

Blue Team Level 1 Certification  
(Standard)

## Introduction to BTL1

Welcome to Blue Team Level 1!

4 Topics

Lab and Forum Access

## SECURITY FUNDAMENTALS DOMAIN

Introduction to Security Fundamentals

1 Topic

Soft Skills

7 Topics

Security Controls

5 Topics 1 Quiz

Networking 101

6 Topics 1 Quiz

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 &amp; APTs

6 Topics 2 Quizzes

TI3) Operational Threat Intelligence

7 Topics 1 Quiz

TI4) Tactical Threat Intelligence

7 Topics 1 Quiz

TI5) Strategic Threat Intelligence

5 Topics 1 Quiz

TI6) Malware and Global Campaigns

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

## Using RDP and SSH

Blue Team Level 1 Certification (Standard) &gt; Using RDP and SSH

IN PROGRESS



Within the BTL1 exam students will be required to access other systems over the network using both Remote Desktop Protocol (RDP) and Windows Secure Copy (WinSCP, which uses SSH). The below guides will teach you how to use these tools if you're unfamiliar, helping you save time in your exam attempt.

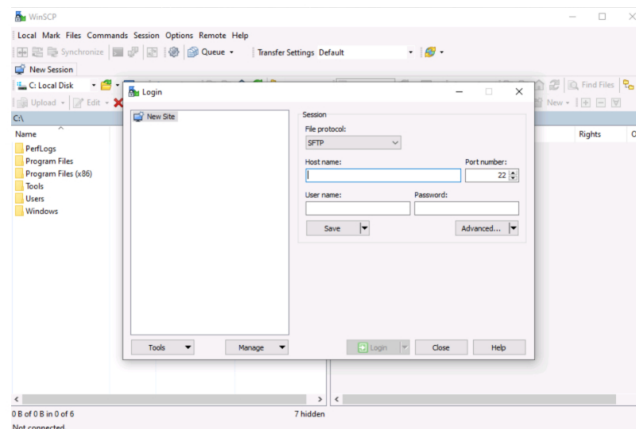
## WINDOWS SECURE COPY

If you've never used SSH to connect from one system to another, don't worry. Below is a short guide on how to connect to a linux-based system (in this case Ubuntu) from a Windows system using WinSCP (a client that allows SSH from Windows to Linux). You will be using WinSCP in the BTL1 exam to access other systems, so ensure that you are familiar with using it to prevent losing time in the exam.

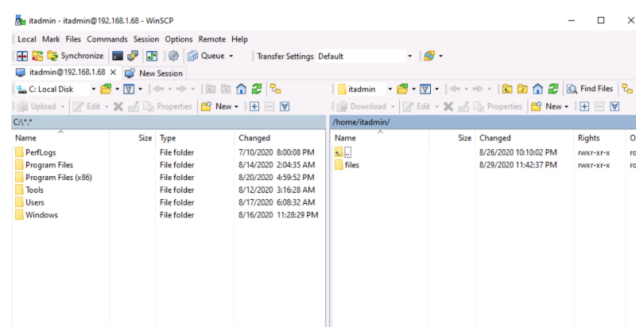
There's a few pieces of information that we need to know before we can connect to the remote system:

- File Protocol to use (sFTP, SCP, + others)
- Remote system IP address
- Port (standard is TCP port 22)
- Valid username
- Valid password

To initiate the connection, we need to launch WinSCP which will open the following windows:



We can see that we're prompted for the information we stated above. Once all fields have been filled in we can click 'Login' to initiate the connection. In the below screenshot you can see we now have access to the file structure of the remote system, allowing us to browse files. We can also right-click directories or files to download them to our local system.



- DF7) Autopsy
- 4 Topics 1 Quiz

## SECURITY INFORMATION AND EVENT MANAGEMENT DOMAIN

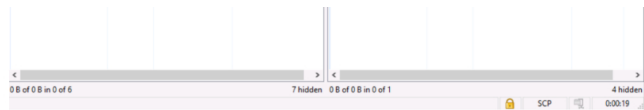
- SI1) Introduction to SIEM
- 7 Topics 1 Quiz
- SI2) Logging
- 6 Topics 2 Quizzes
- SI3) Aggregation
- 2 Topics 1 Quiz
- SI4) Correlation
- 6 Topics 1 Quiz
- SI5) Using Splunk
- 5 Topics 2 Quizzes

