

	Registration Number	Surname	Forename	% Contribution
Student 1	001141646	Iz	Ekrem	25
Student 2	001131628	Chavush	Chisel	25
Student 3	001174434	Turker	Selin	25
Student 4	001141387	Hasan	Zahid	25

Question 01

High Value Assets

The high value assets of the simulation and the target of the attacker. Click on items in the list to get more details.

Filter Models


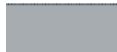











ID	NAME	ATTACK STEP	CONSEQUENCE	PROBABILITY	TTC GRAPH	TTC 50%	RISK	CRITICAL PATH
1	 Clientzone	Compromise	4/10	100%		0 days	High	
2	 Serverzone	Compromise	7/10	75%		22 days	Critical	
3	 CS-SZ	Compromise	7/10	0%	Not reached	N/A	N/A	No path
5	 ServerSystem	Compromise	7/10	67%		43 days	High	
55	 Windows 10 ...	Compromise	5/10	90%		14 days	High	

Figure 1

As can be seen in the report (see Figure 1 page on 1), the network is significantly vulnerable because there is no network security as well as host security setup.

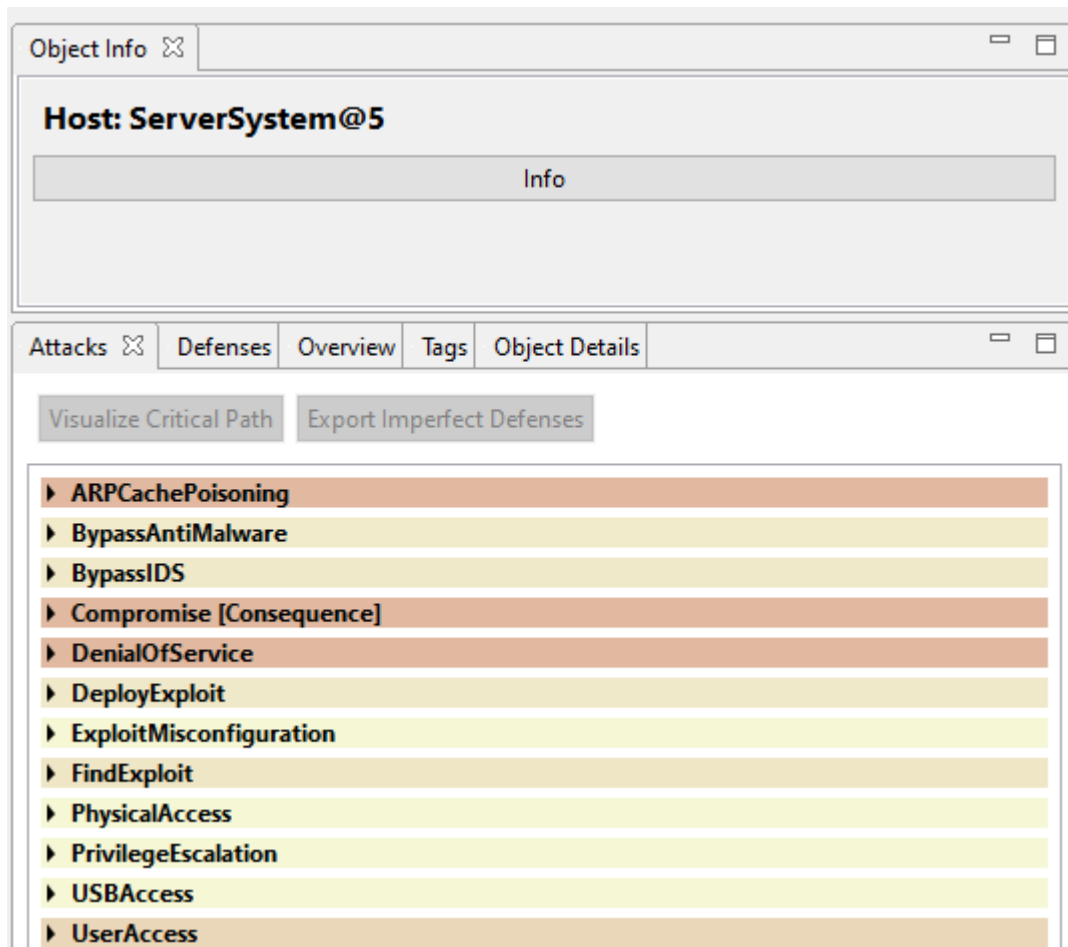


Figure 2

Since most important host is the server host, we prioritize securing the host against the attacker. As it can be seen in the attacks table of server host that it is more vulnerable to the ARP Cache Poisoning, Denial of Service and we can also see that the host is compromised. Therefore, we will start setting some defences on this machine. Firstly, staticARPTables setting has been set up in order to not ask for mac addresses every time the host been connected within the LAN. Then setting antimalware will help host to protect against the malwares, patching up to date and properly configuring the system will fix the previous bugs and security vulnerabilities and setting up host firewall will allow hosts to control which packets will be allowed to get in.

