LAB04-02 ARPspoofing Driftnet

Class: student ID: Name:

Simulation scenario

	Host	Target
VM type	Virtual box, VMware	
OS	Ubuntu, Centos, kali	
IP	Test-bed IP	
Attacking type	ARP Spoofing	
Attacking program	Ettercap, Driftnet	
Analyzing tool	WireShark.exe	
Process	• set test system environment • install Ettercap • install WireShark.exe • install Driftnet • IP forwarding • run driftnet • saving intercepted images • install the Dsniff packet • analze target system using WireShark.exe	

Exercise following ArpSpoofing combination processes and explain each spep

① install Ettercap

② install Wireshark :

③ install Driftnet using apt run:

④ enable IP forwarding by running the following command:

⑤ while Ettercap scans the network run driftnet using the -i flag to specify the interface as in the following example:

⑥ by default, intercepted images are saved inside the /tmp directory with the prefix “drifnet”.

⑦ by adding the flag -d you can specify a destination directory, in the following example I save the results inside the directory called linuxhinttmp:

⑧ install the Dsniff packet through apt by running:

⑨ enable IP forwarding by executing:

⑩ run ArpSpoof defining the interface using the flag -i, define the gateway and target f ollowed by the -t flag:

⑪ launch Driftnet by running: