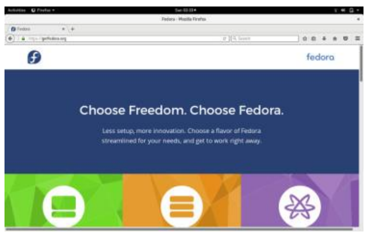
SUNNY TIMES DAILY NEWS PORTAL
www.sunnytimes.in

Daily News and Views Online TV & Cyber media. “Blunt and Sharp Daily News Portal” Sunday 04-03-2018 Portal Website with online news daily at: sunnytimes.in Mobile: 9945116476

M.S.Yatnatti : Editor and Video Journalist: “Blunt and Sharp Daily News Portal” : Swarnamba .R.L Freelance Video Journalist and Reporter

TO CONTROL CYBERCRIME USE “KALI LINUX” 2018.1 AND FEDORA 27 SECURITY LAB AND BACKBOX LINUX- 5 “FOR SECURITY AUDITING”

KALI LINUX™
"the quieter you become, the more you are able to hear"
PENETRATION TESTING, RE-DEFINED
A Project By Offensive Security



Choose Freedom. Choose Fedora.

Less setup, more innovation. Choose a flavor of Fedora streamlined for your needs, and get to work right away.

By : M.S.Yatnatti: Editor and Video Journalist Bengaluru : Prevention is always better than cure. It is always better to take certain precaution while operating the net. Cyber crime refers to any criminal activity that takes place over the Internet. Examples include fraud, malware such as viruses, identity theft and cyber stalking. Never open suspicious documents. Don't give out personal information to people you don't know. And be wary when approached with a suspicious proposition. You can also configure your computer to stop potential cyber criminals from gaining access to sensitive information. Use strong passwords on your accounts that are difficult to guess. Include both letters and numerals in your passwords. Never use a word that is easy to guess -- like your wife's name. Precaution, Prevention, Protection, Preservation and Perseverance for online security. Website owners should watch traffic and check any irregularity on the site. Putting host-based intrusion detection devices on servers will serve the purpose. It is not possible to eliminate cyber crime from the cyber space. It is quite possible to check them. History is the witness that no legislation has succeeded in totally eliminating crime from the globe. The only possible step is to make people aware of their rights and duties and to guard ourselves so that crime has no effect on us.The experts said companies must have a chief cyber security officer and data systems should function on a need to know basis. Recent revelations about leakage of Aadhaar da ta and corresponding transaction data are serious concerns as government is integrating Aadhaar number to various services,“ the study said.Pointing out that post-demonetisation, digital wallets such as PayTM and BHIM gained prominence, last year also saw cyber attacks that compromised more than 3 million ATM and debit cards through Hitachi-engineered ATM machine hacking.The experts said a wider net needed to be cast by the Indian banking system and the government to engage cyber security experts from top institutes as advanced layer of protection was missing in most financial institutions. Quoting a report, the IIT-K experts said India may need $4 billion investment in the private-public model.In its recommendations, the experts said companies must have a chief cyber security officer and data systems should function on a need to know basis. The experts felt that existing cyber security frameworks like CERT-IN was inadequate as there were insufficient inter-disciplinary connections and the governmentprivate sector partnership was neither deep enough nor did it provide the required expertise. New police chief and commissioer of Bengaluru Police T Suneel Kumar conceded on reportedly speaking to reporters that the police force is illequipped to deal with increasing cybercrimes, but said the problem was not unique to the country's IT capital alone .“Cybercrime is increasing across the world and in the country too. The police department is establishing a separate cyber cell in each police station across the state to tackle these cases. There needs to be renewed focus on training,“ Kumar said soon after taking charge. He said: “Special attention will be given to cyber security and we''ll train our personnel.We'll rope in experts from various fields to help us.“.The corporate need to appoint chief information security officers to control cyber crime risks.Demonetisation and the subsequent push for digitisation has reportedly escalated risks relating to cybercrime and reportedly India needs to urgently upgrade its defenses by setting up a cyber security commission on the lines of the Atomic Energy and Space Commissions, according to an IIT-Kanpur study shared with Parliament's committee on finance.Noting that the government has initiated a number of programmes to enhance the participation of citizens in the fully digitalised economy , the study said cyberse curity centres set up by the Reserve Bank of India (RBI) would be insufficient. “While RBI centres often come to IITs such as IIT-Kanpur for expert opinion, IITs do not engage in relevant research on cybersecurity,“ the study said. Incidents of cybercrime in India are rising sharply, recording an increase of over 100% in 2015 from 2014. The number grew from 71,780 in 2013 to 1.49 lakh in 2014 to 3 lakh in 2015. The study said attacks from the `Equation group' -which WikiLeaks reports said was a clandes tine CIA and NSA programme -infected India's telecom and military sectors and research institutes.The committee was briefed by Profs Manindra Agrawal and Sandeep Shukla from IIT-Kanpur (IIT-K). The study pointed out that since the government was pushing Aadhaar-based financial transactions, securing the Aadhaar database against unauthorised usage must be looked at carefully .It has come to light that certain banks were making hundreds of transactions on the Aadhaar numbers of unsuspecting citizens.

