



**June 3 – 5, 2024**

Sheraton Dallas in Dallas, Texas

“Strengthening Ecosystems: Aligning Stakeholders to Bridge the Cybersecurity Workforce Gap”

# ChatGPT Assisted Cybersecurity Training of Veterans and Active Service Military

11:00 AM – 11:45 AM at Dallas D2

**Presenter: Dr. Rob Williams, DLG**

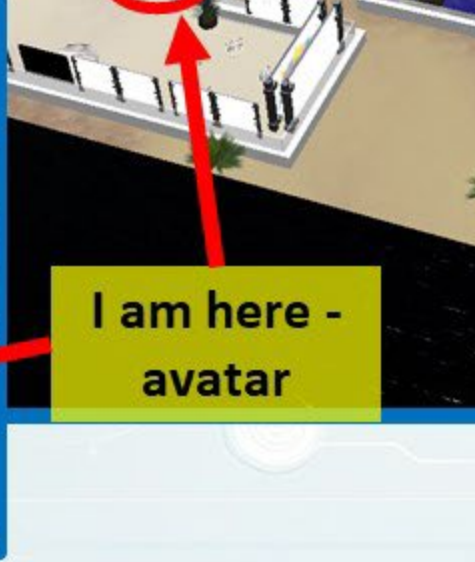
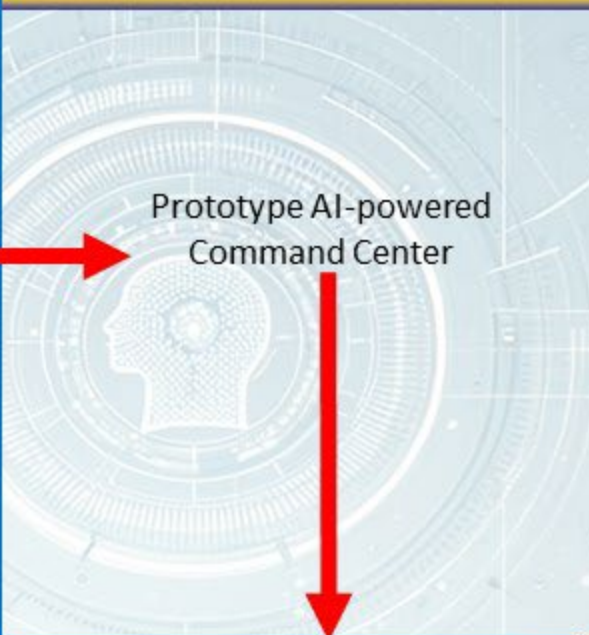
**[Rob.Williams@discoverylabglobal.com](mailto:Rob.Williams@discoverylabglobal.com)**



# Bottom Line Up Front

- 1. Disruptive Gamechanger:** ChatGPT has amplified and accelerated AI plus Cybersecurity project-based learning inside DHX by nearly an order-of-magnitude. CVAP – partnership with **University of Cincinnati** as Dept Labor funded program.
- 2. AI Digital Instructor:** ChatGPT helps students complete our Smart Pong AI project in Deep Learning AI despite starting with very little AI experience.
- 3. AI Digital Tutor:** ChatGPT helps veterans pass the CompTIA Security+ certification exam on 1<sup>st</sup> attempt despite no prior Cybersecurity experience.
- 4. Ask:** CVAP is in our last year. We want to “pass the baton” to continue this “battle-tested” AI-powered, 3D-virtual AI & Cyber campus approach **beyond our DLG.**

# TODAY: Current 3D Virtual DLG Campus Bldg (AI & Cyber) - a potentially powerful convergence of AI, Cybersecurity, and Virtual Reality



# Cybersecurity – Veterans Assistance Program (C-VAP)

## ChatGPT – Digital Tutor for Cybersecurity



**Cybersecurity – Veterans Assistance Program (C-VAP)** – cybersecurity boot camp to help veterans, active service military and others prepare for the **CompTIA Security+** certification exam and to pass it on their first attempt – even if they start our program with zero IT / Cybersecurity background.

heavily stylized, notional illustration of CVAP program inside of DHX.

