Ethical Hacking Prof. Indranil Sengupta Department of Computer Science and Engineering Indian Institute of Technology, Kharagpur

Lecture - 16 Demonstration Part I

Before going to start the demonstration we need to setup our lab. So, in today's session we will basically show how to setup your lab environment. So, in ethical hacking we basically exploit different kind of operating system like starting from the older operating system Windows, XP maybe, Windows 7, Windows 8, Windows 10 and some other Linux operating system are also used as a target wise. And basically preferably we use Kali Linux as the attacker machine; that means, the hackers machine.

So, it is very difficult to arrange so many systems to run all this operating system. So, that is why we use the virtualization to install all these operating system in a single machine. So, there are different tools are available for virtual platform like VMware workstation, VMware player or a VirtualBox. So, VirtualBox is basically free open source software. So, that is why we use VirtualBox to create our own lab environment. So, here is the VirtualBox software. You can also go to the official website of *virtualbox.org* and from there you can download the VirtualBox for different operating system like windows, OS X, Linux, etc.

(Refer Slide Time: 01:53)

- Despire Se	ent X a Duurlaak-Cale Wildaali X +	-
# 10y	pr/mere entralition.org/wite/Downtouts	* 4
	N	
	Winter ID an	
	VITUAIBOX	and.
1	Thradebox	op twee
-	Download VirtualBox	
	Here you will find links to Virtualities binaries and its source code.	
	UldustBay binaries	
60A	by commanding you appear to the three and composed on the impact on many constraints and on our constraints \$2.0 million effect and constraints for 32-bit houlds, as this has been determined in 6.0 Mexican burst and another of the hould be as the hould b	der 3830.
deca	P for a series for the same relations as proceedings, the constraints of points related and one related to a processing of the same related to a series of the same relation of the same related to a processing of the same related to a series of the same relation of the same related to a series of the same relation of the same related to a series of the same related to a series of the same relation of the same relation of the same related to a series of the same relation of the same rel	of these
6)(3	virtueliou s.v.e perioriti peckages	
	 Invisional Network Invisional Network 	
	Indux defectedence Indux defectedence	
	The binaries are rolesaed under the terms of the GPL version 2.	
	See the chargelog for what here charged.	
	You might want to compare the checksions to verify the integrity of downloaded packages. The SH4256 checksions should be favored as the HIDS algorithm must be treated as insecured	
	SH4236 dhedeaunn, MD6 dhedeaunn	
	Note: After upgrading Virtualities it is recommended to upgrade the guest additions as well.	
	VirtualBox 6.0.8 Oracle VM VirtualBox Extension Pack	
	IniAl supported platforms	
	Support for USB 2.0 and USB 3.0 devices, Virtualities RDP, dask encryption, White and PDE boot for Entral casks. See this chapter from the case Hawait for an introduction to this Extension Pack. The Extension Pack Entrale are refer Virtualities Personal View and Exeluation Loomie (VVE). Please install the same version extension pack as proc material research of Virtualities.	sased under the
	VirtualBox 6.0.8 Software Developer Kit (3DK)	
	mult platform	
	User Manual	
	The VirtualBox User Manual is included in the VirtualBox packages above. If, however, you would like to take a look at it without having to install the whole thing, you also access it here:	
	Index Manual (IffM, version)	
	You may also like to take a look at our frequently asked questions list.	
	VirtualBox older builds	
	- Was blocked in this earlies for other blocked and a first of a second and a star offer dear dear the offer featured to a first offer blocked to and first offer blocked to and first offer blocked to a first offer blocked	and Portonian Comm
w-928-1_		Show all

So, now I already downloaded it from *virtualbox.org*. Now, execute this and run. Next.

(Refer Slide Time: 02:21)



Next.

(Refer Slide Time: 02:25)



Create start menu entry and also want to create a shortcut on the desktop and also create a shortcut in the quick launch bar and register file associations. Next. Install. (Refer Slide Time: 02:43)



It basically takes some time to install Oracle VM VirtualBox 6.0.8.