BackBox Linux-5 Arrived: it is a penetration testing and security assessment oriented Linux distribution . Designed to be fast, easy to use and provide a minimal yet complete desktop environment, thanks to its own software repositories that are constantly updated to the latest stable version of the most popular and best known ethical hacking tools.BackBox is more than an operating system, it is a Free Open Source Community project with the aim to promote the culture of security in IT environment and give its contribute to make it better and safer. All this using exclusively Free Open Source Software by demonstrating the potential and power of the community. BackBox Linux is an Ubuntu-based distribution designed for penetration testing and security evaluations. The Backbox distribution is designed to be fast and easy to use with a wide collection of security utilities. It provides a minimal yet complete desktop environment The BackBox project has announced the release of a new version, BackBox 5.

Reportedly The Fedora Project is pleased to announce the immediate availability of Fedora 27, the next big step our journey into the containerized, modular future. Fedora is a global community that works together to lead the advancement of free and open source software. As part of the community’s mission the project delivers three editions, each one a free, Linux-based operating system tailored to meet specific use cases: Fedora 27 Atomic Host, Fedora 27 Server, and Fedora 27 Workstation. Each edition is built from a common set of base packages, which form the foundation of the Fedora operating system. As with all new versions of Fedora, Fedora 27 provides many bug fixes and tweaks to these underlying components, as well as new and enhanced packages, including: Docker 1.12 for building and running containerized applications.Node.js 6.9.1, the latest version of the popular server-side JavaScript engine. Support for Rust, a faster and more stable system programming language.PHP 7, offering improved performance and reduced memory usage.Multiple Python versions — 2.6, 2.7, 3.3, 3.4 and 3.5 — to help run test suites across several Python configurations, as well as PyPy, PyPy3, and Jython. *Reportedly* Open source is making things easier for security professionals. But choosing software to check vulnerabilities still seems difficult for many developers. *Fedora Security Lab is* ***an RPM-based distro.*** *Kali Linux is* ***Debian based Linux distribution.***The Fedora Security Lab provides a safe test environment to work on security auditing, forensics, system rescue and teaching security testing methodologies in universities and other organizations.The spin is maintained by a community of security testers and developers. It comes with the clean and fast Xfce Desktop Environment and a customized menu that provides all the instruments needed to follow a proper test path for security testing or to rescue a broken system. The Live image has been crafted to make it possible to install software while running, and if you are running it from a USB stick created with LiveUSB Creator using the overlay feature, you can install and update software and save your test results permanently. The Fedora Security Lab provides a safe test environment to work on security auditing, forensics, system rescue and teaching security testing methodologies in universities and other organizations.The spin is maintained by a community of security testers and developers. It comes with the clean and fast Xfce Desktop Environment and a customized menu that provides all the instruments needed to follow a proper test path for security testing or to rescue a broken system. The Live image has been crafted to make it possible to install software while running, and if you are running it from a USB stick created with LiveUSB Creator using the overlay feature, you can install and update software and save your test results permanently.

