Windows Tools For Penetration Testing

pentestlab.blog/category/general-lab-notes/page/7

January 7, 2013

Most penetration testers are using either a Mac or a Linux-based platform in order to perform their penetration testing activities.However it is always a good practice to have and a Windows virtual machine with some tools ready to be used for the engagement.The reason for this is that although Windows cannot be used as a main platform for penetration testing some of the utilities and tools can still help us to extract information from our windows targets.So in this post we will see some of the tools that we can use in our windows system.

HashCheck Shell Extension

The HashCheck Shell Extension makes it easy for anyone to calculate and verify checksums and hashes from Windows Explorer. In addition to integrating file checksumming functionality into Windows, HashCheck can also create and verify SFV files (and other forms of checksum files, such as .md5 files).

Netcat

Netcat is often referred to as a “Swiss-army knife for TCP/IP”. Its list of features includes port scanning, transferring files, and port listening, and it can be used as a backdoor.

Metasploit Framework

The Metasploit Project is a computer security project which provides information about security vulnerabilities and aids in penetration testing and IDS signature development.

RealVNC Viewer

Remote access software for desktop and mobile platforms.

GetIf

SNMP tool that allows you to collect information about SNMP devices.

Cain & Abel

Cain & Abel is a password recovery tool for Microsoft Operating Systems. It allows easy recovery of various kind of passwords by sniffing the network, cracking encrypted passwords using Dictionary, Brute-Force and Cryptanalysis attacks, recording VoIP conversations, decoding scrambled passwords, recovering wireless network keys, revealing password boxes, uncovering cached passwords and analyzing routing protocols.

Wireshark

Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development.

PuTTY

PuTTY is an SSH and telnet client for the Windows platform.

Pass The Hash Toolkit

The Pass-The-Hash Toolkit contains utilities to manipulate the Windows Logon Sessions mantained by the LSA (Local Security Authority) component. These tools allow you to list the current logon sessions with its corresponding NTLM credentials (e.g.: users remotely logged in thru Remote Desktop/Terminal Services), and also change in runtime the current username, domain name, and NTLM hashes.

Cachedump

Recovering Windows Password Cache Entries.

Fport

Identify unknown open ports and their associated applications.

Nbtscan

This is a command-line tool that scans for open NETBIOS nameservers on a local or remote TCP/IP network, and this is a first step in finding of open shares.

Burp Suite

Burp Suite is an integrated platform for performing security testing of web applications. Its various tools work seamlessly together to support the entire testing process, from initial mapping and analysis of an application’s attack surface, through to finding and exploiting security vulnerabilities.

Winfo

Winfo uses null sessions to remotely try to retrieve lists of and information about user accounts, workstation/interdomain/server trust accounts, shares (also hidden), sessions, logged in users, and password/lockout policy, from Windows NT/2000/XP. It also identifies the built-in Administrator and Guest accounts, even if their names have been changed.

ClearLogs

ClearLogs clears the event log (Security, System or Application) that you specify. You run it from the Command Prompt, and it can also clear logs on a remote computer.

SQLDict

SQLdict is a dictionary attack tool for SQL Server.

PMDump

PMDump is a tool that lets you dump the memory contents of a process to a file without stopping the process.

GrabItAll

GrabItAll performs traffic redirection by sending spoofed ARP replies. It can redirect traffic from one computer to the attackers computer, or redirect traffic between two other computers through the attackers computer. In the last case you need to enable IP Forwarding which can be done with GrabItAll too.

DumpUsers

DumpUsers is able to dump account names and information even though RestrictAnonymous has been set to 1.

BrowseList

BrowseList retrieves the browse list. The output list contains computer names, and the roles they play in the network. For example you can see which are PDC, BDC, stand-alone servers and workstations. You can also see the system comments (which can be very interesting reading).

Remoxec

Remoxec executes a program using RPC (Task Scheduler) or DCOM (Windows Management Instrumentation).

WMICracker

Brute-force tool for Windows Management Instrumentation (WMI).

Venom

Venom is a tool to run dictionary password attacks against Windows accounts by using the Windows Management Instrumentation (WMI) service. This can be useful in those cases where the server service has been disabled.

SMBAT

The SMB Auditing Tool is a password auditing tool for the Windows-and the SMB-platform. It makes it possible to exploit the timeout architecture bug in Windows 2000/XP, making it extremly fast to guess passwords on these platforms.

RPCScan

RPCScan v2.03 is a Windows based detection and analysis utility that can quickly and accurately identify Microsoft operating systems that are vulnerable to the multiple buffer overflow vulnerabilities released in the MS03-026 and MS03-039 bulletins.

LSASecretsDump

LSASecretsDump is a small console application that extract the LSA secrets from the Registry, decrypt them, and dump them into the console window.

SQLPing

SQL Ping is a nice little command line enumerator that specifically looks for SQL servers and requires no authentication whatsoever.

OAT

The Oracle Auditing Tools is a toolkit that could be used to audit security within Oracle database servers.

Pwdump7

Extract password hashes from local user accounts.

PsTools

The PsTools package provides a set of command line utilities that allow you to manage local and remote systems.

Incognito

Incognito is a tool for manipulating windows access tokens and is intended for use by penetration testers, security consultants and system administrators.

DumpSec

DumpSec is a security auditing program for Microsoft Windows® NT/XP/200x. It dumps the permissions (DACLs) and audit settings (SACLs) for the file system, registry, printers and shares in a concise, readable format, so that holes in system security are readily apparent. DumpSec also dumps user, group and replication information.

X-Deep32

X-Deep/32 is an X Window Server for Windows NT/2000/9X/ME/XP that can be used to connect to host systems running UNIX, LINUX, IBM AIX etc.

LC5

Windows password cracker.

Ophcrack

Ophcrack is a free Windows password cracker based on rainbow tables.

SiVuS

SiVus is the first publicly available vulnerability scanner for VoIP networks that use the SIP protocol. It provides powerful features to assess the security and robustness of VoIP implementations.