(Refer Slide Time: 02:59)



Now, finish. So, Oracle VM VirtualBox is already installed into our system. Now, in the next tutorial, I will show how to install Kali Linux in this virtual platform. Now, in this session we will show how to install Kali Linux in VirtualBox. So, this is the VirtualBox platform. So, first go to the option new and put the name I am going to install Kali Linux version 2019.2 and this is the folder you can also change this folder and it is a Linux operating system and it is Debian 64. So, now, go to next.

(Refer Slide Time: 03:53)



Now, memory size you can also check these things and change it to any other memory size. Recommended memory size is 2 GB that is 2048 MB. Then go to next.

(Refer Slide Time: 04:17)



Then create a virtual hard disk now. Now, VDI, VirtualBox Disk Image.

(Refer Slide Time: 04:21)



(Refer Slide Time: 04:29)



Now, we dynamically allocate the storage on physical hard disk.

(Refer Slide Time: 04:35)



Go to next, and file location and size. This is the file location and this is the size. 8 GB is recommended you can also change it. So, I will change it to 20 GB. Now create.

(Refer Slide Time: 04:55)



So, it will create the VirtualBox.

(Refer Slide Time: 05:09)



Now, go to the settings, and we need to add the file of that particular operating system.

(Refer Slide Time: 05:17)

No. 2010 States States States	
And a second sec	
The second secon	
Constant of the second	
	Const Constant C
an and a second	Construction
California California andresa, andres	Sector V
A Control of the second second	Dearl Alex
C T C C C C C	Dedisorganos (g)
C C C C C C C C C C C C C C C C C C C	
E E E E E E F ST	
C C C C C C C C C	
0 1 8 0 8 8 0 9 8 0 0	🛄 🖗 🛛 👘 Đối NHĐ y

Go to storage and this is empty. Now, choose the virtual optical disk file.

(Refer Slide Time: 05:27)



Now, we choose the Kali Linux 2019.2 ISO file which is available in the website of Kali, that is *Kali.org* and go to the download Kali Linux and you can get the all the available version of Kali Linux.

(Refer Slide Time: 05:51)

KALI				Blog Downloads Training	Documentation	Community About Us	۹
Property and				Kali Linux Down	loads		
Downloa We generate fresh i links to download its Your can find untilfs concurrent connect	nd Kali Kat Linux mag at Linux in to to cat. untented o stans.	Linu e files e atest off weekly r	ux Im wry few mo cial refease eteases at t	ages otto, which we naite availatile for download. For a release history, theok our Kal Linux field manuformage kall orghal weekly. Cowhoads	This page provides the new page. Please note: are rate limited to 5		
Image Name	Develand	Sue	Version	942565m		NOW AVAILABLE ONLINE	
Kall Linus 64 dis	ATTR Tarant	1.35	ana	170heet0heet00a0he7mbest2ca0he7mh	100017+83% 19001214	Advanced Web Attacks and Exploitation (AWAE)	
Kali Linux 32-84	ALL COMPANY	1.16	3143	140425648346644717286364846364799886	388e734358ee4344282	You can now take Office's most popular in-person training as an	
Kali Lisar LIDE 64-bit	setter i formett	1.05	2019.3	uminestamentation/konnectudet	Settion; Hizableachac	ontine course.	
Rail Linux AUTE 44-00	MTM (Toront	5.0	209.2	Micatalite distributed in the Solid Science of Science	teche Self-Risk di Visad		
Kuli Linun Light annthf	HTTP: I Tarrant	Jan.	2010.2	WardWorkWebbaac%c%includedscs	68659676625780	Become a Certified Penetration Tester	
Kult Linux KDC 44-Bit	ettin i turent	1.90	2016.2	1744/68123(14)(73981126586(144))(44(268	(willow/helicit/el/	Errol in Peretration Testing with Kall Unius, the course	
Kali Linar (17 44.00	ieltär i förmet	1.05	2019.3	(4036636034046631436363696963636353	terjiku/Min/sjite/s	required to become an Offensive Security Certified Professional (DSCP) Learn More	
Kall Linux XPCE	ATTR Toront.	1.65	2019.2	Uninitiative and the second second	senatoriamentalite.	ALT CONTRACT	

I install Kali Linux 64 bit, so these one. And the version is 2019.2. This is the latest version.

