Hacking Articles

Raj Chandel's Blog

Penetration Testing

Linux Privilege Escalation using Misconfigured NSF

Linux Privilege Escalation using Sudo Rights

Capture NTLM Hashes using PDF (Bad-Pdf)

Privilege Escalation in Linux using etc/passwd file

Compressive Guide to File Transfer (Post Exploitation)

SNMP Lab Setup and Penetration Testing

6 Ways to Hack SNMP Password

Comprehensive Guide to SSH Tunnelling

4 ways to Hack MS SQL Login Password

Subscribe to Blog via Email

Enter your email address to subscribe to this blog and receive notifications of new posts by email.

Email Address

SUBSCRIBE

Nmap Scan with Timing Parameters

Comprehensive Guide to Crunch Tool

Spawn TTY Shell using Msfvenom (One Liner Payload)

6 Ways to Hack VNC Login Password

6 Ways to Hack PostgresSQL Login

5 Ways to Hack MySQL Login Password

Bypass SSH Restriction by Port Relay

Generating Scan Reports Using Nmap (Output Scan)

Port Scanning using Metasploit with IPTables

Understanding Guide to Mimikatz

Understanding Guide for Nmap Timing Scan (Firewall Bypass)

Understanding Guide for Nmap Ping Scan (Firewall Bypass)

Manual Post Exploitation on Windows PC (Network Command)

Sessions Command in Metasploit

Comprehensive Guide to Nmap Port Status

Bind Payload using SFX archive with Trojanizer

Beginner Guide to IPtables

Post Exploitation Using WMIC (System Command)

Bypass Firewall Restrictions with Metasploit (reverse_tcp_allports)

Manual Post Exploitation on Windows PC (System Command)

Categories

- BackTrack 5 Tutorials
- Best of Hacking
- Browser Hacking
- Cryptography & Stegnography
- CTF Challenges
- Cyber Forensics

- Nmap Scans using Hex Value of Flags
- Forensic Investigation of Nmap Scan using Wireshark
- Post Exploitation in Windows using dir Command
- How to Configure Suricata IDS in Ubuntu
- Detect SQL Injection Attack using Snort IDS
- Check Meltdown Vulnerability in CPU
- Network Packet Forensic using Wireshark
- ICMP Penetration Testing
- TCP & UDP Packet Crafting with CatKARAT
- DOS Attack with Packet Crafting using Colasoft
- Packet Crafting with Colasoft Packet Builder
- DHCP Penetration Testing
- DOS Attack Penetration Testing (Part 2)
- DOS Attack Penetration Testing (Part 1)
- How to Detect NMAP Scan Using Snort
- Understating Guide of Windows Security Policies and Event Viewer
- Configure Snort in Ubuntu (Easy Way)
- Post Exploitation for Remote Windows Password
- Configuring Snort Rules (Beginners Guide)
- Security Onion Configuration in VMware

- Database Hacking
- Domain Hacking
- Email Hacking
- Footprinting
- Hacking Tools
- Kali Linux
- Nmap
- Others
- Penetration Testing
- Social Engineering Toolkit
- Trojans & Backdoors
- Website Hacking
- Window Password Hacking
- Windows Hacking Tricks
- Wireless Hacking
- Youtube Hacking

Facebook Page

Understanding Guide to Nmap Firewall Scan (Part 2)

Command Injection Exploitation using Web Delivery (Linux, Windows)

IDS, IPS Penetration Testing Lab Setup with Snort (Manaually)

Android Mobile Exploitation with Evil-Droid

Understanding Guide to Nmap Firewall Scan (Part 1)

Msfvenom Tutorials for Beginners

7 Ways to Privilege Escalation of Windows 7 PC

Exploiting Remote Machine with Pastejacking

Exploiting Windows Machine with DDE Exploit

Wifi Post Exploitation on Remote PC

Beginner Guide to Classic Cryptography

WiFi Exploitation with WifiPhisher

Comprehensive Guide to Sniffing

4 Ways to Capture NTLM Hashes in Network

MSSQL Peneration Testing using Nmap

MS-SQL Penetration Testing lab Setup

Post Exploitation in VMware Files with Meterpreter

Lab Setup for VOIP Penetration Testing

Understanding Guide to ICMP Protocol with Wireshark

Time Scheduling on SSH Port

4 Ways to DNS Enumeration

Understanding Log Analysis of Web Server

Configure Web Server for Penetration Testing (Beginner Guide)

Understanding Nmap Scan with Wireshark

Bypass UAC in Windows 10 using bypass_comhijack Exploit

Setup DNS Penetration Testing Lab on Windows Server 2012

How to Secure Port using Port Knocking

6 Ways to Hack SSH Login Password

Vulnerability Analysis in Web Application using Burp Scanner

3 ways to scan Eternal Blue Vulnerability in Remote PC

5 Ways to Crawl a Website

Beginner Guide to Meterpreter (Part 1)

Bypass UAC Protection of Remote Windows 10 PC (Via FodHelper Registry Key)

Bypass Admin access through guest Account in windows 10

Hack Legal Notice Caption of Remote PC

Exploit Windows PC using EternalBlue SMB Remote Windows Kernel Pool Corruption

Create SSL Certified Meterpreter Payload using MPM

5 Ways to Directory Bruteforcing on Web Server

Exploit Remote PC using Microsoft Office Word Malicious Hta Execution

How to use Public IP on Kali Linux

Exploit Remote Windows PC with Eternalblue & Doublepulsar Exploit in Metasploit

Hack the billu: b0x VM (Boot2root Challenge)

