

Network Security Basics – Exercise

By Sebastian Medina

Contents

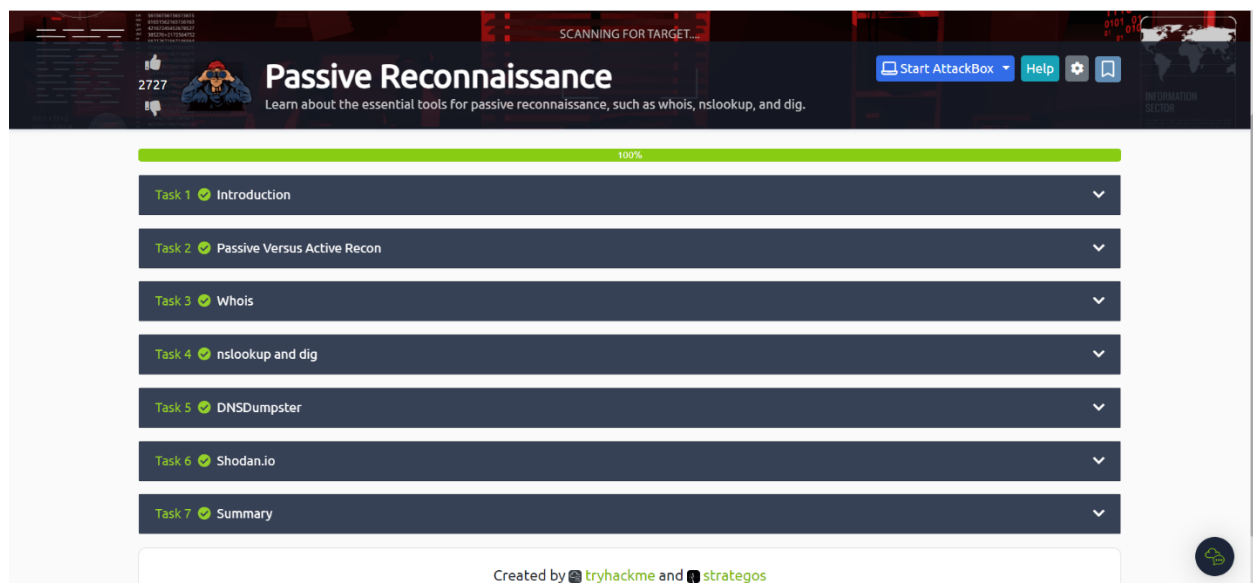
1. Network Security

1.1 Passive Reconnaissance.....	2
1.2 Active Reconnaissance.....	2/3
1.3 Nmap Live Host Discovery.....	3/4

1.1 Passive Reconnaissance

Summary:

In this module I learned what passive reconnaissance is within Network Security. Passive reconnaissance is where you must rely on publicly available knowledge. There are many ways to obtain this information and within this module you learn how to use a few of them. Some command-line tools that was taught to me within this module were whois, nslookup, and dig. Whois command allows you to look up the domain WHOIS record. Nslookup allows you to find the IP address of a domain. However, if you want to do more advanced DNS queries you will use dig and it will return more information. Also, I learned how to use DNSDumpster and Shodan.io two publicly available services. With the use of these tools, I did exercises to know how I can collect information about my targets without directly connecting to them. This is how I learned how to use passive reconnaissance.

