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

Lecture - 20 How to Use Nessus

(Refer Slide Time: 00:15)



Now, today's session we will discuss about the vulnerability assessment using the tool Nessus. Here is my tool Nessus, first we need to login into the tool Nessus. So, use the login credential which you use at the time of installation.

(Refer Slide Time: 00:49)



So, here is the interface to scan a system, first we need to go to the new scan. So, there are several option are available: advance dynamic scan, advance scan, audit cloud infrastructure, badlock detection, basic network scan; lots of option are there. So, for the time being we are using advance scan.

(Refer Slide Time: 01:23)

nessus	Scans Setting:					explote	8
My Scans	New Scan « Back to Scan To	/ Advance	ed Scan				
All Scans	Settings	Credentials	Plugins				
Trash	ALC:						
excorea:	* General		Name	NPTEL			
Policies	Schedule						
Scanners	Notificatio	205	Description	Demo			
	DISCOVERY	>					
	ASSESSMENT		Folder	My Scans			
Community	REPORT						
y Research	ADVANCED		targets	192.168.0.104, 192.168.0.106			
			Upload Targets	Add File			

So, in these field first we need to put the name of the scan, suppose the name is NPTEL and description is a Demo, folder My Scans and target, so, in this case my target is sorry

target IP address is 192.168.0.104 and 192.168.0.106. So, this way we can use multiple IP address for scanning separated by comma.

🗘 Most Visited 🐞 Corner	oar a usar Firefox 🧧 OpenCV Python TU	0	
nessus	Scana Settings	♦ equit	. 8
My Scans	New Scan / Advance « Back to Scan Templates	ed Scan	
All Scans	Settings Credentials	Plugers	
Trash	RASIC > DISCOVERY ~ * Host Discovery	Remote Host Ping Ping the remote host	
 € Scanners Thurse (D) Community (Q) Research 	Port Scanning Senge Discourty Assessment a Advanced	General Settings Vet the local Nessel Not Training specifies where the local Nessel Not Annual Servered where it link within the target renge specifies for the scen. Vet for for testevic discovery P is for testevic discovery	
		Ping Methods V 100 V 100 Detropological publics	

(Refer Slide Time: 02:33)

Now, where is all the option for discovery? Discovery option is a ping method, ARP and TCP and it also use the ICMP and maximum number of tries is 2; that means, it try twice for a particular request. Then port scanning part is also there to enumerate the local port to use SSH and WMI, SNMP and only run network port scanner, if local port enumeration failed.

(Refer Slide Time: 03:35)

a mail failed	and the sheet of and the	
nessus	Scans Settings	septoter (
My Scans	New Scan / Advance « Back to Scan Templates	ed Scan
All Scans	Settings Credentials	Plugins
Trash	MSC	
nooran Roleine	DISCOVERY ~	General Settings
Plugin Rules	Host Discovery	 Proce as ports to two services Attempts to may each open port with the service that is naming on that port. Note that is some use cases, this might dougd some services and cause
g Scanners	Port Scanning	
	* Service Discovery	Search for SSL/TLS services
Community	REPORT	
Research	ADVANCED	Search for SSL/TLS on Known SSL/TLS ports
		identify certificates expiring within x days 60
		Enumerate all SSU/TLS ciphers Who soluted, lineau sports the lat of ciphers advertised by SSU/TLS services, and enumerates them by attempting to installable connections using all penalite ciphers.

So, you can choose your own option, then service discovery enumerate all SSL or TLS cipher.

(Refer Slide Time: 03:47)

Descur	and a spectrum	James Con	lo de la companya de	1-040/2-3	-			
Inessus	Scans Settings			• «	sloter 4			
My Scans	New Scan / A « Back to Scan Temple	dvance ##5	ed Scan					
All Scans Trash	Settings Cr	Artivia Artivia Artivia Artivia Artivia Artivia	Plugins					
	BASIC		Accuracy					
Policies	DISCOVERY		Override normal act	turacy				
Plugin Rules	ASSESSMENT	×	 build extended 	Tala alama				
Plugin Rules	* General		 more pointing 	Server analytics				
	Brute Force		Show potential	laise alarms				
	Web applicatio	Web Articutions Perform thorough tests imay disrupt your network or impact scan speed)						
Scanners Scanners Community Research	Windows							
Research	Malware							
	REPORT		Antivirus					
	ADVANCED		Antivirus definition grace	period (in days): 0 *				
			SMTP					
			Third party domain	example.com				

Now, assessment part is there and in assessment part Brute force assessment, web application assessment, then Windows assessment and malware assessment. All options are there, you can choose your own option; for the time being I am of the scan for malware.