Embedded Backdoor with Image using FakeImageExploiter

2 ways to use Msfvenom Payload with Netcat

Server Side Injection Exploitation in bWapp

Exploit Windows 10 PC with Microsoft RTF File (CVE-2017-0199)

How to Detect Sniffer in Your Network using shARP

Exploit Windows 7 PC using Torrent File

Dump Cleartext Password in Linux PC using MimiPenguin

Mobile Forensics Investigation using Cellebrite UFED

Stealing Windows Credentials of Remote PC with MS Office Document

Bypass Windows Login Password using Android Phone with DriveDroid

Capture VNC Session of Remote PC using SetToolkit

How to Delete Firewall Log in Remote PC using Metasploit

How to Enable and Monitor Firewall Log in Windows PC

Run OS Command against Multiple Session in Metasploit

Hiding Shell with Prepend Migrate using Msfvenom

Shell to Meterpreter using Session Command

Capture VNC Session of Remote PC using Msfvenom

How to Upgrade Command Shell to Meterpreter

How to set and Bypass Outbound Rule in Windows Firewall using Metasploit

How to Secure Your Port using Port Forwarding

Hack Remote PC with Apache OpenOffice Text Document Malicious Macro Execution

Shell Uploading in Web Server through PhpMyAdmin

Expoit Windows PC using Firefox nsSMIL Time Container: :Notify Time Change() RCE

Web Penetration Testing with Tamper Data (Firefox Add-on)

Brute Forcing Multiple Databases using HexorBase

Hack Remote PC using PSEXEC Injection in SET Toolkit

Hack Admin Access of Remote windows 10 PC using Eventvwr Registry Key Exploit

Penetration Testing in Metasploitable 3 with SMB and Tomcat

Exploitation of Metasploitable 3 using Glassfish Service

Manual Penetration Testing in Metasploitable 3

Hack Metasploitable 3 using Mysql Service Exploitation

Perform DOS Attack on Metasploitable 3

Hack Metasploitable 3 using SMB Service Exploitation

Metasploitable 3 Exploitation using Brute forcing SSH

Hack Metasploitable 3 using Elasticsearch Exploit

FTP Service Exploitation in Metasploitable 3

Get Meterpreter Session of Locked PC Remotely (Remote Desktop Enabled)

Hack Locked PC in Network using Metasploit

4 Ways to get Linux Privilege Escalation

Capture Images in Mobile using Driftnet through Wifi Pumpkin

Hack Android Phone using HTA Attack with QR Code

Exploit Windows 10 pc using WinaXe 7.7 FTP Client Remote Buffer Overflow

Play Youtube videos as background sound in Remote PC using Xerosploit

Hack ALL Linux Kernel using Dirtycow Exploit (Privilege Escalation)

Hack Remote Windows 10 PC using HTA Web Server

Hack any Android Phone using Spade APK Backdoor

Hijacking Gmail Message on Air using Burpsuite

Hack Android Phone using Backdoor Apk

Build an Android Penetration Testing lab

Hack Admin Access of Remote Windows 10 PC using TpmInit UACBypass

Penetration Testing Skills Practice with Metasploitable (Beginner Guide)

Setup VPN Penetration Testing Lab in Server 2008

Fun with Metasploit Payloads

Hack Remote Windows PC using Office OLE Multiple DLL Hijack Vulnerabilities

How to Detect Meterpreter in Your PC

Password Cracking using Nmap

Control Remote PC using PSTools

A New Way to Hack Remote PC using Xerosploit and Metasploit

4 ways to Connect Remote PC using SMB Port

5 Ways to Hack SMB Login Password

Penetration Testing in SMB Protocol

Penetration Testing in Active Directory using Metasploit (Part 2)

Hack Remote Windows PC using DLL Files (SMB Delivery Exploit)

Get Admin Access of Remote Windows PC using MS16-016 mrxdav.sys WebDav Escalation

Perform Man in the Middle Attack in Network using Xerosploit

Hack Remote Windows 10 PC using TheFatRat

Firewall Pentest Lab Setup with pfsense in VMware

Proxy Server Lab Setup using Wingate (Part 2)

Wifi Penetration Testing in Remote PC (Part 1)

Proxy Server Lab Setup using Wingate (Part 1)

How to Setup Cloud Computing Penetration Testing Lab

Penetration Testing in Windows Server Active Directory using Metasploit (Part 1)

Capture VNC Session of Remote Windows PC by Payloads Injection

Gather Credential of WebNMS Framework Server using Metasploit

Hack Remote Windows PC using Macros with Msfvenom

Hack Web Server using Tiki Wiki Unauthenticated File Upload Vulnerability

Hack Remote PC using Malicious MS Office Documents

Hack Web Server using PHP Command Injection (Smplshllctrlr)

Exploit Remote Server using Tiki-Wiki CMS Calendar Command Execution

Hack Remote Windows PC using Regsvr32.exe (.sct) Application Whitelisting Bypass Server

Hack Wifi using Evil Twin Method with Linset in kali Linux

OpenSSH User Enumeration Time-Based Attack with Osueta

Hack Password using Rogue Wi-Fi Access Point Attack (WiFi-Pumpkin)

Wifi Penetration Testing using Gerix Wifi Cracker

Hack Remote PC using Microsoft Office Files (Macro Payloads)

Hack Locked Workstation Password in Clear Text

Penetration Testing in Windows/Active Directory with Crackmapexec

Hack Untangle NG Firewall using command Injection Vulnerability

How to Detect Sniffer on Your Network

3 Ways to Crack Wifi using Pyrit, oclHashcat and Cowpatty

Crack Wifi Password using Aircrack-Ng (Beginner’s Guide)

