# **Performance Assessment: Session Hijacking and IDS and Firewall Evasion Techniques**

In this Performance Assessment, you will perform the tasks you have been taught in the Guided Practices (iLabs content from EC-Council). You may use the book and any notes you have. You may look at your prior labs. You may not give or receive help from other students. You may ask your instructor for assistance, but it is likely to cost points.

# How does this practical lab apply in the real world?

Most important communications that occur on the web take place within a session. These sessions are usually authenticated and encrypted. As a penetration tester, you will need to know how to test for and exploit the vulnerabilities in these sessions to determine the risk to an organization.

Most all organizations will use both firewalls and IDS/IPS systems to protect their networks. This makes it imperative that you, as a penetration tester, test these systems and know the common methods used to evade or circumvent them.

In this activity, you will be assessed on your ability to use common tools to hijack a session and evade IDS and firewalls. Document your findings thoroughly, through screenshots and well-written paragraphs that describe the purpose of the tools you used, options you set as well as interpretation of the results.

# Resources Needed

This lab assessment covers Modules 11 and 12 from your EC-council lab content. Thus, all resources you will need will be from your labs, your text, and any research that you might have.

# Level of Difficulty

Moderate

# Important

**Please note the following guidance**: This Assessment should be performed in the VCastle POD using the Parrot Linux virtual machine.

All screenshots should reflect your own work and should have the date, time, and user information (name, student ID) clearly displayed

All takeaways/inferences you can make about your target based on the reconnaissance should be clearly expressed (full sentences without excessive use of bullet points) and should be in your own words and result from you doing the work.

# Instructions

***Tasks:***

1. Using any of the tools available on the ParrotOS virtual machine, perform a session hijacking attack using the Windows 10 machine as a target.
   1. Login to the Windows 10 machine open a browser and login to the firewall using the web interface. Use the following credentials: (**Note**: these will not work, they are used so that you can see the authentication attempt in your hijacked session)
      1. fwadmin
      2. Password1
   2. Provide documentation of the following:
      1. Any commands or tools and settings used to hijack the session
      2. A screenshot of any user authentication information captured.
2. For the exploit in the previous question, explain how the exploit worked and what controls could be used to minimize or eliminate this vulnerability.
3. From the ParrotOS virtual machine, use nmap to perform an Idle scan of a host on the network.
   1. Provide the following documentation:
      1. IP address of the idle (zombie) host:
      2. Screenshot showing the command used to perform the Idle scan and its output.
4. Explain, in your own words, how the TCP Idle scan works.