As described before so many tools and techniques to doing a smart penetration testing well these steps is also used for hacking a network, this is a tutorial based article in which I will show you how to integrate nmap with nessus and get the maximum performance with effective scan (pen test).

The importance of nmap and nessus is not a hidden truth, nmap the best scanner ever and nessus one of our favourite vulnerability scanner, if we combine them to each other than we can make our task to be effective and less time consumer, so here is the tutorial and if you want to learn more about nmap click here and for nessus click here.

First of all i am going to use nmap for a quick scan on my local network, I am running these tools on my Ubuntu box you can use any other Linux box, backtrack is recommended specially backtrack5, you can do the same things with backtrack5 so lets start the tutorial on the terminal.

```
$ nmap 192.168.1.* -oN test.txt
```

This is the basic scan i have not used any operating system finger printing strategy or any other thing, * represent that i want to scan all the host on this gateway you can use ,

```
$ nmap 192.168.1.1/24 -oN test.txt
```

Result will be same because 1/24 is also represent all the host in the subnet and here is --oN test.txt means i want to store my result at test.txt file.

We can directly call this txt file in nessus or we can first arrange this txt file to tell nessus, after this scan you will find different host and their open ports, host depends on your network there are may be two or three or may be a single host that is your own box, well the main objective of this tutorial is to integrate nmap result with nessus, so we dont care about host.

Open your nessus, I have previously demonstrated that how to install and use nessus click here to.
On the nessus click on the scan and add new scan.

In the policy i have choose internal network scan while you can choose some other policy depend on your usage, here the point is that I have not written anything on scan target because i want to import my nmap result, so in the target file option i browse it and choose my nmap result file, that is in the home folder for my case.

Start the scan you will get some vulnerability on your network host, later on we will discuss on how to integrate nessus result with metasploit to own a box, and we have planned to show you how to use autopwn on nessus result. So if you will combine nmap, nessus and metasploit each other you will surely create a awesome testing environment.

**Note:** If you enjoyed this post, you might want to subscribe our RSS feed and Email Subscription or become our Facebook fan! You will get all the latest updates at both the places.

**Related post**

**Backtrack5**
- DarkMYSQLi- MYSQL Injection Tool Tutorial
- Tabnapping Tutorial– Social Engineering Toolkit Backtrack 5
- Autopwn Metasploit Backtrack 5 - Postgresql Solved
- Complemento Backtrack 5 Toolkit

**BackTrack**
- Fern wifi Cracker- A Wireless Penetration Testing Tool
- DarkMYSQLi- MYSQL Injection Tool Tutorial
- Tabnapping Tutorial– Social Engineering Toolkit Backtrack 5
- Autopwn Metasploit Backtrack 5 - Postgresql Solved

and sniffing. Sniffing is an act to capture or v...

**Autopwn Metasploit Backtrack 5 - Postgresql Solved**
Metasploit is one of the best database and a software that has a list of exploits for different softwares, nmap is the great network scan...

**Fast Track Hacking– Backtrack 5 Tutorial**
Backtrack 5 contains different tools for exploitation, as discussed before about metasploit and armitage for this article i will discuss ...

**Backtrack 5 Tutorials**
Backtrack is a wonderful Linux distribution that provides advance features and option for the penetration tester to do the job done, Backtr...

**DarkMYSQLi – MYSQL Injection Tool Tutorial**
SQL injection is one the most common bug or vulnerability in a web application that can easily be exploit, there are mainly two ways to e...
Integrate Nmap With Nessus - Tutorial | Ethical Hacking - Your Way To The World Of IT Security

Which operating system do you like most?

- Windows
- Linux
- MAC

Popular Threads

- How to Find An Email of Facebook Friend | Ethical Hacking - Your Way To The World Of IT Security
  9 comments · 3 days ago

- A History of Hacking [INFOGRAPHIC] | Ethical Hacking - Your Way To The World Of IT Security
  2 comments · 3 days ago

- Complemento Backtrack 5 Toolkit | Ethical Hacking - Your Way To The World Of IT Security
  2 comments · 1 week ago

Recent Comments

- Anonymous - 1337 yes u can send him a link and u wil get there ip sent to your email
  Fast Track Hacking - Backtrack5 Tutorial | Ethical Hacking - Your Way To The World Of IT Security · 16 hours ago

- Ethical Hacking for this purpose you need to make some changes on the kernel side, basically backtrack is based...
  How To Install Backtrack 5 Dual

Powered by Disqus

Follow this blog

This blog by Irfan Shakeel is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported License.

Is there a way to rename the bootloader to not read "Ubuntu, with Linux 2.6.38" and have it...