High Value Assets

The high value assets of the simulation and the target of the attacker. Click on items in the list to get more details.

Filter Models














ID	NAME	ATTACK STEP	CONSEQUENCE	PROBABILITY	TTC GRAPH	TTC 50%	RISK	CRITICAL PATH
1	 Clientzone	Compromise	4/10	100%		0 days	High	
2	 Serverzone	Compromise	7/10	73%		27 days	Critical	
3	 CS-SZ	Compromise	7/10	0%	Not reached	N/A	N/A	No path
5	 ServerSystem	Compromise	7/10	52%		91 days	High	
55	 Windows 10 worksts... Compromise	Compromise	5/10	89%		13 days	High	

Figure 3

As it can be seen clearly in the screenshot (Figure 3 on page 3) that after setting some defences made the vulnerability percentage drop by around 15%.

Question 02

Attacker can access to the server host by using the SSH Protocol. To make his job more complicated and make the host more secure, we need to patch the SSHD server of our server host and configure it properly. Patching SSHD server will allow us to fix potential bugs and more secure.

High Value Assets

The high value assets of the simulation and the target of the attacker. Click on items in the list to get more details.

Filter Models














ID	NAME	ATTACK STEP	CONSEQUENCE	PROBABILITY	TTC GRAPH	TTC 50%	RISK	CRITICAL PATH
1	 Clientzone	Compromise	4/10	100%		0 days	High	
2	 Serverzone	Compromise	7/10	68%		29 days	High	
3	 CS-SZ	Compromise	7/10	0%	Not reached	N/A	N/A	No path
5	 ServerSystem	Compromise	7/10	34%		Infinity days	Medium	
55	 Windows 10 worksts... Compromise	Compromise	5/10	86%		13 days	High	

Figure 4

As it has been shown in the report (Figure 4 on page 3) that we have achieved to decrease the vulnerability percentage even more! This time it has been dropped by 18% which is quite good improvement with such little patching.

High Value Assets

The high value assets of the simulation and the target of the attacker. Click on items in the list to get more details.




















Filter Models								
ID	NAME	ATTACK STEP	CONSEQUENCE	PROBABILITY	TTC GRAPH	TTC 50%	RISK	CRITICAL PATH
1	 Clientzone	Compromise	4/10	100%		0 days	High	
2	 Serverzone	Compromise	7/10	66%		33 days	High	
3	 CS-SZ	Compromise	7/10	0%	Not reached	N/A	N/A	No path
5	 ServerSystem	BypassAntiMalware	7/10	2%		Infinity days	Medium	
5	 ServerSystem	Compromise	7/10	35%		Infinity days	Medium	
5	 ServerSystem	DenialOfService	7/10	35%		Infinity days	Medium	
55	 Windows 10 worksts... Compromise		5/10	87%		13 days	High	

Figure 5

We now have increased the attacks by adding bypassing anti malware that can be happened on server system; this can be seen in the screenshot (Figure 5 on page 4).

As it can be seen in the report that the probability percentage of bypassing the anti-malware is only 2% since we had our anti-malware set up in the server host. This prevents very well against this attack type.

In our simulation, attacker has tried to access and get credentials of our server. There were plenty of attack types that attacker could use. However, the most dangerous attacks were compromise server host by using SSHD (since it wasn't patched up), ARP Cache Poisoning and using the vulnerabilities of old versions of the systems was helping attackers to hack the system easier.

For the defence side, by patching up systems and our SSHD helped the server host a lot in order to secure it. Adding anti-malware and setting firewall to control dataflow make attacker work a lot harder to hack the system.

To sum everything up, we could have added plenty of settings to defence our network and server host. However, main point of doing some small changes is to show that we can defence our system decently without losing lots of times and expending huge amounts of money. In our case we didn't even activate firewall for our router since it would be costly. But we still managed to decrease the probability of getting hacked significantly. We analysed the most crucial paths that attacker could chose to attack our machines and we focused to eliminate them first to make the most important hosts safe.