(Refer Slide Time: 04:13)

🗘 Most Visited 🐞 Com	encar a usar Firefox 📵 OpenCi	Python TUT	h.,	
nessus Internet	Scans Settings New Scan / A	Advance	d Scan	🛦 esploter 🤇
My Sons My Sons Ma Scans Trach Trach Policies Policies Scanners Tructs Community © Research	Settings C BASC DISCOVERY ADSISSMENT HEYORT ADVANCED	Credentials	Processing Override normal verbooly Is have instead dats space. Report as lattle information as possible Report as much information as possible Show missing patches that have been superseded Index results from plugins initiated as a dependency Orsput	
	ĸ		Designate hosts by their DHG name Display hosts that respond to ping Display hosts that respond to ping	

Then report we can also use this option to generate the report.

(Refer Slide Time: 04:19)

Decision Same Settings Control Wy Jams New Scan / Advanced Scan Wy Jams *Lack to Scan herpstres Wy Jams Settings Decision Settings Settings Settings Decision Settings Settings	Most Visited 🐞 Comence	e a usar Firefox 🛛 Op	enCV Python TUT	he state of the st	
New Scan / Advanced Scan My Scans Setting Costnink M Scans Setting Costnink Notices Setting Costnink Policies Setting Costnink Policies Setting Costnink Policies Setting General Settings States Setting Setting States Setting Settings States Setting Settings States Setting Settings States Setting Settings States Profermance Options Setting State doeds per host 3 Max simultaneous hosts per scan 3	nessus	Scana Setting	p		A exploter
Al Scars Setting Codential Pages State MAX BAXX BAXX BAXX Policies BAXX BAXX BAXXX BAXXXX Policies BAXXXXX BAXXXXXX BAXXXXXXX BAXXXXXXXXX Policies BAXXXXXXXXXXXXXXXXXX Baserial BaxXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	My Scans	New Scan + Back to Scan	/ Advance Templates	d Scan	
Note: Note: Central Settings Polois: Biccontral Settings Index set duels: Polois: AXXXXMIN Index set duels: Polois: AXXXXMIN Index set duels: Sceners: AXXXMIN Index set duels: Intervention: Sceners: AXXXMIN Intervention: Intervention: Sceners: AXXXMIN: Intervention: Sceners: Intervention: Sceners: Sceners: Interventin: Scen	All Scans	Settings	Credentials	Plugies	
Aremany Aremany Aremany Aremany Aremany Performance Option Subor doon the scan when network congection is detected Metwork timeout (n seconds) S Mas simultaneous horts per scan S	ISDURCES Policies Plugin Rules <u> è</u> Scanners Inness	BASIC DISCOVERY ASSESSMENT REPORT ADVINICED		General Settings ✓ Enable safe checks Sop scanning hosts that become unresponsive during the scan Scan ₱ addresses in a random jjother	
	2 Community 1 Research			Performance Options Store down the scan when network congestion is detected Network timeout (in seconds) 3 Max simultaneous sheds per host 5 Max simultaneous hots per scan 5	

And in advance part there are some options are also there, network timeout; here network timeout is 5 and a maximum simultaneous check per host that is also 5. Maximum simultaneous host per scan that is also 5, you can also change your own option.

	en a san riveer 🖕 oper	a channe constru		_	20.2011	
nessus	Scans Settings				Filter Search Plages Family	🔍 🔺 exploter
My Scans	New Scan / « Back to Scan Ter	Advanced Scan				Disable All Enable All
All Scans Trash	Settings	Credentials Plugins				Show Enabled Show A
	status	PLUGIN FAMILY -	TOTAL	a status	PLUGIN NAME	PLUGIN ID
Policies	DURKE	ADI Local Security Checks	11366		No plugin family selected.	
Plugin Rules	INABLID	Amazon Linux Local Security Checks	1366	1		
Scanners	DMMLID	Backdoors	126			
	INALIO	CentOS Local Security Checks	2819			
Community	DMBJD	CGI abuses	4117			
Research	DABID	CGI abuses : XSS	672			
	DMR.ED	cisco	1042			
	DURLED	Databases	626			
	0048.00	Debian Local Security Checks	6306			
		Pudwik Linix Ascessed	120	¥		- M

(Refer Slide Time: 04:41)

Now, where presidential is there and plug in part are also there. So, you already install plug in part which is show in the tool installation part. So, all the plug in are here which can help us to find out the different vulnerability right; save this scan.

(Refer Slide Time: 05:03)

Nessus Essentials / Folder	s/M X +			- 0 ×
€) → ୯ @	(i) 🔒 https://localhost/8834/#/sci	ans/folders	🖸 🕹 🛨	IN (D @ Ø E
O Most Visited 👲 Corner	ncar a usar Firefox 🧧 OpenCY Python TUTO			
	Scans Settings			🔺 exploter 🕹
	My Scans		Import New Fold	er O New Scan
🖬 My Scans 🛛 👌				
Al Scans	Search Scare, Q. 15	can		
Trash	Name	Schedule	Last Modified -	Pause
O Policies	NPTEL	On Demand	O Today at 2:25 AM	5 *
Plugin Rules				
🖞 Scanners				
Community				
Research				
0 # 9 8	🖿 🕒 🚯 Nessus Essentials / Fo 🚺 VMmare Wi	orlation	£ ^ 4 ***	di ENG 225 AM 🔛

Now, I am starting the scan by clicking on the button launch, scan already started and it will take some time to complete the whole scan. And, once we got the scan result and by analyzing that result we can only find out the vulnerabilities and using that vulnerabilities further we can try to penetrate inside the victim machine. So, let us wait for some time to get the result of vulnerability scanning, now see Nessus complete the scan. So, let check the result.