## INCIDENT RESPONSE DOMAIN

- IR1) Introduction to Incident Response
- 8 Topics 1 Quiz
- IR2) Preparation Phase
- 10 Topics 2 Quizzes
- IR3) Detection and Analysis Phase
- 7 Topics 4 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



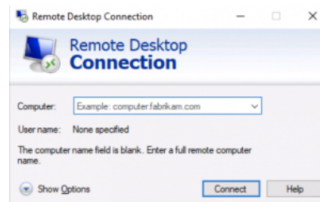
# REMOTE DESKTOP PROTOCOL

Similar to how SSH works, RDP is a method for connecting from one Windows-based system to another providing a graphical user interface. Below is a short guide on how to connect from one Windows system to another using RDP. You will be using this method in the exam to access other systems, so ensure that you are familiar with using it to prevent losing time in the exam.

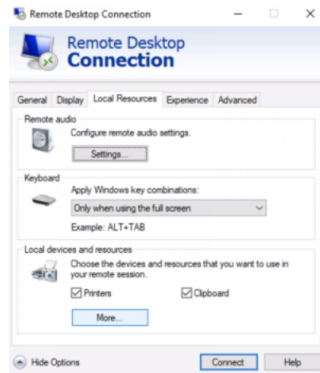
Before we can connect to another system using RDP, we need the following information:

- Remote system IP address
- Valid username
- Valid password

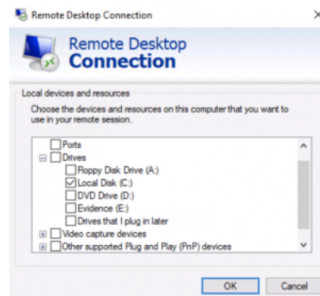
Once you open RDP via a shortcut or from the Windows search bar, the following window will appear:



One interesting thing we can do with RDP is create a link between a hard drive on our local system so that it can be accessed from the remote system. This is great for pulling files back to our system for later analysis. To do this, first click on 'Show Options' at the bottom of the Window. Next click on the 'Local Resources' tab and click the 'More...' button at the bottom.

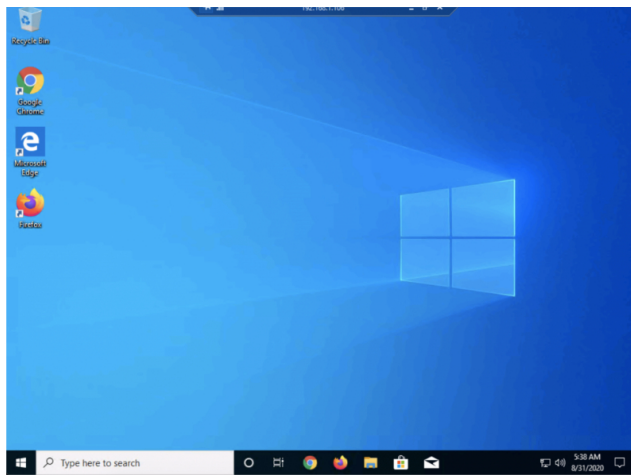


If you expand the Drives section we can toggle the C: drive, which means it will now be available through our RDP session!

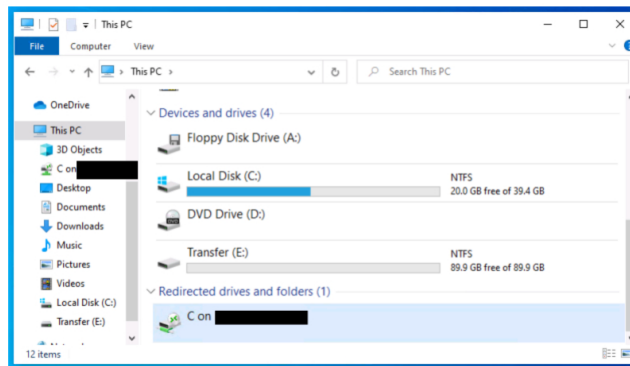


Once we initiate the connection, it'll look as if you're actually on the system itself! The only difference is the toolbar at the top of the Window.





As mentioned before, we have mapped our local C: drive, so let's head over to This PC to confirm we can access it.



We can see the local drives on the remote system at the top, then down the bottom we have the C: drive on our local system. We can now copy files from the remote system to that drive, and then access them once we close the RDP session!

[< Previous Lesson](#)[Mark Complete ✓](#)[Next Lesson >](#)[Back to Course](#)[Privacy & Cookies Policy](#)