

Forum:[Hack Forums](#)

Thread: [HACKING TOOLS \(Port Scanners, Packet Sniffers , Password Crackers,Encryption Tools...](#)

Thie500 - February 11, 2012, 7:38 am

-: Hacking Tools :-

Port Scanners :-

Nmap :- This tool developed by Fyodor is one of the best unix and windows based port scanners. This advanced port scanner has a number of useful arguments that gives user a lot of control over the process.

Home:- <http://adf.ly/5Jr5z>

Latest Release:- Nmap 5.50

Download:- <http://adf.ly/2320MI>

Superscan :- A Windows-only port scanner, pinger, and resolver
SuperScan is a free Windows-only closed-source TCP/UDP port scanner by Foundstone. It includes a variety of additional networking tools such as ping, traceroute, http head, and whois.

Home:- <http://adf.ly/5Jr60>

Latest Release:- SuperScan v4.0

Download:- <http://adf.ly/2321B>

Angry IP Scanner :- A fast windows IP scanner and port scanner. Angry IP Scanner can perform basic host discovery and port scans on Windows. Its binary file size is very small compared to other scanners and other pieces of information about the target hosts can be extended with a few plugins.

Home:- <http://adf.ly/5NdUy>

Latest Release:- IPScan 3.0-beta3

Download:- <http://adf.ly/2321a>

Unicorns can :- Unicorns can is an attempt at a User-land Distributed TCP/IP stack for information gathering and correlation. It is intended to provide a researcher a superior interface for introducing a stimulus into and measuring a response from a TCP/IP enabled device or network. Some of its features include asynchronous stateless TCP scanning with all variations of TCP flags, asynchronous stateless TCP banner grabbing, and active/passive remote OS, application, and component identification by analyzing responses.

Home:- <http://adf.ly/2321w>

Latest Release:- Unicorns can 0.4.7-2

Download:- <http://adf.ly/2321w>

OS Fingerprinting Tools :-

Nmap :- This tool developed by Fyodor is one of the best unix and windows based active os fingerprinting tool.

Home:- <http://adf.ly/5Jr5z>
Latest Release:- Nmap 5.50
Download:- <http://adf.ly/2320M>

P0f :- A passive OS fingerprinting tool. P0f is able to identify the operating system of a target host simply by examining captured packets even when the device in question is behind an overzealous packet firewall. P0f can detect firewall presence, NAT use, existence of load balancers, and more!

Home:- <http://adf.ly/5NdV1>
Latest Release:- p0f v2 (2.0.8)
Download:- <http://adf.ly/5NdV1>

Xprobe2 :- Active OS fingerprinting tool. XProbe is a tool for determining the operating system of a remote host. They do this using some of the same techniques as Nmap as well as some of their own ideas. Xprobe has always emphasized the ICMP protocol in its fingerprinting approach.

Home:- <http://adf.ly/5NdV7>
Latest Release:- Xprobe2 0.3
Download:- <http://adf.ly/5NdV8>

Password Crackers :-

Cain and Abel :- The top password recovery tool for Windows. This Windows-only password recovery tool handles an enormous variety of tasks. It can recover passwords by sniffing the network, cracking encrypted passwords using Dictionary, Brute-Force and Cryptanalysis attacks, recording VoIP conversations, decoding scrambled passwords, revealing password boxes, uncovering cached passwords and analyzing routing protocols.

Home:- <http://adf.ly/5P8uB>
Latest Release:- cain & abel v4.9.40
Download:- <http://adf.ly/2322M>

John the Ripper :- A powerful, flexible, and fast multi-platform password hash cracker. John the Ripper is a fast password cracker, currently available for many flavors of Unix, DOS, Win32, BeOS, and OpenVMS. Its primary purpose is to detect weak Unix passwords. It supports several crypt(3) password hash types which are most commonly found on various Unix flavors, as well as Kerberos AFS and Windows NT/2000/XP LM hashes. Several other hash types are added with contributed patches.