Hack Any Android Phone with DroidJack (Beginner’s Guide)

5 Ways to Surf Internet Anonymously in Android Phone

Exploit Linux PC using IPFire Bash Environment Variable Injection (Shellshock)

HTTP RAT Tutorial for Beginners

5 ways to Create Permanent Backdoor in Remote PC

Exploitation in Linux Firewall using IPFire proxy.cgi RCE

Detect Hacker in Network using Android Phone

Cracking WiFi Password using Fern WIFi Cracker

Hack Wi-Fi using Social Engineering with Fluxion (Evil Twin Attack)

Hack Wireless Network using Airgeddon

How to Create Botnet for D-Dos Attack with UFONet

Automating Exploitation of Remote PC using Metasploithelper

Hack Remote PC using BrowserBackdoor – JavaScript WebSocket Backdoor

Hack your Network through Android Phone using cSploit

Bypass All Antivirus and Hack Remote Windows 10 PC using Hercules

Hack Remote PC with Reverse PowerShell using Brosec

Hack Gmail and Facebook Password in Network using Bettercap

Access Sticky keys Backdoor on Remote PC with Sticky Keys Hunter

Exploit Remote PC using Advantech WebAccess Dashboard Viewer upload Image Common Arbitrary File Upload

Hack Remote Windows PC using Dell SonicWALL Scrutinizer 11.01 methodDetail SQL Injection

Hack Remote Windows 10 PC using Cypher (Adding Shellcode to PE files)

Detect Vulnerability Scanner in Network using Kfsensor

How to identify Network Vulnerabilities using Nessus (Beginner Guide)

Detect Hacker in Network using kfsensor Honeypot

Hack Windows Server in Network using Atelier Web Remote Command

Information Gathering using Maltego (Beginner Guide)

Vulnerability Scanning in Network using Retina

Hack Web Server using ATutor 2.2.1 SQL Injection / Remote Code Execution

Hack Web Server using PHP Utility Belt Remote Code Execution

Weeman – HTTP Server for Phishing

Setup Firewall Pentest Lab using Clear OS

Hack Remote Windows PC using Office OLE multiple DLL side loading vulnerabilities

Hack Remote Linux PC using PHPFilemanager 0.9.8 Remote Code Execution

Pentest Lab Setup for Windows Server 2008 R2

Hack Remote Windows PC using PCMAN FTP Server Buffer Overflow – PUT Command

Hack Remote Windows PC using Easy File Sharing HTTP Server 7.2 SEH Overflow

Gather Browser and OS Information of Remote PC using Http Client Exploit

Hack Remote Windows 10 Password in Plain Text using Wdigest Credential Caching Exploit

Finding Vulnerability in EasyCafe Server using Metasploit

Hack anyone’s Whatsapp through QR code (Working)

Finding Vulnerability in Server/Client using Nmap

Hack Wallpaper of Remote Android Phone using Metasploit

Hack Call Logs, SMS, Camera of Remote Android Phone using Metasploit

Hack Remote Windows 10 PC using JSRAT

DOS Attack in Network using Colasoft Packet Builder (Beginner Guide)

Setup Browser Based Framework for Web Penetration Testing in Kali Linux (Mantra Toolkit)

Setup Web Penetration Testing Lab using OWASP Mth3l3m3nt Framework

Web Penetration Lab Setup using Webgoat in kali Linux

Hack Remote Windows 10 PC using ARCANUS (Bypass All Antivirus)

Setup Web Pentest Lab using Broken Web Applications (Beginner Guide)

Exploit Windows 10 PC using msfven.sh Script

Web Hacking Lab Setup using DVNA in Kali Linux

Web Pentest Lab setup for Beginners using DVWS

How to Setup VyOS (Virtual Router Pentest Lab)

4 Ways to Hack Telnet Passsword

Wifi Forensic Investigation using Wifihistoryview

Hack Remote Windows 10 PC using Discover Tool

Hack Remote Linux PC using PHP File

6 Ways to Hack FTP Password

2 Ways to Hack Remote Desktop Password using kali Linux

Network Scanning using NMAP (Beginner Guide)

How to Configure Untangle Firewall for Network Security (Beginner Guide)

Exploit Remote Windows PC using PSploitGen

Hack Remote Windows 10 PC using psmsf

Hack Remote PC using Darkcomet RAT with Metasploit

Exploit Remote Windows PC using HTA Attack with Net Tools

Find the Vulnerable Router on Internet using RouterhunterBR

2 Ways to Hack Windows 10 Password Easy Way

Exploit Remote Windows PC using ps1encodeTool

3 ways to Capture HTTP Password in Network PC

Denial of Service Attack on Network PC using SET Toolkit

Hack Remote PC with Nettool MitM Pentesting Toolkit

Hack Gmail or Facebook Password of Remote PC using NetRipper Exploitation Tool

Exploitation of Windows PC using Venom: Shellcode Generator

Hack Remote PC with PHP File using PHPSploit Stealth Post-Exploitation Framework

Hack Remote Windows PC using VNC Keyboard Remote Code Execution

Hack Remote Windows or Linux PC using MPC

Privilege Escalation on Windows 7,8,10, Server 2008, Server 2012 using Potato

Hack Windows 7 Password from Guest Account using 2015-1701 Exploit (Easy Way)

Winpayloads: Undetectable Windows Payload Generation

SimplyEmail: Email Recon Tools (Email Footprinting)