Now, see I already downloaded it and select this ISO file of Kali Linux 2019.2, then open, now ok. Now, start the machine, and say it will start the installation.

(Refer Slide Time: 06:45)



Now, you need to control this using keyboard. Now, go to the install part.

(Refer Slide Time: 06:59)

If if Stant and large tables If if Stant and tables If if Stant an	here the Auto capture keyboard option turned on. The off cause the initial Notice is an	which coppose the instance over, there the VM which as activated and name it consumbles to other applications coming on your head matchese. Into the instance of a copposed, of instances into the VM and a disected in the VM.	85
1(1) Enter your institute We solicit the system will be used for at your the provide the their actions. This is a invertisal to institute based on the Largeage you subscript. Genome "states" is Out the system will be used in the Largeage you subscript. Genome "states" is Contray. Invertisal to institute based on the Largeage you subscript. Genome "states" is Contray. Invertisal you interest. Marking and Bernach Marking and Bern	What Pachine reports that the guest (i) exports measure pointer integrations. This reserv	ter più de net need to applice for move porte fo be alle for an Cen para part 50 - al move adores no perform inter de move parte is mer the instal factors's diploy and desty sector for part 50.27 the move is correctly appliced, 1 al te automaticity acque	tret 🚯
		Util Britti gave mattine i The stratest factories allowed is to save the provide state factories to below the stratest factories when the the people gave material. Choose "tates" is the stratest factories when the the people gave material. Choose "tates" is the stratest factories when the the people gave material. Choose "tates" is the stratest factories when the the people gave material. Choose "tates" is the stratest factories when the the people gave material. Choose "tates" is the stratest factories when the the people gave material. Choose "tates" is the stratest factories when the stratest the stratest factories when the stratest between the stratest factories when the	

Suppose, I select English and location United States and configure the keyboard as American English.

(Refer Slide Time: 07:13)

		-
where the Auto capture keylmost option turned on. This will cause the listual Machine to automatical	completes the leads and income the RM version is activated and note a consolidate to other applications covering any new heat matheme when the leads and a septement, ad larger tables ploying systems over the RM half of the directed to the RM.	85
e in tuel Hachren reports that the guind CS apports measure pointer integration. This recent that you	h na read to applice from an partie to be die to an En yau part 25 - dimans actives yn perfors sher the mone partie to me fre inhalthaben's dapie, ere diects wet to the part 25. If the mone is coverly opticed, if while automatic unapp	nt. (85)
	Lindig Mill Sind Enquerits : It Ant foliag etai-setan	
	2012/12/20	

You can also select your own choice.

(Refer Slide Time: 07:41)

have the Auto capture keyloard option turned on. This will cause the initial Pactime is a	torotaly appears the leduced every line the 4% ondex is attended and note it prevaible to the applications using on our heat hadrone when the leduced's optimal, all injections (including optimizers and the 10 feb) will be decided to the 4%.	85
What Machine reports that the guint CE exports mouse pointer integration. This report	The point of the finance partice for a detained on the part of a dimension and perform when the mean partice is not the intradictive of depins of the finance of the mean exceeder particles, it will be automatically	nastrel 🛞
	If 15 contains the instance is any part - device any end-set in management is a first indevice lapse in a structure in good, if it is support of this support. If and any title instance for this support If any title instance of this support If any title inst	sates. 5

Hostname, you can also change the hostname.

