./RNDTX

I'm a bit of a hacker fanatic and know a fair bit about that industry and cyber crime and cyber warfare.
Indonesia, Tangerang

Awesome Pentest

Dec 26, 2015

Awesome Penetration Testing

A collection of awesome penetration testing resources

Vulnerability Scanners
Network Tools
Wireless Network Tools
SSL Analysis Tools
Hex Editors
Crackers
Windows Utils
DDoS Tools
Social Engineering Tools
OSInt Tools
Anonimity Tools
Reverse Engineering Tools
Books
Penetration Testing Books
Hackers Handbook Series
Network Analysis Books
Reverse Engineering Books
Malware Analysis Books
Windows Books
Social Engineering Books
Lock Picking Books
Vulnerability Databases
Security Courses
Information Security Conferences
Information Security Magazines

License

Online Resources

Penetration Testing Resources * Metasploit Unleashed - Free Offensive Security metasploit course * PTES - Penetration Testing Execution Standard * OWASP - Open Web Application Security Project

Shellcode development

Shellcode Tutorials - Tutorials on how to write shellcode
Shellcode Examples - Shellcodes database

Social Engineering Resources

Social Engineering Framework - An information resource for social engineers

Lock Picking Resources

Schuyler Towne channel - Lockpicking videos and security talks
/r/lockpicking - Resources for learning lockpicking, equipment recommendations.

Tools

Penetration Testing Distributions * Kali - A Linux distribution designed for digital forensics and penetration testing * BlackArch - Arch Linux-based distribution for penetration testers and security researchers * NST - Network

* `BackBox` - Ubuntu-based distribution for penetration tests and security assessments

Basic Penetration Testing Tools

`Metasploit Framework` - World's most used penetration testing software
`Burp Suite` - An integrated platform for performing security testing of web applications
`ExploitPack` - Graphical tool for penetration testing with a bunch of exploits

Vulnerability Scanners

`Netsparker` - Web Application Security Scanner
`Nexpose` - Vulnerability Management & Risk Management Software
`Nessus` - Vulnerability, configuration, and compliance assessment
`Nikto` - Web application vulnerability scanner
`OpenVAS` - Open Source vulnerability scanner and manager
`OWASP Zed Attack Proxy` - Penetration testing tool for web applications
`Secapps` - Integrated web application security testing environment
`w3af` - Web application attack and audit framework
`Wapiti` - Web application vulnerability scanner
`WebReaver` - Web application vulnerability scanner for Mac OS X

Network Tools

`nmap` - Free Security Scanner For Network Exploration & Security Audits
`tcpdump/libpcap` - A common packet analyzer that runs under the command

`Network Tools` - Different network tools: ping, lookup, whois, etc
`netsniff-ng` - A Swiss army knife for for network sniffing
`Intercepter-NG` - a multifunctional network toolkit
`SPARTA` - Network Infrastructure Penetration Testing Tool

Wireless Network Tools

`Aircrack-ng` - a set of tools for auditing wireless network
`Kismet` - Wireless network detector, sniffer, and IDS
`Reaver` - Brute force attack against Wifi Protected Setup

SSL Analysis Tools

`SSLyze` - SSL configuration scanner
`sslstrip` - a demonstration of the HTTPS stripping attacks

Hex Editors

`HexEdit.js` - Browser-based hex editing

Crackers

`John the Ripper` - Fast password cracker
`Online MD5 cracker` - Online MD5 hash Cracker

Windows Utils

`Sysinternals Suite` - The Sysinternals Troubleshooting Utilities
`Windows Credentials Editor` - security tool to list logon sessions and add

DDoS Tools

`LOIC` - An open source network stress tool for Windows
`JS LOIC` - JavaScript in-browser version of LOIC

Social Engineering Tools

`SET` - The Social-Engineer Toolkit from TrustedSec

OSInt Tools

`Maltego` - Proprietary software for open source intelligence and forensics, from Paterva.

Anonimity Tools

`Tor` - The free software for enabling onion routing online anonymity
`I2P` - The Invisible Internet Project

Reverse Engineering Tools

`IDA Pro` - A Windows, Linux or Mac OS X hosted multi-processor disassembler and debugger
`IDA Free` - The freeware version of IDA v5.0
`WDK/WinDbg` - Windows Driver Kit and WinDbg
`OllyDbg` - An x86 debugger that emphasizes binary code analysis
`Radare2` - Opensource, crossplatform reverse engineering framework.
`x64_dbg` - An open-source x64/x32 debugger for windows.

Immunity Debugger - A powerful new way to write exploits and analyze malware
Evan's Debugger - OllyDbg-like debugger for Linux

Books

Penetration Testing Books * The Art of Exploitation by Jon Erickson, 2008 * Metasploit: The Penetration Tester's Guide by David Kennedy and others, 2011 * Penetration Testing: A Hands-On Introduction to Hacking by Georgia Weidman, 2014 * Rtfm: Red Team Field Manual by Ben Clark, 2014 * The Hacker Playbook by Peter Kim, 2014 * The Basics of Hacking and Penetration Testing by Patrick Engebretson, 2013 * Professional Penetration Testing by Thomas Wilhelm, 2013 * Advanced Penetration Testing for Highly-Secured Environments by Lee Allen,2012 * Violent Python by TJ O'Connor, 2012 * Fuzzing: Brute Force Vulnerability Discovery by Michael Sutton, Adam Greene, Pedram Amini, 2007 * Black Hat Python: Python Programming for Hackers and Pentesters, 2014 * Penetration Testing: Procedures & Methodologies (EC-Council Press),2010