Kali Linux rolling distribution (2018.1) is a Debian based Linux distribution aimed at advanced penetration testing and security auditing including forensic and reverse engineering. Kali contains several hundred tools which are geared towards for various information security tasks such as penetration testing ,security research ,computer forensic and reverse engineering. Security of networks is very important .offensive security is best for defense. The latest release comes with updated packages and updated kernel that provide better hardware support .This fine release contains all updated packages and bug fixes since the 2017 .3 release .Kali Linux has a shiney new 4.14.12 Linux Kernel. You can find complete documentation and the user guide at http://docs.kali.org The Kali Linux rolling distribution released. Kali switched to a rolling release model back when they hit version 2.0 (codename “sana”), however the rolling release was only available via an upgrade from 2.0 to kali-rolling for a select brave group. After 5 months of testing their rolling distribution (and its supporting infrastructure), they were confident in its reliability – giving users the best of all worlds – the stability of Debian, together with the latest versions of the many outstanding penetration testing tools created and shared by the information security community.The automated notification system of updated penetration testing tool releases has been working well over the past 5 months and has ensured that the kali-rolling repository always holds the latest stable releases of monitored tools. This usually leaves a gap of around 24-48 hours from notification of a new tool update, to its packaging, testing, and pushing into thier repositories. They would also like to introduce our new Kali Linux Package Tracker which allows you to follow the evolution of Kali Linux both with email updates and a comprehensive web interface.Kali Linux rolling distribution (2016.1) is a Debian based Linux distribution aimed at advanced penetration testing and security auditing including forensic and reverse engineering.Kali contains several hundred tools for various information security tasks including forensic and reverse engineering . Security of networks is very important .offensive security is best for defense .

The BackTrack is re-born as Kali Linux is a GPL-compliant Linux distribution built by penetration testers for penetration testers with development staff consisting of individuals spanning different languages, regions, industries, and nationalities. The evolution of Kali took place over many years of development, penetration tests, and unprecedented help from the security community. Kali Linux originally started with earlier versions of live Linux distributions called BackTrack, Whoppix, IWHAX, and Auditor.When it was initially developed, Kali was designed to be an all-in-one live CD to be used on security audits and was specifically crafted to not leave any remnants of itself on the system. With millions of downloads, it has become the most widely adopted penetration testing framework in existence and is used by the security community all over the world including Governments defence establishments.Kali Linux is an open source project that is maintained and funded by Offensive Security, a provider of world-class information security training and penetration testing services.In addition to Kali Linux, Offensive Security also maintains the Exploit Database and the free online course, Metasploit Unleashed.

After almost two years of public development (and another year behind the scenes), Kali Linux Developers announced their first point release of Kali Linux – version 1.1.0. This release brings with it a mix of unprecedented hardware support as well as rock solid stability. For us, this is a real milestone as this release epitomizes the benefits of their move from BackTrack to Kali Linux over two years ago. As they look at a now mature Kali, they see a versatile, flexible Linux distribution, rich with useful security and penetration testing related features, with over 300 hundred penetration testing tools and running on all sorts of weird and wonderful ARM hardware. But enough talk, here are the goods :The new release runs a 4.0 kernel, patched for wireless injection attacks.Our ISO build systems are now running off live-build 4.x.Improved wireless driver support, due to both kernel and firmware upgrades.NVIDIA Optimus hardware support.Updated virtualbox-tool, openvm-tools and vmware-tools packages and instructions.A whole bunch of fixes and updates from our bug-tracker changelog.And most importantly, we changed grub screens and wallpapers!.Founded in 2007, Offensive Security was born out of the belief that the best way to achieve sound defensive security is through an offensive approach. The team is made up of security professionals with extensive experience with attacking systems to see how they respond. They share this information through trainings, free tools, and publications.The strong technical foundation of the Offensive Security training content, coupled with a rigorous testing process has established the OSCP certification as the most relevant education in the pen-testing space. Accuvant LABS requires any prospective consultants to pass the OSCP exam before applying to our attack & penetration team. With the motto “Try Harder ®”, the Company’s trainings and certifications are well-respected and considered amongst the most rigorous available, creating a model adopted across the industry. In addition, the Exploit Database, Metasploit Unleashed, and BackTrack Linux community projects are highly-regarded and used by security teams in governmental and commercial organizations across the world.

