

Name: Charlie Arbol  
Course: CBS 404A(IT42S3)

Date: May 05, 2024  
Instructor: Mr. Dalisay

## Cyber Security Webinar - Key Takeaways

The recent cybersecurity webinar hosted by MEC Network Corporation proved to be highly enlightening, delving into crucial aspects of cybersecurity essential for safeguarding our digital infrastructure. The session provided a comprehensive overview of the historical evolution of firewalls, the emergence of Software-Defined Wide Area Networks (SDWANs), insights into the Mitre ATT&CK Framework, and fundamental design principles imperative for building resilient IT infrastructures.

One key highlight of the discussion was the evolution of firewalls, progressing from traditional packet-filtering mechanisms to advanced Next-Generation Firewalls (NGFWs). These advancements have become necessary to counter sophisticated cyber threats, such as those necessitating deep packet inspection and application-awareness capabilities, thereby underlining the importance of integrating intelligence into network security devices.

Additionally, the webinar shed light on the transformative potential of Software-Defined Networking in Wide Area Networks (SDWANs), promising enhancements in speed and reliability while revolutionizing network architecture. However, it also emphasized the necessity of implementing precautions, particularly in areas like safeguarding direct internet access and ensuring end-to-end encryption to mitigate potential security vulnerabilities.

Furthermore, the discussion touched upon the Mitre ATT&CK framework, which serves as a valuable repository of adversary tactics and techniques, offering organizations insights into potential vulnerabilities within their systems. It underscored the critical importance of robust security measures to counteract potential threats effectively.

Lastly, the webinar emphasized fundamental design principles essential for establishing secure and resilient IT infrastructures. These principles encompass adopting multi-layered defense mechanisms, implementing minimum necessary privilege controls, conducting regular security assessments, and fostering a culture of awareness and responsibility for information protection across all organizational levels.

In conclusion, the MEC Network Corporation cybersecurity seminar provided invaluable insights into various facets of cybersecurity, ranging from the evolution of firewalls to the significance of SDWANs, the Mitre ATT&CK framework, and fundamental design principles. In an era marked by heightened global connectivity, organizations must remain vigilant and informed to effectively mitigate the diverse risks posed by evolving cyber threats.

#### ATTENDANCE:

The screenshot displays a Zoom Workplace interface during a webinar. The main window shows a presentation titled "MITRE AND ATT&CK" with a table of 17 techniques categorized into Reconnaissance, Resource Development, Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, and Credential Access. The source is cited as <https://attack.mitre.org/>. The right sidebar shows a list of 56 participants. The participant "TIP MNL - Arbol, Charlie" is circled in the list. The list includes names like Apuli, Emilie Mae L. (Me), BT-JM Dalisay (Host), MEC\_FRED GERONIMO (Co-host), J.torio@mec.ph (Co-host), Shania Mhier delos Reyes, and others.

Category	Technique	Count	
Reconnaissance	Active Scanning	13	
	Cyber Victim Host Information	13	
	Cyber Victim Identity Information	13	
	Cyber Victim Network Information	13	
	Cyber Victim Org Information	13	
	Phishing for Information	13	
	Search Closed Sources	13	
	Search Open Technical Sources	13	
	Search Open Websites Domains	13	
	Search Victim-Owned Websites	13	
	Resource Development	Acquire Infrastructure	7
		Compromise Account	7
		Compromise Infrastructure	7
Develop Capabilities		7	
Exfiltrate Data		7	
Obtain Capabilities		7	
Stage Capabilities		7	
Initial Access	Cloud by Compromise	5	
	Exploit Public-Facing Application	5	
	Internal Service Services	5	
	Malware	5	
	Phishing	5	
Execution	Command and Scripting Interactions	5	
	Container Administration Command	5	
	Deploy Container	5	
	Exploitation for Client Execution	5	
	Inter-Process Communication	5	
Persistence	Account Manipulation	5	
	BTLS Jobs	5	
	Boot or Logon Automation	5	
	Event or Logon Installation	5	
	Event or Logon Installation	5	
Privilege Escalation	Abuse Elevated Control Mechanism	5	
	Access Token Manipulation	5	
	Build or Logon Automation	5	
	Event or Logon Installation	5	
	Event or Logon Installation	5	
Defense Evasion	Abuse Elevation Control Mechanism	5	
	Access Token Manipulation	5	
	Build or Logon Automation	5	
	Event or Logon Installation	5	
	Event or Logon Installation	5	
Credential Access	Abuse Elevation Control Mechanism	5	
	Access Token Manipulation	5	
	Build or Logon Automation	5	
	Event or Logon Installation	5	
	Event or Logon Installation	5	