Home:- <http://adf.ly/5P8uD>
Latest Release:- John the Ripper 1.7
Download:- <http://adf.ly/2322t>

THC Hydra :- A Fast network authentication cracker which support many different services. When you need to brute force crack a remote authentication service, Hydra is often the tool of choice. It can perform rapid dictionary attacks against more than 30 protocols, including telnet, ftp, http, https, smb, several databases, and much more.

Home:- <http://adf.ly/5P8uE>
Latest Release:- THC-Hydra v5.4
Download:- <http://adf.ly/2323f>

L0phtcrack :- Windows password auditing and recovery application

L0phtCrack, also known as LC5, attempts to crack Windows passwords from hashes which it can obtain (given proper access) from stand-alone Windows NT/2000 workstations, networked servers, primary domain controllers, or Active Directory. In some cases it can sniff the hashes off the wire. It also has numerous methods of generating password guesses (dictionary, brute force, etc).

Home:- Not Available

Latest Release:- L0phtcrack v5.04

Download:- <http://adf.ly/2326M>
<http://adf.ly/2326m> (keygen)

Pwdump :- Windows password recovery tool.

Pwdump is able to extract NTLM and LanMan hashes from a Windows target, regardless of whether Syskey is enabled. It is also capable of displaying password histories if they are available. It outputs the data in L0phtcrack-compatible form, and can write to an output file.

Home:- <http://adf.ly/5P8uF>

Latest Release:- pwdump6 version 1.7.2

Download:- <http://adf.ly/2328L>

RainbowCrack :- An Innovative Password Hash Cracker.

The RainbowCrack tool is a hash cracker that makes use of a large-scale time-memory trade-off. A traditional brute force cracker tries all possible plaintexts one by one, which can be time consuming for complex passwords. RainbowCrack uses a time-memory trade-off to do all the cracking-time computation in advance and store the results in so-called "rainbow tables". It does take a long time to precompute the tables but RainbowCrack can be hundreds of times faster than a brute force cracker once the precomputation is finished.

Home:- <http://adf.ly/5P8uG>

Latest Release:- rainbowcrack v1.2

Download:- <http://adf.ly/2328r>

Brutus :- A network brute-force authentication cracker

This Windows-only cracker bangs against network services of remote systems trying to guess passwords by using a dictionary and permutations thereof. It supports HTTP, POP3, FTP, SMB, TELNET, IMAP, NTP, and more.

Home:- <http://adf.ly/5P8uH>

Latest Release:- brutus-aet2

Download:- <http://adf.ly/2329B>

Vulnerability Scanners :-

Nessus :- Premier UNIX vulnerability assessment tool

Nessus is the best free network vulnerability scanner available, and the best to run on UNIX at any price. It is constantly updated, with more than 11,000 plugins for the free (but registration and EULA-acceptance required) feed. Key features include remote and local (authenticated) security checks, a client/server architecture with a GTK graphical interface, and an embedded scripting language for writing your own plugins or understanding the existing ones.

Home:- <http://adf.ly/5P96e>

Latest Release:- Nessus 4

Download:- <http://adf.ly/2329b>

GFI LANguard :- A commercial network security scanner for Windows

GFI LANguard scans IP networks to detect what machines are running. Then it tries to discern the host OS and what applications are running. It also tries to collect Windows machine's service pack level, missing security patches, wireless access points, USB devices, open shares, open ports, services/applications active on the computer, key registry entries, weak passwords, users and groups, and more. Scan results are saved to an HTML report, which can be customized/queried. It also includes a patch manager which detects and installs missing patches.

Home:- <http://adf.ly/5P96j>

Latest Release:- GFI LANguard Network Security Scanner 8

Download:- <http://adf.ly/232AS>

Retina :- Commercial vulnerability assessment scanner by eEye

Like Nessus, Retina's function is to scan all the hosts on a network and report on any vulnerabilities found. It was written by eEye, who are well known for their security research.

Home:- <http://adf.ly/5P96o>

Latest Release:- Retina Network Security Scanner v5.15.7

Download:- <http://adf.ly/232B8>

Core Impact :- An automated, comprehensive penetration testing product. It is widely considered to be the most powerful exploitation tool available. It sports a large, regularly updated database of professional exploits, and can do neat tricks like exploiting one machine and then establishing an encrypted tunnel through that machine to reach and exploit other boxes.