Penetration Testing with Kali Linux is the Offensive Security flagship course, designed and written by the Kali Linux developers themselves. With years of experience in penetration testing, security research, tool development, and International Black Hat trainings, we have the experience and passion to teach you all about penetration testing. Penetration Testing with Kali Linux is also the only official security course revolving around the Kali Linux distribution.Unlike most security training programs and certification, “Penetration Testing with Kali Linux” is a performance based online course. Our certification process does not involve easy to remember multiple choice questions, but rather hands on penetration testing of live machines in a controlled, monitored lab environment. This makes the OSCP certification one of the hardest, and most sought after, professional certifications in the field.Seven years of developing BackTrack Linux has taught us a significant amount about what we, and the security community, think a penetration testing

==

distribution should look like. We've taken all of this knowledge and experience and implemented it in our "next generation" penetration testing distribution.After a year of silent development, Offensive Security is proud to announce the release and public availability of "Kali Linux", the most advanced, robust, and stable penetration testing distribution to date.Kali is a more mature, secure, and enterprise-ready version of BackTrack Linux. Trying to list all the new features and possibilities that are now available in Kali would be an impossible task on this single page. Therefore you to visit new Kali Linux Website and Kali Linux Documentation site to experience the goodness of Kali for yourself. Penetration Testing with Kali Linux (PWK) is an online training course designed for network administrators and security professionals who need to acquaint themselves with the world of offensive information security. This penetration testing training introduces the latest hacking tools and techniques in the field and includes remote virtual penetration testing labs for practicing the course materials. Penetration Testing with Kali Linux attempts to simulate a full penetration test, from start to finish, by injecting the student into a rich, diverse, and vulnerable network environment.Penetration Testing with Kali Linux is an entry-level course but still requires students to have certain knowledge prior to attending the class. A solid understanding of TCP/IP, networking, and reasonable Linux skills are required. This course is not for the faint of heart; it requires practice, testing, and the ability to want to learn in a manner that will grow your career in the information security field and defeat any learning plateau. Offensive Security challenges you to rise above the rest, dive into the fine arts of advanced penetration testing, and to Try Harder™.Challenge yourself with the highly respected OSCP certification exam where you get immersed in an unknown network and need to exploit the exam targets. Once you have completed the course, you're ready to take the certification challenge – a real-world, hands-on penetration test. You will be expected to dive into an unknown network and exploit weaknesses in order to pass the certification exam.

