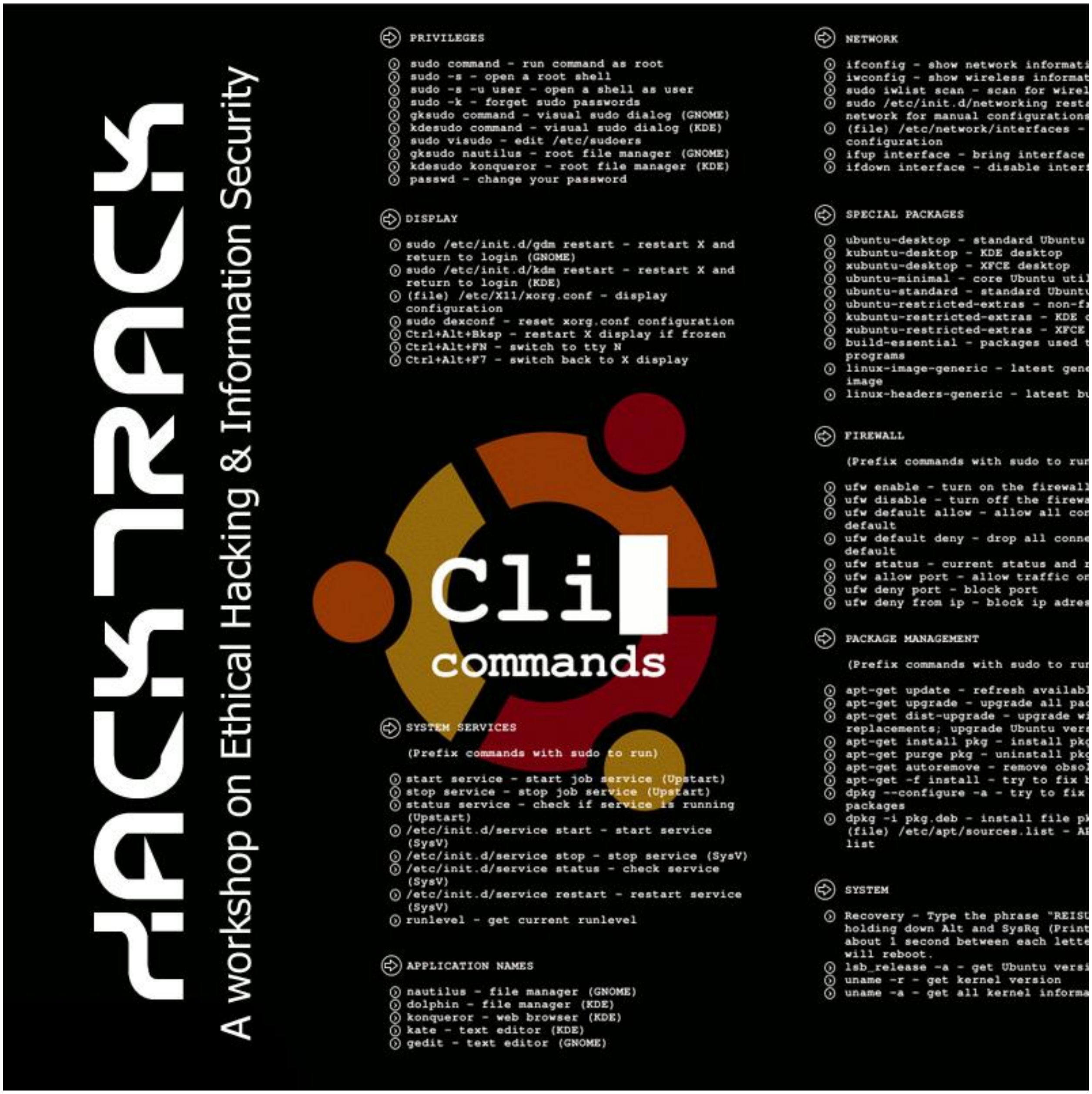

HACKTRACK

A workshop on Ethical Hacking & Information Security

Cli commands

PRIVILEGES

- sudo command - run command as root
- sudo -s - open a root shell
- sudo -s -u user - open a shell as user
- sudo -k - forget sudo passwords
- gksudo command - visual sudo dialog (GNOME)
- kdesudo command - visual sudo dialog (KDE)
- sudo visudo - edit /etc/sudoers
- gksudo nautilus - root file manager (GNOME)
- kdesudo konqueror - root file manager (KDE)
- passwd - change your password