Home:- <http://adf.ly/5P96r>

Latest Release:- Core Impact 4.0

Download:- <http://adf.ly/232Bq>

ISS Internet Scanner :- Application-level vulnerability assessment

Internet Scanner started off in '92 as a tiny open source scanner by Christopher Klaus. Now he has grown ISS into a billion-dollar company with a myriad of security products.

<http://adf.ly/5P9H3>

SARA :- Security Auditor\92s Research Assistant

SARA is a third generation network security analysis tool that Operates under Unix, Linux, MAC OS/X or Windows. The first generation assistant, the Security Administrator's Tool for Analyzing Networks (SATAN) was developed in early 1995. It became the benchmark for network security analysis for several years. However, few updates were provided and the tool slowly became obsolete in the growing threat environment.

Home:- <http://adf.ly/5P96x>

Download:- <http://adf.ly/232Ep>

Packet Sniffers :-

Ethereal :- This (also known as Wireshark) is a fantastic open source network protocol analyzer for Unix and Windows. It allows you to examine data from a live network or from a capture file on disk. You can interactively browse the capture data, delving down into just the level of packet detail you need. Ethereal has several powerful features, including a rich display filter language and the ability to view the reconstructed stream of a TCP session. It also supports hundreds of protocols and media types.

Home:- <http://adf.ly/5P9QJ>

Latest Release:- Wireshark 1.0.4 (Ethereal)

Download:- <http://adf.ly/5P9QL>

Kismet :- A powerful wireless sniffer. Kismet is a console based 802.11 layer2 wireless network detector, sniffer, and intrusion detection system. It identifies networks by passively sniffing, and can even decloak hidden networks if they are in use. It can automatically detect network IP blocks by sniffing TCP, UDP, ARP, and DHCP packets, log traffic in Wireshark/TCPDump compatible format, and even plot detected networks and estimated ranges on downloaded maps.

Home:- <http://adf.ly/5P9QM>

Latest Release:- Kismet-2008-05-R1

Download:- <http://adf.ly/5P9QO>

Tcpdump :- The classic sniffer for network monitoring and data acquisition. It is great for tracking down network problems or monitoring activity. There is a separate Windows port named WinDump. TCPDump is the source of the Libpcap/WinPcap packet capture library.

Home:- <http://adf.ly/5P9QP>

Latest Release:- TCPDUMP 4.0.0

Download:- <http://adf.ly/5P9QR>

Ettercap :- Ettercap is a terminal-based network sniffer/interceptor/logger for ethernet LANs. It supports active and passive dissection of many protocols (even ciphered ones, like ssh and https). Data injection in an established connection and filtering on the fly is also possible, keeping the connection synchronized. Many sniffing modes were implemented to give you a powerful and complete sniffing suite. Plugins are supported. It has the ability to check whether you are in a switched LAN or not, and to use OS fingerprints (active or passive) to let you know the geometry of the LAN.

Home:- <http://adf.ly/5P9QT>

Latest Release:- Ettercap NG-0.7.3

Download:- <http://adf.ly/5P9QU>

DSniff :- A suite of powerful network auditing and penetration-testing tools. This popular and well-engineered suite by Dug Song includes many tools. dsniff, filesnarf, mailsnarf, msgsnarf, urlsnarf, and webspy passively monitor a network for interesting data (passwords, e-mail, files, etc.). arpspoof, dnsspoof, and macof facilitate the interception of network traffic normally unavailable to an attacker (e.g, due to layer-2 switching). sshmitm and webmitm implement active monkey-in-the-middle attacks against redirected ssh and https sessions by exploiting weak bindings in ad-hoc PKI. Overall, this is a great toolset. It handles pretty much all of your password sniffing needs.

Home:- <http://adf.ly/5P9QX>

Latest Release:- dsniff-2.3

Download:- <http://adf.ly/5P9QY>

Encryption Tools :-

GnuPG / PGP :- Secure your files and communication with the advanced encryption. PGP is the famous encryption program by Phil Zimmerman which helps secure your data from eavesdroppers and other risks. GnuPG is a very well-regarded open source implementation of the PGP standard

(the actual executable is named gpg). While GnuPG is always free, PGP costs money for some uses.