Practice your new-found skills in our realistic penetration testing labs containing multiple subnets and all mainstream operating systems. The OSCP examination consists of a virtual network containing varying configurations and operating system. The successful examinee will demonstrate their ability to research the network (information gathering), identify any vulnerabilities and execute tools, including modifying exploit code, all with the goal to compromise the systems and gain administrative access. The candidate is expected to submit a comprehensive penetration test report, containing in-depth notes and screen shots detailing their findings. Points are awarded for each compromised host, based on their difficulty and level of access obtained. An OSCP, by definition, is able to identify existing vulnerabilities and execute organized attacks in a controlled and focused manner, write simple bash or python scripts and modify existing exploit code to their advantage, perform network pivoting and data exfiltration, and compromise poorly written PHP web applications. The twenty-four hour examination also demonstrates that OSCP's have a certain degree of persistence and determination. Perhaps more importantly, an OSCP has demonstrated their ability to think "outside the box" and "laterally.".The intent of an Information Security certification is to provide confirmation that a specific individual has specific characteristics related to the field. The concept is great, you get a certification and use that as proof to a potential employer that you actually know your stuff. As this is a complex field, this is wonderful for an employer as it provides some level of assurance that the person you are hiring to do the work actually is competent.The problem is, a number of certifications on the market just don't provide that level of assurance. Like many IT certifications of the late 90s, a multiple choice test approach where you get the majority of the questions correct is enough to win you the certification. This leads to memorization quests on the part of test takers, where they focus more on what the right answer is and not so much on what the right answer means. The obvious result from this has been that many people just don't respect infosec certifications.On the other hand, with Infosec professionals at a shortage, the need for an effective measure of ones technical abilities has never been so critical and urgent – and this is where we believe we're making a difference. With our entry level certification (the OSCP) now identified by organizations as a leading technical certification – more and more are starting to use the OSCP as an industry standard.

Interestingly, it's not only the private industry that has responded to the OSCP certification – we're seeing more and more government entities incorporate Offsec in their information security training programs. The latest example for this is the UK Government Ministry of Defense – which has placed the OSCP on the shortlist of desirable qualifications for potential job candidates.The Kali Linux penetration testing platform contains a vast array of tools and utilities, from information gathering to final reporting, that enable security and IT professionals to assess the security of their systems.Google Hacking Databas : Originally created by Johnny Long of Hackers for Charity, The Google Hacking Database (GHDB) is an authoritative source for querying the ever-widening reach of the Google search engine. In the GHDB, you will find search terms for files containing usernames, vulnerable servers, and even files containing passwords. When The Google Hacking Database was integrated in The Exploit Database, the various googledorks contained in the thousands of exploit entries were entered into the GHDB. The direct mapping allows penetration testers to more rapidly determine if a particular web application has a publicly available exploit.

Bibliography: https://www.offensive-security.com and Official Kali Linux Documentation website and https://www.kali.org We believe the fastest way to get to know Kali Linux is to follow the documentation site and explore the new features available and http://tools.kali.org/tools-listing and https://www.backbox.org/blog/backbox-linux-44-released . getfedora.org. and https://backbox.org/portal/blog/backbox-linux-5-released

ADVERTORIALS AND CONSULTANCY HELP LINE

You may have problems with Government Departments PWD, BDA, BMRDA, KIADB, TOWN PLANNING DEPARTMENTS AND Development Authorities BBMP, Taluka office, D.C. Office, Corporation, K.S.R.T.C., Commercial Tax Offices, K.E.B., Pension problems, Acquisitions of Land Problems , Khata, Bifurcation, Tax Revision. Banks Problems etc, which may be have been pending for months, and years in Government files etc.

Everybody is facing Problems, Problems?

Kindly write to us, we analyze and convince our selves and if appropriate then we will take your problems, to concerned authorities, ministries, i.e., through our news paper property politics and try to help you. We also provide consultancy and Liaison service on case to case bases as per agreed terms and fees. Write your problems with Xerox copies,

M.S.Yatnatti , Consultant Mobile: 9945116476 E-Mail: msyatnatti@yahoo.com propertypolitics@gmail.com

==

Online Portal Edited Printed Published and Owned By M.S YATNATTI No.107 , Ground Floor "Royal Residency" Apartment Complex "Enkay Farms Valagerahalli, Dubasiplaya Kengeri Bangalore – 560 059
Editor –In –Chief M.S YATNATTI E-mail :sunnytimes.in@gmail.com Phone : 9945116476

Unsolicited material may not be returned. The opinion of writers are their own ,not our .We are not responsible for incorrect advertisement listings and .We do all we can to ensure correctness ,but readers are advised to recheck with concerned establishment before entering into binding contract .No part of this publication should reproduced without our written permission. Legal jurisdiction restricted to Bangalore only