Killchain: A Collection of Powerful Hacking Tools

How to Create unlimited Folder in Remote Victim PC using Metasploit

How to Access Unauthorized on Remote PC using Metasploit

How to Gather Information of Antivirus in Remote Victim PC using Metasploit

Hack Remote Windows PC using ManageEngine OpManager Remote Code Execution

Hack Remote Windows PC Manage Engine Desktop Central 9 File Upload Servlet Connection Id Vulnerability

Hack Gmail and Facebook of Remote PC using DNS Spoofing and SET Toolkit

Hack Remote PC using HTA Attack in SET Toolkit

Wifi Hacking with Evil Twin Attack using Linset

Hack Windows Password in Clear Text using Mimikatz and Windows Credentials Editor

Session Hijacking using Ettercap, Hamster and Ferret (A Beginner Guide)

Hack Remote PC using WinRAR SFX Remote Code Execution Vulnerability

Hack Remote Windows PC using The Backdoor factory with Metasploit

Hack Remote PC using Fake Updates Scam with Ettercap and Metasploit

Hacking with Empire – PowerShell Post-Exploitation Agent

How to Hack Windows Wallpaper of Remote PC

Hack Android Phone WhatsApp and all Directories using Mercury Browser Vulnerability

Hack Remote PC using Watermark Master Buffer Overflow (SEH)

Hack Remote PC using Pupy – Remote Administration Tool

How to show all Possible Exploits in Victim PC using Windows-Exploit-Suggester

Hack Remote Windows PC using PDF Shaper Buffer Overflow

Hack Remote Windows PC using Konica Minolta FTP Utility 1.00 Post Auth CWD Command SEH Overflow

Hack Remote Windows PC using MS15-100 Microsoft Windows Media Center MCL Vulnerability

How to Hack Saved sessions in Putty using Metasploit

Exploit Remote PC using Firefox PDF.js Privileged Javascript Injection

Windows 7 Sticky Key Hack Attack using Metasploit

Hack Remote Windows PC using Video Charge Studio Buffer Overflow (SEH)

Magic Unicorn – PowerShell Downgrade Attack and Exploitation tool

Exploit Remote PC using Adobe Flash Player ByteArray Use After Free

Exploit Remote PC using Adobe Flash opaque Background Use After Free

How to Gather WIFI Password in Remote Windows PC

Bypass Antivirus and Hack Remote Windows PC with shelter

Exploit Remote PC using Adobe Flash Player Nellymoser Audio Decoding Buffer Overflow

Exploit Remote PC using Adobe Flash Player Drawing Fill Shader Memory Corruption

Hack Browsers, Chat, Databases, Mails, Wifi Password in Remote Windows or Linux PC

Hack Remote Windows PC using Windows Client Copy Image Win32k Exploit

Hack the Password in Plain text of Remote Windows PC

Hack Saved Password in Windows and Linux PC using LaZagne Project

Exploit Remote PC using Adobe Flash Player ShaderJob Buffer Overflow

Exploit Remote PC using Adobe Flash Player domainMemory ByteArray Use After Free

Exploit Remote PC using Adobe Flash Player NetConnection Type Confusion

Exploit Remote PC using Adobe Flash Player Uncompress Via Zlib Variant Uninitialized Memory

Exploit Remote PC using Adobe Flash Player copy Pixels to ByteArray Integer Overflow

Exploit Remote PC using Adobe Flash Player PCRE Regex Vulnerability

Exploit Remote PC using Adobe Flash Player Byte Array with Workers Use after Free

Exploit Remote PC using Adobe Flash Player Byte Array Uncompress via ZlibVariant Use after Free

Exploit Remote Windows, Linux, OSX PC using Firefox Proxy Prototype Privileged JavaScript Injection

Hack Remote Windows PC using Publish-It PUI Buffer Overflow (SEH)

How to find the usage of files in Remote victim PC (Remote PC Forensics)

Hack Remote Windows Password using Phishing Login Prompt Exploit

Hack Remote Windows PC using Achat Unicode SEH Buffer Overflow

Hack Remote Windows PC using BulletProof FTP Client BPS Buffer Overflow

Hack Remote Windows PC using i-FTP Schedule Buffer Overflow

Network Penetration Testing using Android Phone (zANTI Tutorial Part 1)

Hack Saved LastPass Master Password in Remote Windows, Linux, MAC PC

Hack Remote Windows PC using Windows Track Popup Menu Win32k NULL Pointer Dereference

Hack Remote Windows PC using BadBlue Exploit

How to Gather Applied Patches in Remote Windows PC

Hack Remote Windows PC using Wing FTP Server Authenticated Command Execution

Exploit Remote Windows, Linux or MAC PC using Firefox WebIDL Privileged Javascript Injection

Exploit Remote Windows, Linux, MAC PC using Firefox to String console.time Privileged JavaScript Injection

How to Delete ALL Files in Remote Windows PC

Website Security Certificate Attack on Remote Windows PC

Best of Remote Windows PC Hacking Tricks (Part 1)

Hack ALL Security Features in Remote Windows 7 PC

How to Shutdown, Restart, Logoff, and Hibernate Remote Windows PC

Hack WIFI Setting of Remote Windows PC

Hack Remote Windows PC using Ericom AccessNow Server Buffer Overflow

How to Change ALL Files Extension in Remote PC (Confuse File Extensions Attack)

Hack Remote Windows PC using Easy File Management Web Server Stack Buffer Overflow

