Hakin9

PRACTICAL PROTECTION

IT SECURITY MAGAZINE

starterkit

HOW TO PENTEST WITH BACKTRACK

HOW ANYONE CAN BE COMPROMISED

SECURITY PENTESTING WITH BACKTRACK

HOW TO CONDUCT A PENETRATION TEST – A BEGINNER'S GUIDE

A CRASH COURSE IN PENTESTING WITH BACTRACK

Vol.3 No.09
Issue 03/2013(9) ISSN: 1733-7186

PLUS

MY NETWORK IS ILL, I FEAR THAT HE HAS THE YERSINIA (PESTIS)

Similarly, you can try running other exploits, on the target machine. For more information on metasploit, refer to *http://www.offensive-security.com/metasploit-unleashed*.

Post-Exploitation Phase

While doing the pen-test, it is a best practice to manage our results at a centralized location, and once, we have successfully pen-tested the target, we will be required to submit the documents and report supporting the claims. Tools like MagicTree and Dradis available in BackTrack can help us achieve those objectives. Let us look at an example using MagicTree:

MagicTree

Go to Applications -> BackTrack -> Reporting Tools -> Evidence Management -> magictree.

Step 1

At the screen above, press [Ctrl+N], to add a new node, and enter your target machine's IP address when asked for the node value and click OK, as shown in Figure 26.

Step 2

Click on Q*, on the left-top panel. Now, enter the following command on the right panel in the *Command* field: `nmap -sS -A -oX $out.xml $host`, and click *Run* (Figure 27).

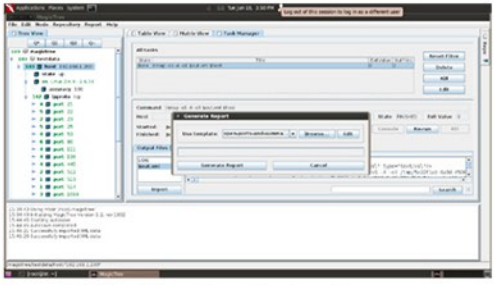

Figure 30. *MagicTree – Generating Report*

Figure 31. *MagicTree – Final Report*

-oX = Output the result to out.xml
$host = Variable that stores the host IP

Step 3

Once it is completed, you will get the results output into the file "out.xml". Select "out.xml", and click on *Import* (Figure 28 and Figure 29).

Step 4

Click on *Report* in the top menu -> *Generate Report*. Browse and select "open-ports-and-summary-of-finding-hosts.odt" as the template, and click on *Generate Report*.

Note: Run `apt-get install openoffice.org`, to install OpenOffice to view the report (Figure 30 and Figure 31).

A description of the reports and deliverables should be provided at the conclusion of the penetration test. The report is broken down into two major sections in order to communicate the objectives, methods, and results of the testing conducted to various audiences:

- Executive Summary
- Technical Report

Conclusion

BackTrack is one dedicated Linux distribution for penetration testing and digital forensics that has the support of a great community of security professionals across the globe. It started with BT v1.0 in May 2006 and the latest version being Kali Linux, released in March 2013. It already contains a host of tools, which can assist you in completing the penetration test for a small/medium/large scale organization. This article covered a bird's eye view of PenTesting with BT; there is still a lot of fun stuff left to explore. Good Luck!

PIYUSH VERMA

Piyush Verma, currently works as an Information Security Consultant at KOENIG Solutions, Dubai. Additionally, he delivers training to professionals across the globe on various Information Security Certifications such as CompTIA Security+, CEH v8, ECSA|LPT, CHFI v8, Advanced PenTesting with BackTrack & other trending courses. His areas of interest include, but are not limited to, finding, exploiting and patching vulnerabilities, computer forensics investigations, cryptography, and writing technical articles.