DISPLAY

- sudo /etc/init.d/gdm restart - restart X and return to login (GNOME)
- sudo /etc/init.d/kdm restart - restart X and return to login (KDE)
- (file) /etc/X11/xorg.conf - display configuration
- sudo dexconf - reset xorg.conf configuration
- Ctrl+Alt+Bksp - restart X display if frozen
- Ctrl+Alt+FN - switch to tty N
- Ctrl+Alt+F7 - switch back to X display

SYSTEM SERVICES

(Prefix commands with sudo to run)

- start service - start job service (Upstart)
- stop service - stop job service (Upstart)
- status service - check if service is running (Upstart)
- /etc/init.d/service start - start service (SysV)
- /etc/init.d/service stop - stop service (SysV)
- /etc/init.d/service status - check service (SysV)
- /etc/init.d/service restart - restart service (SysV)
- runlevel - get current runlevel

APPLICATION NAMES

- nautilus - file manager (GNOME)
- dolphin - file manager (KDE)
- konqueror - web browser (KDE)
- kate - text editor (KDE)
- gedit - text editor (GNOME)

NETWORK

- ifconfig - show network informati
- iwconfig - show wireless informat
- sudo iwlist scan - scan for wirel
- sudo /etc/init.d/networking resta network for manual configurations
- (file) /etc/network/interfaces - configuration
- ifup interface - bring interface
- ifdown interface - disable interf

SPECIAL PACKAGES

- ubuntu-desktop - standard Ubuntu
- kubuntu-desktop - KDE desktop
- xubuntu-desktop - XFCE desktop
- ubuntu-minimal - core Ubuntu uti
- ubuntu-standard - standard Ubunt
- ubuntu-restricted-extras - non-f
- kubuntu-restricted-extras - KDE
- xubuntu-restricted-extras - XFCE
- build-essential - packages used programs
- linux-image-generic - latest gen image
- linux-headers-generic - latest bu

FIREWALL

(Prefix commands with sudo to run

- ufw enable - turn on the firewall
- ufw disable - turn off the firewa
- ufw default allow - allow all co default
- ufw default deny - drop all conne default
- ufw status - current status and
- ufw allow port - allow traffic o
- ufw deny port - block port
- ufw deny from ip - block ip adres

PACKAGE MANAGEMENT

(Prefix commands with sudo to run

- apt-get update - refresh availab
- apt-get upgrade - upgrade all pa
- apt-get dist-upgrade - upgrade w replacements; upgrade Ubuntu vers
- apt-get install pkg - install pk
- apt-get purge pkg - uninstall pk
- apt-get autoremove - remove obso
- apt-get -f install - try to fix
- dpkg --configure -a - try to fix packages
- dpkg -i pkg.deb - install file p (file) /etc/apt/sources.list - A list

SYSTEM

- Recovery - Type the phrase "REISU holding down Alt and SysRq (Print about 1 second between each lett will reboot.
- lsb_release -a - get Ubuntu vers
- uname -r - get kernel version
- uname -a - get all kernel inform

Workshop Session Schedule

Modules	Particulars	Duration (Hours)
1.	**Cyber Ethics** ✓ Hackers & hacking methodologies ✓ Types of hackers ✓ Communities of Hackers ✓ Malicious Hacker Strategies ✓ Steps to conduct Ethical Hacking ✓ Hiding your identity while performing attacks	**0.5**
2.	**Information Gathering & Scanning Methodologies** ✓ Get to know how hacker gather information about victim on internet ✓ Information gathering of websites & networks ✓ Scanning & Structuring of websites ✓ Finding Admin Panel of websites	**1.0**
3.	**Trojans, Backdoors** ✓ How to control victim’s computer using Trojans ✓ Binding Trojans with another file ✓ Undetection process of Trojans from Antivirus ✓ Removal of Trojans from your computer ✓ Analysis of Trojans/Virus	**0.5**

4.	**Google Hacking** ✓ Using Google as hacking tool ✓ Advanced operators of Google ✓ Finding Vulnerable websites using Google ✓ Finding Target networks using Google	**0.5**
5.	**Wireless Hacking & Security** ✓ Wireless Protocols ✓ Wireless Routers-Working ✓ Attacks on Wireless Routers ✓ Cracking Wireless routers password(WEP) ✓ Securing routers from Hackers ✓ Countermeasures	**0.5**
6.	**Mobile, VoIP Hacking & Security** ✓ SMS & SMSC Introduction ✓ SMS forging & countermeasures ✓ Sending & Tracking fake SMSes ✓ VoIP Introduction ✓ Installing VoIP Server ✓ Forging Call using VoIP	**2.0**

