiz
TI6) Malware and Global Campaigns

Ports and Services

The purpose of this lesson is to introduce you to what ports and services are, and some common protocols and services that you should become familiar with for general IT, networking, and cybersecurity usage.

WHAT ARE PORTS & SERVICES?

In computer networking a port is a communication endpoint. At the software level a port identifies a specific process or a type of network service. The port numbers are divided into three ranges; well-known ports, registered ports, and private ports.

- **Well-known ports** range from 0 to 1023. This is where some of the most common ports are, such as FTP, SSH, DNS, and HTTPS. We will cover more of these below.
- **Registered ports** range from 1024 to 49151.
- **Private ports** range from 49152 to 65535. These are typically used for "ephemeral" ports, which is the name given to the source port used by a client in a server-client communication. For example, if we're connecting to a web server on port 443 HTTPS (destination port) then our source port would be a random port between 49152 to 65535.

Now let's jump into some of the most common and important ports and services. You can find a complete list of ports here.

Port 20, 21 – File Transfer Protocol (FTP)

This protocol is used to transfer files between systems, where users can connect to an FTP product and can view, upload, or download them. An example of usage would be a company using a server for file storage, where employees can connect in via FTP and retrieve files. FTP is extremely insecure as the communication is in clear text, including the username and password used, which can easily be captured by attackers that are listening to network traffic.

Port 22 – Secure Shell (SSH)

SSH allows users to connect to a remote host, such as a server, if they have SSH open. This channel is encrypted, so any data moved between two connected systems will not be clearly visible. An example of usage would be an IT technician using SSH to connect to a server from their desktop to carry out maintenance.

Port 23 – Telnet

This service was used before SSH, and offers the same functionality, however, Telnet does not use encryption, so the traffic can be captured and read by an attacker. Telnet should not be used due to this weakness, and SSH should always be implemented instead.

6 Topics | 1 Quiz

DIGITAL FORENSICS DOMAIN

DF1) Introduction to Digital Forensics
5 Topics

DF2) Forensics Fundamentals
10 Topics | 5 Quizzes

DF3) Digital Evidence Collection
8 Topics | 1 Quiz

DF4) Windows Investigations
3 Topics | 3 Quizzes

DF5) Linux Investigations
4 Topics | 2 Quizzes

DF6) Volatility
3 Topics | 1 Quiz

DF7) Autopsy
4 Topics | 1 Quiz

SECURITY INFORMATION AND EVENT MANAGEMENT DOMAIN

SI1) Introduction to SIEM
7 Topics | 1 Quiz

SI2) Logging
6 Topics | 2 Quizzes

SI3) Aggregation
2 Topics | 1 Quiz

SI4) Correlation
6 Topics | 1 Quiz

SI5) Using Splunk
5 Topics | 2 Quizzes

INCIDENT RESPONSE DOMAIN

IR1) Introduction to Incident Response
8 Topics | 1 Quiz

IR2) Preparation Phase
10 Topics | 3 Quizzes

IR3) Detection and Analysis Phase
7 Topics | 5 Quizzes

IR4) Containment, Eradication, and Recovery Phase
5 Topics | 1 Quiz

IR5) Lessons Learned and Reporting
7 Topics

IR6) MITRE ATT&CK
13 Topics | 2 Quizzes

BTL1 EXAM

Exam Preparation

Using RDP and SSH

How to Start Your Exam

always be implemented instead.

Port 25 – Simple Mail Transfer Protocol (SMTP)

This protocol is used to send emails between servers within the network, or to external networks, such as over the internet. This is just a transport method, to actually download and view emails you need to use an email client and the protocol POP or IMAP.

Port 53 – Domain Name System (DNS)

DNS operates on TCP and UDP ports 53 and uses relational databases to convert human-readable hostnames and domain names (such as Google.com) into their respective IP addresses so that communications can be sent to and from these hosts. The reason we use domain names is because they're easy to remember. You remember **securityblue.team**, but you probably won't remember **3.9.68.12**!

Port 67, 68 – Dynamic Host Configuration Protocol (DHCP)

DHCP is designed to assign IP address-related information to any hosts on the network automatically, such as the subnet mask and IP address. When you connect your phone to your network, it is being assigned an IP on the network because of the dynamic host configuration protocol. DHCP uses 2 ports; UDP port 67 and UDP port 68.

Port 80 – Hypertext Transfer Protocol (HTTP)

HTTP allows clients (browsers such as Chrome and Firefox) to connect to web servers and request content, which appears in the form of file downloads, web pages, and streaming services. So if you want to view the securityblue.team homepage, your browser will make a HTTP request to our web server, requesting to download the HTML web page. The server will respond with a 200 status code (which means "OK", it has been successful) and then send the HTML page to the client, so you can view it on your screen. As HTTP is not encrypted, it is possible to conduct sniffing attacks and see cleartext data as it is transmitted between the client and the server, such as passwords.

Port 443 – Hypertext Transfer Protocol Secure (HTTPS)

HTTPS is a secure version of HTTP and has the same functionality of retrieving content from web servers. However, the difference between the two is that HTTPS uses encryption to protect the transfer of data between a web server and a client. How do you turn HTTP into HTTPS? You need to use Transport Layer Security (TLS) formerly known as Secure Socket Layer (SSL). Sites that use HTTPS are less susceptible to man-in-the-middle and sniffing attacks.

Port 514 – Syslog (UDP)

A Syslog server will have port 514 open and listening for incoming Syslog notifications, transported by UDP protocol packets. These packets are generated by remote systems that have been set up to forward Syslog information to the server. This is typically used to send information about IT systems to a SIEM platform so that devices can be monitored for security events or issues.

Want to test your knowledge?

We recommend using the following online port quiz if you want to test your knowledge of port numbers.

In the next section, we will cover some of the basic Network tools that are used, as well as highlighting one of the most common port-scanning application Nmap and an example of how Nmap can be used to conduct a port scan on a website.

Privacy & Cookies Policy

Privacy - Terms