(Refer Slide Time: 06:05)

norrue								
Eventuit	Scana Settings					1	exploi	er.
My Scans	NPTEL « Back to My Scans		Configure Aud	śt Trail Laur	ch *	Report *	Export	•
All Scans Trash	Hosts 2 Vulnerabilities 75	Remediations 2 History 1						
Doncas.	Ref .	Q, 2 Hotts						
Policies	Hest	Vulnerabilities +		Scan D	rtails			
Plugin Rules Scanners	92,165,0,104		129	X Policy: Status:	Advan Comp	ced Scan leted		
	192.168.0.106	14		× Scanner	Local	Scanner		
Community				Endt	Augus	t 17 at 2:34 Af	vi Vi	
Research				Elapsed	9 min	.tes		
				W. dave	bills/			
				v uniters	Contract	-		
						 Libca High 		
						 Mediu Low 	m	
					~	• info		

So, you basically scan for 2 systems, one is with the IP address 192.168.0.104.

(Refer Slide Time: 06:17)

)→ ୯ ଜ	@ 🔒 h	https://localhost/8834/#/scans/reports/5/h	osts/2/w/inerabilities				9 G		¥ #		9
	Scans Settings	actrymunititit.								≜ eq:	loter
CLEARS	NPTEL / 19 « Back to Hosts	2.168.0.104		Configure	Au	dit Trail	Laurch	•	Report •	Expor	t *
All Scans Trash	Vulnerabiliti	ies 70									
routon Policies	filter * So	Name -	erabilites 2. Multiple Issuel	Count +		0					
Plugin Rules Scanners	C Ontox	1 SSL (Multiple issues)	Gain a shell remotely	3	0	1	Host:	192. Ils	168.0.104		•
	C RITCH	Bind Shell Backdoor Detection	Backdoors	5			P:	192.168.0	104		
Community	О опос	NFS Exported Share Information Discl	RPC	1 0			MAC: OS:	945330:73:95:C3			
Research	C Other	rexecd Service Detection	Service detection	î.		×	Start	(hardy) August 12	1 at 224 AN	4	
	CI CITCL	Unix Operating System Unsupported	General	τ.		1	End: Elapsed:	August 1 9 minutes	# 234 AN	ř.	
	Comos,	UnrealRCd Backdoor Detection	Backdoors	1			18	Download	4		
	Ослок	VNC Server 'password' Password	Gain a shell remotely	1			Vulnerabi	ities			
	13 MOLD	1 SSL (Multiple issues)	Service detection	3			6		Citic High	al .	

And, it has several vulnerabilities, total 70 vulnerability is there and out of this 70 vulnerability 9 critical vulnerability is there, 5 high vulnerability is there, 23 medium vulnerability and 8 low vulnerability is there and 129 that all are the information. And, here is the details of all the vulnerability SSL multiple issues and a bind shell backdoor detection.

(Refer Slide Time: 06:53)



A shell is listening on the remote port without any authentication being required, an attacker may use it by connecting to the remote port and sending command directly. So,

using this vulnerability one can attack to the victim machine and some other vulnerabilities also there. Let us check the other IP address 192.168.0.106, but I have total 21 vulnerability and 1 critical vulnerability is there and 2 medium vulnerability is there and 36 information is there.

(Refer Slide Time: 07:41)



And, see MS17 - 010 security update for Microsoft Windows SMB server and the remote Windows host is affected by the vulnerability with the CVE number 2017 – 0143, *CVE* 2017 – 0144, *CVE* 2017 – 0145 and also *CVE* 2017 – 0146 and *CVE* 2017 – 0148. An information disclosure vulnerabilities also exist in this machine and some other vulnerability is also there.

(Refer Slide Time: 08:27)



Like in medium vulnerability $MS \, 17 - 047$ is also there, remote Windows host is affected by an elevation of privilege vulnerability in the SAM and local security authority. So, all the vulnerability and the possible solution are listed here. So, this way we can find out all the vulnerability using the tool Nessus and further we use all these vulnerability to penetrate inside the victim machine. So, this phase is basically call vulnerability assessment phase and in vulnerability assessment phase, we find out all the possible way by which a attacker can penetrate inside the victim machine.

But in the next phase; that means, in penetration testing phase a attacker can try with all these vulnerability to check which vulnerability is working and which one is not; so, that is called penetration testing. So, in the next week, in next tutorial I will show you how to use all the thing, all the information gathering part which we covered in this week and using all that information how can one penetrate inside the victim machine.

Thank you.