DALHOUSIE UNIVERSITY

Network Security (CSCI-6708)

Assignment - 2

Shivam Gupta
B00810723

Scenario	Intrusion(s)	Security Goal(s) violated	Justification
Bob crashes Alice's computer system by sending a flood of packets	Interruption	Availability	This is a classic case of a DoS attack and hence falls under the category of interruption. Alice's computer is unavailable for her use and hence the security goal violated is Availability.
Alice copies Bob's assignment by eavesdropping on traffic from his machine.	Interception	Confidentiality	This is a case of sniffing, where the attacker is eavesdropping on the traffic of victim's machine. As the attacker is eavesdropping, confidentiality has been compromised.
Bob copies Alice's assignment by accessing her hard drive.	Interception	Access Control	As there is no modification, this is the case of Interception, where the attacker is just trying to get information. It violates the access control security goal as bob accessed Alice's computer without her knowledge.
Alice changes the amount on Bob's cheque when it is being transmitted.	Modification	Integrity	This is a case of man in the middle, where Alice changes the amount between transaction. Integrity security goal has been violated as the amount is changed.
Bob sends a property deed to the Registrar in the name of Alice by forging Alice's signature.	Modification	Authentication	This is also a case of modification, where attacker is trying to modify the victim's signature. Authentication security goal is violated as the sender's validation is not done.
Alice spoof's Bob's IP address to gain access to his office server.	Modification	Authentication	This is a case of man in the middle, where attacker is spoofing IP address between victim and server. Authentication is violated as Sender's validation is not done.
Bob installs malware on Alice's computer.	Fabrication	Access control	This is a case of fabrication as a malware is injected into the victim's machine. Access control is violated as bob could access Alice's computer without Alice's knowledge.
Bob obtains Alice's credit card information online and has the credit card company replace it with another card bearing a different account number.	Invasion	Availability	This is a case of session hijacking, where attacker is taking complete control over victim's credit card and changes the information, which result in DoS for the victim. Availability is violated as Alice can't use her credit card.
Alice has a fake third party authenticate her server as legitimate.	Modification	Certification Access control Authentication	This case is of modification as Alice is modifying and accessing the server as legitimate user. Certification and access control and authentication are violated, as Alice provides a fake authentication with fake certification and could access the server.

Aircrack-ng:

Aircrack-ng is a network security tool used for wireless network security and to crack WEP and WPA. It uses the best cracking algorithm to recover wireless keys after gathering encrypted packets. Basically, it uses Linux as primary operating system but can also work in Windows, Mac OS X, FreeBSD, OpenBSD, NetBSD and Solaris. It was started in end of February 2006.

Aircrack-ng's Features:

- It has a better documentation compared to other tools in the marker, like forums, GitHub, IRC and Free node.
- It can support more cards and drivers.
- It can support Linux, Windows, Mac OS X, FreeBSD, OpenBSD, NetBSD and Solaris.
- It has various kinds of attacks like PTW attack, WEP dictionary attack, fragmentation attack, WPA1/2 cracking and has a WPA migration mode.
- It has a faster speed for cracking networks.
- It has variety of tools like airtun-ng, packetforge-ng (improved arpforge), wesside-ng, easside-ng, airserv-ng, airolib-ng, airdriver-ng, airbase-ng, tkiptun-ng and airdecloak-ng.

What it provides:

It focuses on four Wi-Fi security areas: Monitoring, Attacking, Testing, Cracking.

- Monitoring: It catches encrypted packed and export data to text, which can be used by other network security application.
- Attacking: It can launch attacks in various ways like Replay attacks, deauthentication, fake access points or via packet injection.
- Testing: It can test for Wi-Fi cards and the driver capabilities of the wireless network.
- Cracking: It can crack WEP and WPS PSK (WPA 1 and WPA 2).

How it works:

- First method is PTW method, where RC4 cipher keystream is used to crack WEP
- Second method is FMS/Korek method, where multiple techniques are combined to crack the WEP key, like Statistical techniques, Koreks attack or brute force method. Every byte is handled separately, and key is guessed by IV (initialization vector) or brute force is used where full key is guessed by dictionary attack or other brute force attacks like fudge factor.
- Fudge factor comes in a brute force attack and determines till how long brute force should be done. It's a trade off between length of time and likelihood of finding.
- To crack WPA- pre shared keys, dictionary attack is used, a four-way handshake is done, and a word list is matched with the result, result in identifying the pre shared key.
- Lastly, tools like john the ripper are used to generate guessed password and are fed into the air crack-ng to crack the network.

How it is useful to a network security specialist:

- Aircrack-ng is useful for Network security specialist as with this tool, user can check the security of the wireless network and see how long it takes to penetrate the security.
- Cracking WEP is easy with this tool and WEP are rarely used, so let's look at cracking own WPA password, which could help the security specialist to improve the wireless security.
- Step-1: disconnected from all network and Configure the wireless card in Linux by using the command: airmon-ng, which displays the all the wireless list available to crack.
- Step-2: Monitor the network by using command: airodump-ng mon0, after this, track the network and copy the BSSID of the network to be cracked.
- Step-3: Use airodump and aireplay to create handshake by opening new terminal and use aireplay command.
- Step-4: Crack the password, once grabbing the handshake, encrypted password will the recovered and ready to crack.
- Step-5: Use Aircrack-ng to crack password using brute force.
- Depending upon how good the password is, the more time it'll take to crack, which will help security specialist to know how good the security is.

How it may be used for harmful purposes by a hacker:

- This tool can be used by attacked in the same way it's used to provide security, just attacker will crack other networks wireless password.
- Attacker can use this tool to crack any wireless security and can launch attacks after getting inside the network.

References:

1) Aircrack-ng, https://www.aircrack-ng.org/doku.php?id=aircrack-ng#how_does_it_work
2) Aircrack-ng, http://www.aircrack-ng.org/doku.php
3) How to hack your own network and beef up the security, https://lifehacker.com/how-to-hack-your-own-network-and-beef-up-its-security-w-1649785071