Gather Cookies and History of Mozilla Firefox in Remote Windows, Linux or MAC PC

Exploit Save Password in Mozilla Firefox in Remote Windows, Linux or MAC PC

How to Find ALL Excel, Office, PDF, and Images in Remote PC

How to Gather MUICache Entries in Remote Windows PC

How to Crash Running Wireshark of Remote PC using CAPWAP Dissector DoS

Gather WLAN Information and Geolocation of Remote Windows, Linux or MAC PC

Hack Remote Windows PC using Windows NT User Message Call Win32k Kernel Pool Overflow (Schlamperei)

Hack Remote PC using Wireshark wiretap/mpeg.c Stack Buffer Overflow

Hack Remote Victim PC with MS Office Document

Set New Password of Victim PC Remotely

Hack Remote Windows PC using WinRAR Filename Spoofing

How to Gather Skype Logs, Firefox History and Chrome history of Remote Victim PC

Pompem – Tool to Find Exploits in Major Database

Bypass UAC Protection of Remote Windows PC in Memory Injection

Hack Remote Windows PC using ALLPlayer M3U Buffer Overflow

Hack Internet Explorer in Remote PC set your desired Home page

Hack Remote Windows PC using Total Video Player 1.3.1 Buffer Overflow

How to Delete Passwords/Cookies/History/Temp Internet File of Internet Explorer in Remote Victim PC

Forensics Investigation of Remote PC (Part 2)

How to Lock Drive of Remote Windows Victim PC

Hack Remote Windows PC using Audiotran PLS File Stack Buffer Overflow

Hack Remote Windows PC using Easy CD-DA Recorder PLS Buffer Overflow

How to Perform Blue Screen Death Attack on Remote Windows 7 PC

Shrink the Partition of Remote Windows PC

Forensics Investigation of Remote PC (Part 1)

HackPack – Collection of Hacking Scripts

PwnSTAR: Pwn SofT Ap scRipt

LazyKali -script for Kali Linux

Hack Android Phone with Metasploit in Kali Linux

Remotely Scan Malware/Virus in Victim PC with Metasploit

Hack Remote Windows 7 PC Using IBM Forms Viewer Unicode Buffer Overflow

Hack Remote PC Using Real Networks RealPlayer Version Attribute Buffer Overflow

Hack Remote PC Using Adobe Reader ToolButton Use After Free

How to Broadcast YouTube Video in Remote Windows System

Hack Remote PC with Windows EPATHOBJ::pprFlattenRec Local Privilege Escalation

Hacked Remote PC Using Cool PDF Image Stream Buffer Overflow

Hack Remote PC using Open Office Exploit

Hacked Remote PC Using Digital Music Pad Version 8.2.3.3.4 Stack Buffer Overflow

Hack PC in Network using MJM Core Player 2011 .s3m Stack Buffer Overflow

Exploit PC in LAN using Shadow Stream Recorder 3.0.1.7 Buffer Overflow

Hack Remote PC Using MJM QuickPlayer 1.00 Beta 60a / QuickPlayer 2010 .s3m Stack Buffer Overflow

Get Admin Privilege of Remote Victim PC using Windows SYSTEM Escalation via KiTrap0D

Hack Remote PC Using Beetel Connection Manager NetConfig.ini Buffer Overflow

Hack PC in Network Using Microsoft Windows Theme File Handling Arbitrary Code Execution

Hack Remote Windows PC Using PCMAN FTP Server Post-Authentication STOR Command Stack Buffer Overflow

Hack Remote Windows PC Using A-PDF WAV to MP3 v1.0.0 Buffer Overflow

Exploit Remote Windows PC using Firefox XMLSerializer Use After Free

Access Kali Linux Remotely on Windows System through Putty

Hack Remote Windows or Linux PC with Java store Image Array() Invalid Array Indexing Vulnerability

Hack Remote PC using Intrasrv 1.0 Buffer Overflow

Hack Remote PC using MiniWeb (Build 300) Arbitrary File Upload

Exploit Windows PC using Ultra Mini HTTPD Stack Buffer Overflow

Hack Remote PC, IPhone, Android using XSSF in Metasploit

Hack FTP Remotely using Open-FTPD 1.2 Arbitrary File Upload

Hack Remote Windows 7 PC using Chasys Draw IES Buffer Overflow

XSSF Cross-Site Scripting Framework in Metasploit (Part 1)

Bypass Antivirus and Hack Remote Windows PC with Syringe

Hack Remote Windows PC using Apple Quicktime 7 Invalid Atom Length Buffer Overflow

Exploit Remote Windows PC using Corel PDF Fusion Stack Buffer Overflow

Hack Windows 7 PC Remotely using MediaCoder .M3U Buffer Overflow

Hack Windows 7 PC Remotely using ERS Viewer 2013 ERS File Handling Buffer Overflow

Hack Remote Windows PC using ABBS Audio Media Player .LST Buffer Overflow

Hack Windows, Linux or MAC PC using Java Applet Provider Skeleton Insecure Invoke Method

Hack Windows PC using Novell Client 4.91 SP4 nwfs.sys Local Privilege Escalation

Exploit Windows, Linux or MAC PC using Java Applet Driver Manager Privileged toString() Remote Code Execution

Hack Remote PC using Sun Java Web Start Double Quote Injection

How to Install Simple-Ducky Payload Generator

Veil – A Metasploit Payload Generator to Bypass Antivirus

Exploit Windows, Linux or MAC PC using Firefox 17.0.1 + Flash Privileged Code Injection

Hack Remote Windows PC Using AdobeCollabSync Buffer Overflow Adobe Reader X Sandbox Bypass

Recover Deleted Data from Remote Victim PC

Exploit Remote Windows PC using ERS Viewer 2011 ERS File Handling Buffer Overflow