Hackers Handbook Series

The Shellcoders Handbook by Chris Anley and others, 2007
The Web Application Hackers Handbook by D. Stuttard, M. Pinto, 2011
iOS Hackers Handbook by Charlie Miller and others, 2012
Android Hackers Handbook by Joshua J. Drake and others, 2014
The Browser Hackers Handbook by Wade Alcorn and others, 2014

Network Analysis Books

Nmap Network Scanning by Gordon Fyodor Lyon, 2009
Practical Packet Analysis by Chris Sanders, 2011
Wireshark Network Analysis by by Laura Chappell, Gerald Combs, 2012

Reverse Engineering Books

Reverse Engineering for Beginners by Dennis Yurichev (free!)
The IDA Pro Book by Chris Eagle, 2011
Practical Reverse Engineering by Bruce Dang and others, 2014
Reverse Engineering for Beginners

Malware Analysis Books

Practical Malware Analysis by Michael Sikorski, Andrew Honig, 2012
The Art of Memory Forensics by Michael Hale Ligh and others, 2014
Malware Analyst's Cookbook and DVD by Michael Hale Ligh and others, 2010

Windows Books

Windows Internals by Mark Russinovich, David Solomon, Alex Ionescu

Social Engineering Books

The Art of Deception by Kevin D. Mitnick, William L. Simon, 2002
The Art of Intrusion by Kevin D. Mitnick, William L. Simon, 2005

Social Engineering: The Art of Human Hacking by Christopher Hadnagy, 2010
Unmasking the Social Engineer: The Human Element of Security by Christopher Hadnagy, 2014
Social Engineering in IT Security: Tools, Tactics, and Techniques by Sharon Conheady, 2014

Lock Picking Books

Practical Lock Picking by Deviant Ollam, 2012
Keys to the Kingdom by Deviant Ollam, 2012
CIA Lock Picking Field Operative Training Manual
Lock Picking: Detail Overkill by Solomon
Eddie the Wire books

Vulnerability Databases

NVD - US National Vulnerability Database
CERT - US Computer Emergency Readiness Team
OSVDB - Open Sourced Vulnerability Database
Bugtraq - Symantec SecurityFocus
Exploit-DB - Offensive Security Exploit Database
Fulldisclosure - Full Disclosure Mailing List
MS Bulletin - Microsoft Security Bulletin
MS Advisory - Microsoft Security Advisories
Inj3ct0r - Inj3ctor Exploit Database

`CXSecurity` - CSSecurity Bugtraq List
`Vulnerability Laboratory` - Vulnerability Research Laboratory
`ZDI` - Zero Day Initiative

Security Courses

`Offensive Security Training` - Training from BackTrack/Kali developers
`SANS Security Training` - Computer Security Training & Certification
`Open Security Training` - Training material for computer security classes
`CTF Field Guide` - everything you need to win your next CTF competition
`Cybrary` - online IT and Cyber Security training platform

Information Security Conferences

`DEF CON` - An annual hacker convention in Las Vegas
`Black Hat` - An annual security conference in Las Vegas
`BSides` - A framework for organising and holding security conferences
`CCC` - An annual meeting of the international hacker scene in Germany
`DerbyCon` - An annual hacker conference based in Louisville
`PhreakNIC` - A technology conference held annually in middle Tennessee
`ShmooCon` - An annual US east coast hacker convention
`CarolinaCon` - An infosec conference, held annually in North Carolina
`HOPE` - A conference series sponsored by the hacker magazine 2600
`SummerCon` - One of the oldest hacker conventions, held during Summer
`Hack.lu` - An annual conference held in Luxembourg
`HITB` - Deep-knowledge security conference held in Malaysia and The

`Troopers` - Annual international IT Security event with workshops held in Heidelberg, Germany
`Hack3rCon` - An annual US hacker conference
`ThotCon` - An annual US hacker conference held in Chicago
`LayerOne` - An annual US security conerence held every spring in Los Angeles
`DeepSec` - Security Conference in Vienna, Austria
`SkyDogCon` - A technology conference in Nashville
`SECUINSIDE` - Security Conference in `Seoul`
`DefCamp` - Largest Security Conference in Eastern Europe, held anually in Bucharest, Romania

Information Security Magazines

`2600: The Hacker Quarterly` - An American publication about technology and computer "underground"
`Phrack Magazine` - By far the longest running hacker zine

Awesome Lists

`SecTools` - Top 125 Network Security Tools
`C/C++ Programming` - One of the main language for open source security tools
`.NET Programming` - A software framework for Microsoft Windows platform development
`Shell Scripting` - Command-line frameworks, toolkits, guides and gizmos
`Ruby Programming by @dreikanter` - The de-facto language for writing exploits

`JavaScript Programming` - In-browser development and scripting
`Node.js Programming by @sindresorhus` - JavaScript in command-line
`Node.js Programming by @vndmtrx` - JavaScript in command-line
`Python tools for penetration testers` - Lots of pentesting tools are written in Python
`Python Programming by @svaksha` - General Python programming
`Python Programming by @vinta` - General Python programming
`Android Security` - A collection of android security related resources
`Awesome Awesomness` - The List of the Lists

Contribution

Your contributions and suggestions are heartily♥ welcome. (✿◕‿◕)

License