(Refer Slide Time: 07:49)

es De Auto capture keylouerd uptor turned or. The of cause the total Plaches to a	constantly coplane for section of which is all values of eace is an ended to other applications covery or pair feed matters when the industrial approxit, of insystems producy opensions for Art (all) of the directed is the VF.	•
tual Hachere reports that the guest OS apports mouse pointer integration . This recen	a their sou do not read to upply the mean parties to be dife to use to your part (S) - driving activer you perform when the nouse parties is one the initial Parties's depicy are directly sent to the gasel (S). If the mean is correctly applied, it will be address	tatioly proptiest. 🚷
	10 bit or user and extended	
	The one of the star descence of the control of the starter exception and the starter of the unquicities over with more increases can have descence more than a grant should be an choose a near passed that is not away to passe. It should not be a work found to distributes or an work that could be easily associated with you.	
	A good person of will contain a mixture of letters, numbers and punctuation and should be charged at regular intervals.	
	The root user should not have an empty passand. It you have this empty, the root account will be dysamined new requeres a notical user account will be given the power to become root using the "Name" commend.	
	Note that you will not be able to see the password as you type it.	
	Root pessendi	
	Construction Research and Const	
	vice Becks	
	2010/0001	
	and the second	
	(Tabl moves) closers princis (chiers activates buttons	
	DOM # C	the second se

I simply continue, and root password, then continue.

(Refer Slide Time: 08:01)

nanonandron genes the forgenes and anonany andron being were for any benefit agree of the sound of the sound anonanous for the	Riedwand is die M. 😽
1.1.1.5 Set is one is and assumed a 1- Fiscal other many out assumed has not verify that you have typed in correction- tion-white assumed to verify The set of the set of the set of the Set of the set of the se	rerly spirel, tol te atomisky orspirel. 🛞
Not wint: Open saletti Oher ettinde latter	

Then reenter and continue again.

(Refer Slide Time: 08:07)



(Refer Slide Time: 08:09)

over the Auto capture keyboard option turned on. This will cause the Wittal Pitchere to a	toration's constant the landscale area the life and noise is activated and noise it unavailable to other applications ravering on your heat mathemic when the landscale is approved, all larger takes (including nor	an ans Re All fab) will be directed to the VK. 😽
that Pactors reports that the punct CD supports essanse punctur integration . This reser	That you do not read to approve the reason portion to be able to use if in your guard (C) - advecues extensi you perform when the reason portion is new the initial Hadren's deploy are directly eart to the guard	n 21. 3' Die maar is converty captured, it wil be automatically orcuptured. 🛞
	I i i for an ison to see the set of the set	
	this works dynam adaptic dofers activates bottom	

Now, configure the clock. I choose the default one.

(Refer Slide Time: 08:23)



Now, partition disk. I choose the guided use entire disk. All file in one partition.

(Refer Slide Time: 08:31)

It is a the set of the spectrum of the provided set of the set of the standard is spectral to set out a provide standard is a size duration of the spectral to set out a provide standard is a size duration of the spectral to set out a provide standard is a size duration of the spectral to set out a spectr	
To instruction region to the grant (2 march associated barry barrier), and the second	89
() Vertiling case.) Sedented for partitioning: Sedim 001 (sol) - with work imposition 71.5 GB The disk can be partitioned using one of terminal different schemes. If you are insure, choose the first day. Partitioning schemes	natudo unaștorei. 💌 🖓
Hernitz Avon prillin Hernitz Avon prillin (# 160)	
	1.0.10

It is recommended for new users.

(Refer Slide Time: 08:41)



Now, finish partitioning and write changes to disk. Yes. Now, put yes.

(Refer Slide Time: 08:45)

Einit deve westerte part it was neede alle blands to de alle de transporte to de la alte transporte de la deve de la deve de la alte transporte de la deve de la alte de la deve de la alte de la deve de la deve de la deve deve deve deve de la deve de la deve deve deve deve deve deve deve dev
have here her her here and a speen despective. The even here as is and an and a partition of a speech and is and a speech and is a speech and a
(10) Analysis data If you continue, the charges jushed bills will be written to the datas. Tokawain, you will be able to not offer the datas models are of charges Statis 100-AP (100) The datas of partition of any single to be framework Statis 100-AP (100) The charges to State? Write the charges to State? (Note: Market datas in the data in the

Now, it will take some time to install the system.