Hack Windows PC using AudioCoder .M3U Buffer Overflow

Hack Remote Windows, Linux or MAC PC using Java Applet Reflection Type Confusion Remote Code Execution

Hack Remote PC using Free Float FTP Server USER Command Buffer Overflow

How to Encrypt Drive of Remote Victim PC

Hack Windows PC using Java CMM Remote Code Execution

How to Install Kali linux Step by Step Guide

Hack Windows PC using Firebird Relational Database CNCT Group Number Buffer Overflow

OWASP Xenotix XSS Exploit Framework v3 2013

Exploit Windows, Linux or MAC PC using Java Applet JMX Remote Code Execution

How to Gather Recent Files Dump of Remote PC

Hack netNTLM Credential using Microsoft Word UNC Path Injector

How to Lock/Unlock Folder in Remote Victim PC using Metasploit

Hack Remote Windows PC using VMWare OVF Tools Format String Vulnerability

How to Hide File in Remote Victim PC

Hack Remote Windows Password using Keylogger in Meterpreter

How to Check Enabled Remote Desktop Service in Network with Metasploit

Hack Remote Windows Passwords in Plain Text with WCE

Windows Manage Memory Payload Injection

Attacking on Windows, Linux or MAC PC using Java Applet Method Handle Remote Code Execution

Hack Windows, Linux or MAC PC using Java Applet AverageRangeStatisticImpl Remote Code Execution

Exploit Windows PC using Freesshd Authentication Bypass

Hack Windows, Linux or MAC PC using Java Applet JMX Remote Code Execution

Hack Windows PC using Orbital Viewer ORB File Parsing Buffer Overflow

Hack Windows PC using Cyber Link Power2Go name attribute (p2g) Stack Buffer Overflow Exploit

Hack Remote Windows PC using Real player RealMedia File Handling Buffer Overflow

How to Enable Remote Desktop in Victim PC using Metasploit

How to Hack Hosts File of Remote Windows 7 PC (Host File Injection)

How to Hack XAMPP of Remote PC using Metasploit

Bypassing Antivirus using Multi Pyinjector Shell Code Injection in SET Toolkit

Netdiscover – Active/Passive ARP Scanner

Hack Windows PC in Neiwork using FreeFloat FTP Server Arbitrary File Upload

Exploting Windws 7 PC using Maxthon3 about:history XCS Trusted Zone Code Execution

How to Delete Local User Account of Remote PC using Metasploit

Hack Windows 7 PC in LAN using Blaze Video HDTV Player Pro v6.6 Filename Handling Vulnerability

Hack Remote PC using Apple QuickTime 7.7.2 TeXML Style Element font-table Field Stack Buffer Overflow

Hack Remote Windows or Linux PC using Java Applet JAX-WS Remote Code Execution

Windows Gather Directory Permissions Enumeration

How to Install BeEF in Windows PC

Best of Metasploit Meterpreter Script

Best of JAVA Hacking Exploit

Hack Remote PC using Orbit Downloader URL Unicode Conversion Overflow

How to Gather Installed Application in Victim PC

How to Gather USB Drive History of Victim PC

How to Gather Windows Product Key of Remote victim PC

How to Gather Microsoft Outlook Saved Password in Remote PC

How to Hack Save Password in FileZilla of Remote PC

How to Detect Install OS in Victim Virtual BOX

Best of Mozilla Firefox Hacking Exploits

Pen Testing for iPhone Part 1

Hack Remote Linux PC using msfpayload in BackTrack

Cymothoa – Runtime shellcode injection Backdoors

How to Create a Backdoor in Server using BackTrack (Weevely Tutorial)

Webacoo – Web Backdoor Cookie Script-Kit

Hack Remote Windows PC using Open VPN Trusted Path Privilege Escalation

Hack Windows 7 PC using USB Device and SET Toolkit (Infectious Media Generator Attack)

PyInjector Shellcode Injection attack on Remote PC using Social Engineering Toolkit

Hack Remote PC using Microsoft Internet Explorer exec Command Use-After-Free Vulnerability

How to Find OS of Remote PC (OS Footprinting)

Hack Remote Windows PC using Ratte Server in Social Engineering Toolkit

Hack Remote Windows 7 PC using Winamp MAKI Buffer Overflow

Hack Remote Windows or Linux PC using Java 7 Applet Remote Code Execution

Hack Windows7 PC using Powershell Attack Vector in Social Engineering Toolkit (Bypassing Antivirus)

Attacking on Remote PC using Adobe Flash Player 11.3 Font Parsing Code Execution

Hack Remote Windows 7 PC Easy Way (Msfvenom Tutorial)

Hack Remote Windows PC using Microsoft Office word MS12-027 MSCOMCTL ActiveX Buffer Overflow

Hack Remote Windows 7 PC using global SCAPE Cute ZIP Stack Buffer Overflow

BlindElephant-Web Application Fingerprinter

Hack Remote Windows 7 PC using Simple Web Server Connection Header Buffer Overflow

Mutillidae (Web Pen-Test Practice Application)

Hack Remote Windows 7 PC using Microsoft XML Core Services MSXML Uninitialized Memory Corruption

Hack Remote PC using Java Applet Field Bytecode Verifier Cache Remote Code Execution

Hack Windows 7 PC with Poison Ivy 2.3.2 C&C Server Buffer Overflow

Hack Remote Windows PC using Apple QuickTime TeXML Stack Buffer Overflow

Hack Remote Windows PC using Adobe Flash Player Object Type Confusion

Hack Windows PC in LAN using Fat Player Media Player 0.6b0 Buffer Overflow

Hack Windows PC using Lattice Semiconductor PAC-Designer 6.21 Symbol Value Buffer Overflow