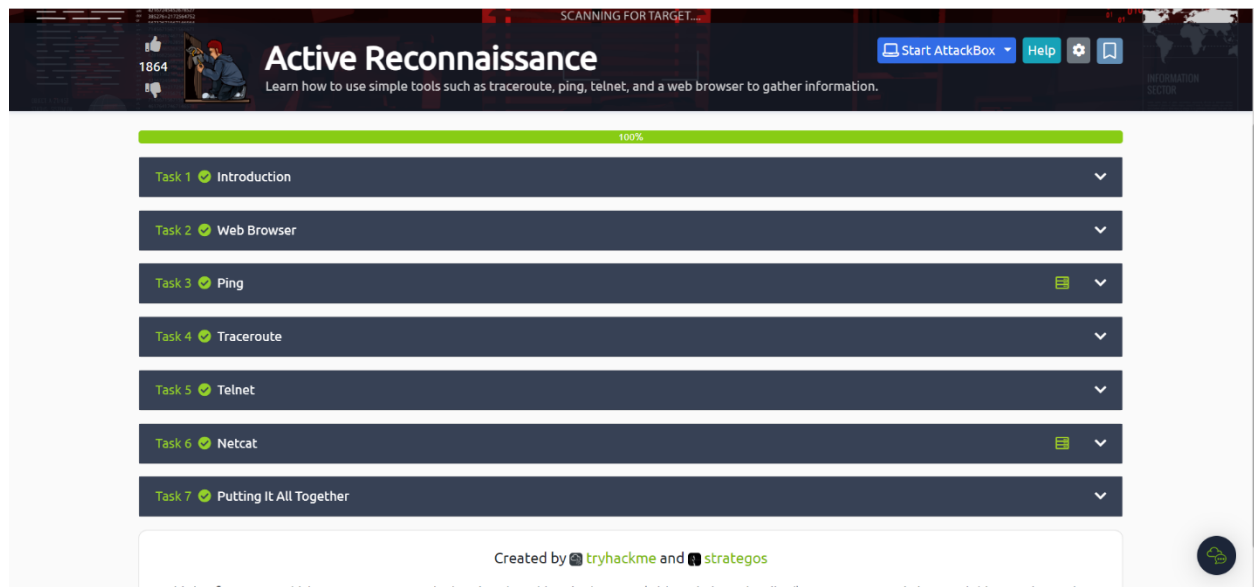


1.2 Active Reconnaissance

Summary:

Within the active reconnaissance module introduced me to active reconnaissance and how I can use certain tools to accomplish active reconnaissance. Active reconnaissance is where you gather information about your target, however you must make some kind of contact with your target. Some command line tools that I learned were traceroute, ping, and telnet. All these tools allow you to gain information about your target, however you do have to connect to your target to gain the information. For example, traceroute can be used to map the path to your target. Ping allows you to check if the remote system is online. Lastly there

is telnet that allows you to communicate with a remote system via a command-line. When done correctly you can use these tools to gain information about your target system there for completing your active reconnaissance.



1.3 Nmap Live Host Discovery

Summary:


The goal of this module is to use tools on our desired network target to find an efficient way to help us handle repetitive tasks and find out which systems are up and what services are these systems running. Before learning about some of the tools we reviewed a couple of terms like; Network segment were group of computers connected using a shared medium, Subnetwork is when one or more network segments connect and use the same router. Within this module we also learned how ARP, ICMP, TCP, and UDP can be used to detect live hosts with nmap. ARP has many options to customize your scan, but one option is arp-scan -l where it sends ARP queries to all vatoesses on your local network. ICMP echoes allows you to ping every IP address on your targeted network, however most firewalls do block it. Lastly there is TCP and UDP we can use TCP to send a synchronize flag to set port 80 to default and wait for a response. We can also use TCP to send an ACK flag. UDP can be used to discover if the host is online or not were you well gain back a ICMP port if you ping a closed UDP port. These are some of the tools where you can accomplish finding an efficient way to help us handle repetitive tasks and find out which systems are up and what services are these systems running.

2484





Nmap Live Host Discovery

Learn how to use Nmap to discover live hosts using ARP scan, ICMP scan, and TCP/UDP ping scan.

[Show Split View](#)[Help](#)

100%

Task 1  Introduction


Task 2  Subnetworks


Task 3  Enumerating Targets

Task 4  Discovering Live Hosts

Task 5  Nmap Host Discovery Using ARP

Task 6  Nmap Host Discovery Using ICMP

Task 7  Nmap Host Discovery Using TCP and UDP

Task 8  Using Reverse-DNS Lookup

Task 9  Summary