(Refer Slide Time: 09:01)

the back over the first gas 10 legens management back by the for any part of the part of t	The Aulta capture keyboard option turned on. The will cause the initial Machine to automat	Sch. capture Te lactural every time Te W under a activated of national standards to other applications coving on nur had natione, when Terlinducard's spaces, of leavisides lockading covins own lie 40-201-of te descted to Ter M.	
(1) Configer term particularly and the second of the second term part to de the term part of the second of the			
It is confured to annexe because) Intervent above on law and a subjectment the ontrary test is included on the Gh-soc. State way also been reversion on confurer builded. Use a relation subject of confurer builded. do beach do beach doe word: doech subjects: down builded butter	e Machine reports that the guard CE apports measure position indegration. This resard that a	pu do not need to capture for mean portier to be dire to your gave CS - of means actions you perform when the means portier to nee the initial Reddev) deploy and to the part CIS. If the means to unreally captured, if while automatically programs	8
		Intervented over the sector and th	

A configure the package manager; use a network mirror, I select no. Now, it is installing grub boot loader. It is very important.

(Refer Slide Time: 09:15)

the first first first content includes of other transform. The off cases for initial literature is a meaning	nation to industriant test for Washing and with a close to construct one on the testing of the factorial distances in the UNAL after description of the Armonic Sciences and a UNAL after description of the Armonic Science	
n des la vers referes sublime des roues or the second second second		•
e tribal Radee reports that the parel dis apports ensure puinter integration . The many that y	to not need to approve the manufacture to be able to use it to your guest CD - with maximum parties when the maximum parties is over the initial Machine's diploy are deadly write to the part CD. If the maximum parties a converty approved, it will be automatically unapproved to approve the maximum parties and the part CD. If the maximum parties are the initial Machine's diploy are deadly write the part CD. If the maximum parties are the part CD. If the maximum parties are the initial Machine's diploy are deadly write the part CD. If the maximum parties are the part CD. If the maximum parties are the part CD. If the maximum parties are the initial Machine's diploy are deadly write the part CD. If the maximum parties are the part CD. If the parties are the pa	ptret 80
	The numerical state of the state is a state of the state	
	D A M & A D R & A D R & A	10000

So, install the grub boot loader on a hard disk, always yes.

(Refer Slide Time: 09:19)



Now, for the first time not manually use /dv/hda.

(Refer Slide Time: 09:37)

La 2012 Revery Data Minuta	1.10	-
To here the Auto-capture Replaced prior services. The of source for installation is accountly capture to instance on the IN online a accountly order a sound of source and and rate regulations sorring or nor host numbers offer the instance folding com	en ones like All ¹ dd(vill be directed to the VM.	8%
The installable repetited to get (3) agent means participation. The react the sub-in it is apprend to apprend to a date to see part (3) - diman states sing of the neuroparties over the install-balance's date, we doub, we doub, we have been apprend to be apprend to a diman states and the install-balance date (3) and the part	26. If the mover's currently capitured, it will be automatically uncapitured.	852
(Acadega (ke politika)an) Bar Ranging quarte ingtrant	200# <i>2</i> 78#081	Apple Col
0 2 6 0 x 6 8 x k 0 11 x 8	#01-Net 10	

Now, it is finishing the installation. Finish the installation, continue.

(Refer Slide Time: 09:49)



Now, Kali Linux is already installed and it opening now.

(Refer Slide Time: 09:57)



So, now use the username root and password which we which we provide at the time of installation. Yes, now there is the Kali Linux. We successfully installed Kali Linux into the virtual platform.

Now, always remember that before going to install any operating system into virtual platform, always enable the virtualization option in your BIOS setup. Now, this way you

can install other operating system such as windows XP, windows 7, 8, 10, and other Linux operating system also and this way you can set up your own lab environment.

Thank you.