7.	**Web Application Attacks** ✓ Web Application Overview ✓ Web Application Attacks ✓ OWASP Top 10 Vulnerabilities ✓ Putting Trojans on websites ✓ SQL injection attacks ✓ Executing Operating System Commands ✓ Getting Output of SQL Query ✓ Getting Data from the Database Using ODBC Error Message ✓ How to Mine all Column Names of a Table ✓ How to Retrieve any Data ✓ How to Update/Insert Data into Database ✓ SQL Injection in Oracle ✓ SQL Injection in MySql Database ✓ Attacking Against SQL Servers ✓ SQL Server Resolution Service (SSRS) ✓ SQL Injection Automated Tools ✓ Blind SQL Injection ✓ Preventing SQL Injection Attacks ✓ XSS attacks ✓ Finding & Fixing XSS in websites ✓ Local File inclusion attacks ✓ Remote file inclusion attacks ✓ Buffer Overflow attacks ✓ Session Hijacking attacks ✓ 20 Hands on Demonstrations on real websites ✓	**4.0**
8.	**System & Network hacking** ✓ Hacking Administrators password ✓ Enumeration of networks ✓ Use of Sniffers to sniff network data.	**1.0**

9.	**Email Hacking** ✓ Making fake pages ✓ How to use keyloggers to hack mail ids ✓ Social Engineering Techniques	**1.0**
10.	**Introduction to Cyber Crime Investigation** ✓ Types of Cyber Crimes ✓ Report Cyber Crimes	**1.0**
11.	**Investigation Methodologies** ✓ Different Logging Systems ✓ Investigating Emails (Email Tracing) ✓ Ahmedabad Bomb Blasts Terror Mail case study ✓ Investigating Phishing Cases ✓ Investigating Data Theft Cases ✓ Investigating Orkut Profile Impersonation Cases ✓ Cyber Law & IT Act,2000	**2.0**
12.	**Difficulty Handling Session & Exam 2.0**	**2.0**
	Total Hours	**16.0**

Note: These are just the major aspects that we will be discussing, each point will be elaborated in detail with demonstrations of the tools and techniques

Program Benefits & Highlights

- ✓ Learn & Interact with renowned Industry Experts
- ✓ Receive an unparalleled education on the art of computer security with personal one-on-one attention from Sunny Vaghela.
- ✓ Hands on Demonstrations of Latest Hacking Techniques & Tools.
- ✓ Hands on Demonstrations of various cases solved by Sunny Vaghela.
- ✓ PowerPoint Presentation, Live Demos, Interactive Question & Answer sessions and comprehensive reading material.
- ✓ Toppers of each workshop to be personally interviewed Sunny Vaghela and will receive a chance to work with him on security projects.

Key points of TechDefence

- ✓ We have rich experience working on cases & training for Crime Branch, Ahmedabad, Rajkot, Surat, Nashik & Hyderabad.
- ✓ Conducted more than 160 workshops & seminars for Students & Professionals across globe.
- ✓ We helped Top Investigating Agencies to solve Cyber Terrorism Cases like Ahmedabad & Mumbai Blasts Cases.
- ✓ We do not use third party tools. We have developed our Crypters, Trojans, and Scripts etc.
- ✓ Our Director & Trainer is supported by Ministry of Home Affairs, Malaysia.

Workshop Trainer

Sunny Vaghela (To know more about Sunny Vaghela please visit www.sunnyvaghela.com)

Course material & CDs

✓ Comprehensive course material will be provided to participants.

✓ Ethical Hacking Toolkit worth Rs.500 (Containing Tools, Videos, EBooks, Presentations)

Course Duration

✓ 2 Days (8 hours/day).

Fees & Certification

✓ Rs. 1100 Rs/Participant (This includes Registration Kit, Ethical Hacking Toolkit, and Course Material).

✓ Certificate of "**Certified Ethical Hacking Expert – Level 1**" will be given to participants from **TechDefence & Techfest, IIT Bombay.**

Contact Details

If you have any queries, Kindly contact us on hacktrack@techdefence.com

Vikalp Mehta,
TechDefence Pvt Ltd,
Mobile: +91 8128031223, 9974673864
Email: vikalp@techdefence.com