Hack Remote Windows PC using TFM MMPlayer (m3u/ppl File) Buffer Overflow

Hack Windows 7 using Microsoft Office Click Once Unsafe Object Package Handling Vulnerability

Hack Remote Windows PC using Video LAN VLC ModPlug ReadS3M Stack Buffer Overflow

Hack Remote XP PC using Microsoft Windows OLE Object File Handling Remote Code Execution

Hack Remote Windows PC using CCMPlayer 1.5 m3u Playlist Stack Based Buffer Overflow

Hack Remote Windows PC using Windows Media Encoder 9 wmex.dll ActiveX Buffer Overflow

Hack Remote Windows PC using Internet Explorer COM Create Object Code Execution

Exploit Remote Windows PC using Mozilla Firefox Interleaved document. write/append Child Memory Corruption

ExploitRemote Windows PC using Mozilla Firefox Array.reduceRight () Integer Overflow

Hack Windows PC in LAN using Internet Explorer Web View Folder Icon setSlice() Overflow

Hack Remote Windows PC using Microsoft DirectShow (msvidctl.dll) MPEG-2 Memory Corruption

Exploit Remote PC using Mozilla Firefox “nsTreeRange” Dangling Pointer Vulnerability

Hack Remote PC using Aviosoft Digital TV Player Professional 1.0 Stack Buffer Overflow

Wapiti – Web application vulnerability scanner

Hack Windows PC in Network using VLC Media Player Real Text Subtitle Overflow

Hack Remote Windows PC using MicroP 0.1.1.1600 (MPPL File) Stack Buffer Overflow

Hack Remote Windows PC using VUPlayer M3U Buffer Overflow

Hack Remote Windows PC using Foxit PDF Reader 4.2 JavaScript File Write Exploit

Hack Windows Remote PC using ispVM System XCF File Handling Overflow

Hack Windows PC using Apple QuickTime 7.6.6 Invalid SMIL URI Buffer Overflow

Hack Remote Windows XP using Sun Java Web Start Plugin Command Line Argument Injection

Hack Remote XP PC using Adobe util.printf() Buffer Overflow

Hack any PC in LAN using Adobe Doc.media.newPlayer Use After Free Vulnerability

Hack PC in LAN using Wireshark LWRES Dissector getaddrsbyname_request Buffer Overflow

Hack Remote Windows PC with AstonSoft DeepBurner (DBR File) Path Buffer Overflow

web-sorrow – A Remote Web Scanner for Version Detection, Misconfiguration, and Server Enumeration

Hack Windows PC using Awing Soft Winds3D Player 3.5 SceneURL Download and Execute

How to Create Backdoor in Remote PC (metsvc Tutorial)

Hack Remote Windows PC using Winamp Media Player

Hack Windows PC using Wireshark <= 1.4.4 packet-dect.c Stack Buffer Overflow (remote)

Attacking on Remote PC if Victim is using Wireshark

w3af -Web Application Attack and Audit Framework (Tutorial Part 1)

How to Capture Log with HTTP java Script Keylogger in Metaspolit

Hack Windows XP using Adobe Reader U3D Memory Corruption Vulnerability

Hack Windows PC using Foxit Reader 3.0 Open Execute Action Stack Based Buffer Overflow

Hack Remote Windows PC using ACDSee FotoSlate PLP File id Parameter Overflow

How to Attack on Remote PC using HTTP Code Injection Technique

Subterfuge (Man-in-the-Middle Attack Framework)

PentBox Tutorial (A Penetration Testing Tool)

Hack Remote PC using Visiwave VWR File Parsing Vulnerability

Hack Remote Windows XP using Xenorate 2.50 (.xpl) universal Local Buffer Overflow (SEH)

Hacking Windows XP with WebSploit

Hack Remote XP with Pro Show Gold v4.0.2549 (PSH File) Stack Buffer Overflow

How to Attack on Remote Windows PC using DVD X Player Exploit

Hack Remote Windows PC with Websploit Toolkit

How to Attacking on Remote PC Using Real VNC

Hack Remote Windows XP using StreamDown 6.8.0 Buffer Overflow

Exploit Windows XP with Firefox 8/9 Attribute Child Removed() Use-After-Free

How to Install WebSploit Toolkit in Backtrack

How to Hack Remote Web Browser with BeEF (Browser Exploitation Framework)

How to Hack Remote using PC Millenium MP3 Studio

How to Hack PC in LAN Network using MyMP3Player

How to Attacking on Remote PC using Firefox nsSVG Value Out-of-Bounds Access Vulnerability

Hack Remote Windows XP PC using VLC AMV Dangling Pointer Vulnerability

How to Hack Remote Windows 7 PC

Hack Remote PC with Internet Explorer Daxctle.OCX Key Frame Method Heap Buffer Overflow Vulnerability

Hack Remote PC using Windows ANI Load AniIcon() Chunk Size Stack Buffer Overflow (HTTP)

How to Get Access of Remote Victim PC using Internet Explorer create Text Range () Code Execution

Hack Windows XP in LAN with JavaScript OnLoad Handler Remote Code Execution

How to Hack Remote PC using McAfee Visual Trace ActiveX Control Buffer Overflow

How to Attacking on Remote PC using VLC Media Player Exploit

Hack Remote PC with Sun Java JRE AWT setDiffICM Buffer Overflow

Hack Remote Windows XP PC using Internet Explorer Winhlp32.exe MsgBox Code Execution