<http://adf.ly/5P9fp>

<http://adf.ly/5P9fs>

OpenSSL :- The premier SSL/TLS encryption library. The OpenSSL Project is a collaborative effort to develop a robust, commercial-grade, full-featured, and open source toolkit implementing the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) protocols as well as a full-strength general purpose cryptography library. The project is managed by a worldwide community of volunteers that use the Internet to communicate, plan, and develop the OpenSSL toolkit and its related documentation.

<http://adf.ly/5P9fw>

Tor :- An anonymous Internet communication system Tor is a toolset for a wide range of organizations and people that want to improve their safety and security on the Internet. Using Tor can help you anonymize web browsing and publishing, instant messaging, irc, ssh, and other applications that use the TCP protocol. Tor also provides a platform on which software developers can build new applications with built-in anonymity, safety, and privacy features.

<http://adf.ly/5P9fy>

Stunnel :- A general-purpose SSL cryptographic wrapper. The stunnel program is designed to work as an SSL encryption wrapper between remote client and local or remote server. It can be used to add SSL functionality to commonly used inetd daemons like POP2, POP3, and IMAP servers without any changes in the programs' code.

<http://adf.ly/5P9g5>

OpenVPN :- A full-featured SSL VPN solution. OpenVPN is an open-source SSL VPN package which can accommodate a wide range of configurations, including remote access, site-to-site VPNs, WiFi security, and enterprise-scale remote access solutions with load balancing, failover, and fine-grained access-controls. OpenVPN implements OSI layer 2 or 3 secure network extension using the industry standard SSL/TLS protocol, supports flexible client authentication methods based on certificates, smart cards, and/or 2-factor authentication, and allows user or group-specific access control policies using firewall rules applied to the VPN virtual interface. OpenVPN uses OpenSSL as its primary cryptographic library.

<http://adf.ly/5P9gB>

TrueCrypt :- Open-Source Disk Encryption Software for Windows and Linux. TrueCrypt is an excellent open source disk encryption system. Users can encrypt entire filesystems, which are then on-the-fly encrypted/decrypted as needed without user intervention beyond entering their passphrase initially. A clever hidden volume feature allows you to hide a 2nd layer of particularly sensitive content with plausible deniability about whether it exists. Then if you are forced to give up your passphrase, you give them the first-level secret. Even with that, attackers cannot prove that a second level key even exists..

<http://adf.ly/5P9gE>

ForgetMe - February 26, 2012, 7:10 pm

this is an awesome collection bro! thanks so much! anyway you can pack them all into one file?
haha

iloveSara - February 26, 2012, 7:33 pm

I agree with ForgetMe. It would be much easier if you would compress all of the files into a .zip file.

AlbertoJ - February 28, 2012, 4:49 am

interesting tools ^^ nice collection thx for sharing!

Thie500 - May 7, 2013, 5:34 am

(Feb 26, 2012 08:10 PM)ForgetMe Wrote: [\[CITE\]](#) this is an awesome collection bro! thanks so much! anyway you can pack them all into one file? hahaNp :D I'll do it when I find some time. :D

blaizer_12 - July 31, 2013, 2:48 pm

i luv this tools the seem very useful and essensial.
thanks bro.

Filthy Frank - July 31, 2013, 5:07 pm

i do not find this legit, i'm not trusting a person with 2 posts

Mr.Evil - July 31, 2013, 5:26 pm

Sweet collection, very well put together. Itll be nice to C&A again...thx bro

bianky - August 3, 2013, 9:19 pm

thanks for sharing awesome[i will download it font=Times New Roman][[/font]

killer3101 - August 4, 2013, 2:46 am

thx for this, i go try our tool :)

thx again

9/11 - August 4, 2013, 12:53 pm

Wow great list. There are lots of download links but if you have a DarkComet crypter please pm the link and can it please be free.

WOUALAS - December 27, 2016, 10:05 pm

WOW really everything you need to do good job
thanks for this list?