Hack windows PC with Internet Explorer CSS Set User Clip Memory Corruption Exploit

Hack Remote PC using Internet Explorer 7 CFunction Pointer Uninitialized Memory Corruption

How to Attacking on Windows PC in LAN using WinZip

Hacking Windows PC with Sun Java JRE get Sound bank file:// URI Buffer Overflow

How to Attack on Remote PC using Adobe PDF Escape EXE Social Engineering (No JavaScript)

Attacking on Remote Victim PC using Apple QuickTime PICT PnSize Buffer Overflow

Hack Remote Windows PC using Sun Java Calendar Deserialization Privilege Escalation

Hack Windows XP using Adobe Acrobat Bundled LibTIFF Integer Overflow

Attack on Remote PC with Adobe Collab.collect Email Info() Buffer Overflow

Hack Windows PC in LAN with TugZip 3.5 Zip File Parsing Buffer Overflow Vulnerability

Hack Windows PC in Network using Mini-Stream RM-MP3 Converter Buffer Overflow Attack

Hack any PC in LAN using MS Office Buffer Overflow Attack

Hack Windows PC with Java MixerSequencer Object GM_Song Structure Handling Vulnerability

How to Hack Remote PC using MP3 CD Ripper Exploit

How to Blue Screen Death Attack on Windows XP PC in LAN

How to Exploit Windows 7 PC in LAN Attacking on Mozilla Firefox

How to Hack Remote PC using Foxit Reader

Hack PC in LAN using EFS Easy Chat Server Buffer Overflow Attack

How to Hack Remote Victim PC with java Applet Rhino Script

How to Attack on Remote PC through Sun Java Web start Execution

How to Attack on Remote PC through PDF

How to Get Access of Remote PC through Real Player

Hack Remote PC with Sun Java Applet2ClassLoader Remote Code Execution

Hack PC in LAN with Sun Java Runtime Buffer Overflow Attack

Hacking with Java RMIConnectionImpl Deserialization Privilege Escalation Exploit

Hack Remote PC with java Trusted Chain Method

Hack Remote with PC Real Networks Real player QCP Parsing Heap Overflow Exploit

Hack Remote PC using Microsoft Help Center XSS

How to Hack Remote PC using Apple QuickTime

Hack Remote PC with Java AtomicReferenceArray Type Violation Vulnerability

Hack Remote Windows 7 PC Using UltraVNC Buffer Overflow Attack

Hack remote PC using Adobe CoolType SING Table “uniqueName” Stack Buffer Overflow

Hack Remote PC using Sun Java Command Line Injection

How to Change MAC Address in Backtrack5

Hack any Remote PC with Adobe JBIG2Decode Heap Corruption Exploit

How to Hack Remote PC using PDF

Hack Remote PC with Adobe Collab.getIcon() Buffer Overflow

Hack Remote PC with Operation Aurora Attack

How to Attack in LAN PC using Internet Explorer DHTML Behaviors

Hack Windows XP using Shell Link Code Execution

Hack Remote XP using Heap Overflow Attack

Hack windows 7 PC using MS11_003 Internet Explorer Exploit

How to Hide Drives of Remote PC using Metaspolit

Hack Windows PC using java Signed Applet Method

How to Create hidden user in Remote PC

How to use Keylogger in Meterpreter

Backtrack 5 Commands for Beginners (Part 1)

Hack Remote PC using Payload in BackTrack 5

How to Hack Windows 7 in LAN using Metaspolit

Antivirus Forensics Tools

How to Hack Email using Web Jacking Method

How to capture Screenshot of Remote PC with Metaspolit

CMS Explorer-Discover the CMS components behind the site

How to Extract Email Address of Domain using Metasploit

How to Hack Gmail, Facebook with Backtrack 5

Metasploit Tutorial for Beginners (Part 2)

How to Hack Windows XP in LAN using Backtrack 5

Metasploit Tutorial for Beginners (Part 1)

How to Set up Armitage in Backtrack 5

How to Dual Boot Backtrack 5 with Windows XP

Social Engineering Toolkit Tutorial-Backtrack 5

How to Find DNS using Backtrack 5

How to Install Backtrack 5 in Windows PC

How To Install Backtrack 5 from USB Drive

How to Install BackTrack 5 (Tutorial)

Backtrack 5

6 Comments → PENETRATION TESTING

SACHIN JOSEPH June 24, 2014 at 10:30 am

sir, didn’t get this folder/file (/root/.msf4/local/msf.pls)

i’m using kali linux 1.0.7.

can you plz tell me where i get this file in kali linux?

thank you.

REPLY ↓

RAJ CHANDEL June 24, 2014 at 2:00 pm

by default .msf4 is hidden in root directory press ctrl h

REPLY ↓

TAHIR May 18, 2015 at 9:17 pm

back track5 is no longer available can i install alternative it would be good be good for hacking kindly reply…..

REPLY ↓

RAJ CHANDEL May 19, 2015 at 5:28 am

use kali linux

REPLY ↓

PETER UBUNTU February 20, 2016 at 1:49 am

take a look at this post-exploitation auxiliary module to cover footprints left after a successfully exploitation 😉 https://sourceforge.net/p/msf-auxiliarys/discussion/general/thread/642cc0f1/?limit=25

REPLY ↓

SAM January 8, 2018 at 6:56 am

Oh.... Damn...

This Site is a treasure....

REPLY ↓

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment

Name *

Email *

Website

□

Save my name, email, and website in this browser for the next time I comment.

POST COMMENT

□ Notify me of new posts by email.