# Why CompTIA Security+ Certification?

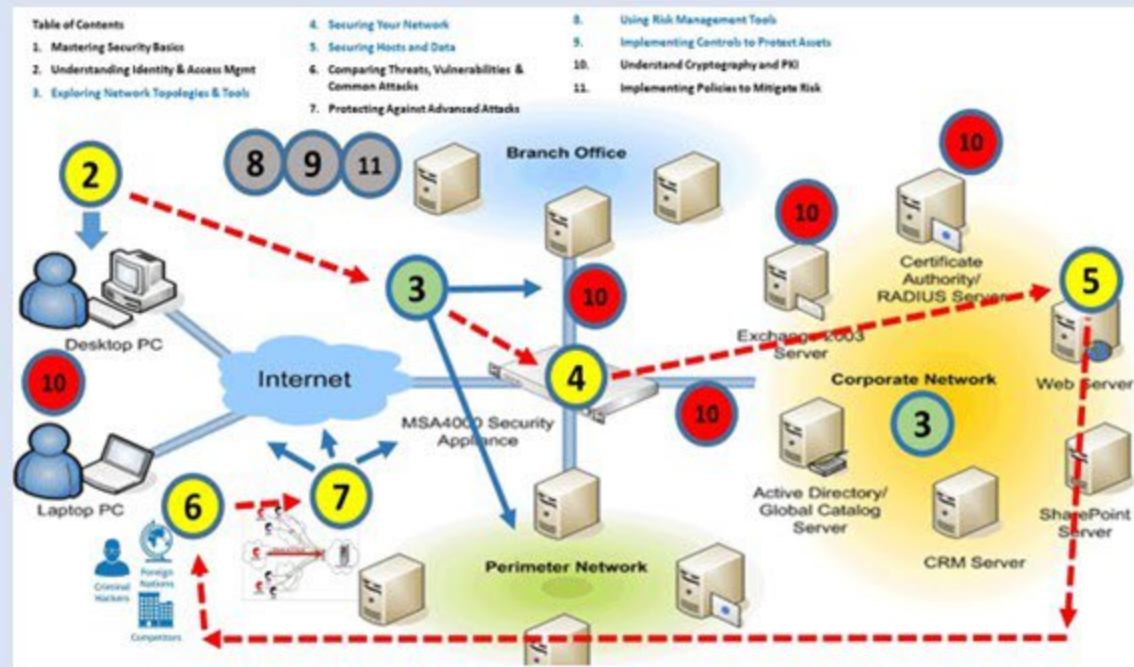
1. **Security+ is a certification sponsored by CompTIA, the Computing Technology Industry Association.**
2. **Security+ is an authorized certification for DoD.**
  - Viewed by many in government and in industry as a **“gold standard”** for entry level certification.
3. **One of the more popular cybersecurity certification for most DoD personnel largely because**
  - It validates familiarity with key cybersecurity concepts
  - It has no mandatory experience requirements
  - It is vendor agnostic – more generalized
  - It focuses on a broad spectrum of important topics



Examples from the internet

# Table of Contents – Course Synopsis

1. Mastering Security Basics
2. Understanding Identity & Access Mgmt
3. Exploring Network Topologies & Tools
4. Securing Your Network
5. Securing Hosts and Data
6. Comparing Threats, Vulnerabilities & Common Attacks
7. Protecting Against Advanced Attacks
8. Using Risk Management Tools
9. Implementing Controls to Protect Assets
10. Understand Cryptography and PKI
11. Implementing Policies to Mitigate Risk



# One chart summary of ChatGPT

## Attention Is All You Need

Ashish Vaswani\*  
Google Brain  
avaaswani@google.com

Noam Shazeer\*  
Google Brain  
noam@google.com

Niki Parmar\*  
Google Research  
nikip@google.com

Jakob Uszkoreit\*  
Google Research  
usz@google.com

Llion Jones\*  
Google Research  
llion@google.com

Aidan N. Gomez†  
University of Toronto  
aidan@cs.toronto.edu

Lukasz Kaiser\*  
Google Brain  
lukaszkaizer@google.com

Illia Polosukhin\*  
illia.polosukhin@gmail.com

### Abstract

The dominant sequence transduction models are based on complex recurrent or convolutional neural networks that include an encoder and a decoder. The best performing models also connect the encoder and decoder through an attention mechanism. We propose a new simple network architecture, the Transformer, based solely on attention mechanisms, dispensing with recurrence and convolutions entirely. Experiments on two machine translation tasks show these models to be superior in quality while being more parallelizable and requiring significantly less time to train. Our model achieves 28.4 BLEU on the WMT 2014 English-to-German translation task, improving over the existing best results, including ensembles, by over 2 BLEU. On the WMT 2014 English-to-French translation task, our model establishes a new single-model state-of-the-art BLEU score of 41.8 after training for 3.5 days on eight GPUs, a small fraction of the training costs of the best models from the literature. We show that the Transformer generalizes well to other tasks by applying it successfully to English constituency parsing both with large and limited training data.

### 1 Introduction

Recurrent neural networks, long short-term memory [13] and gated recurrent [7] neural networks in particular, have been firmly established as state of the art approaches in sequence modeling and

\*Equal contribution. Listing order is random. Jakob proposed replacing RNNs with self-attention and started the effort to evaluate this idea. Ashish, with Illia, designed and implemented the first Transformer models and has been crucially involved in every aspect of this work. Noam proposed scaled dot-product attention, multi-head attention and the parameter-free position representation and became the other person involved in nearly every detail. Niki designed, implemented, tuned and evaluated countless model variants in our original codebase and tensor2tensor. Llion also experimented with novel model variants, was responsible for our initial codebase, and efficient inference and visualizations. Lukasz and Aidan spent countless long days designing various parts of and implementing tensor2tensor, replacing our earlier codebase, greatly improving results and massively accelerating our research.

†Work performed while at Google Brain.

‡Work performed while at Google Research.

## Generative Pre-trained Transformers

### Deep Learning Neural Networks

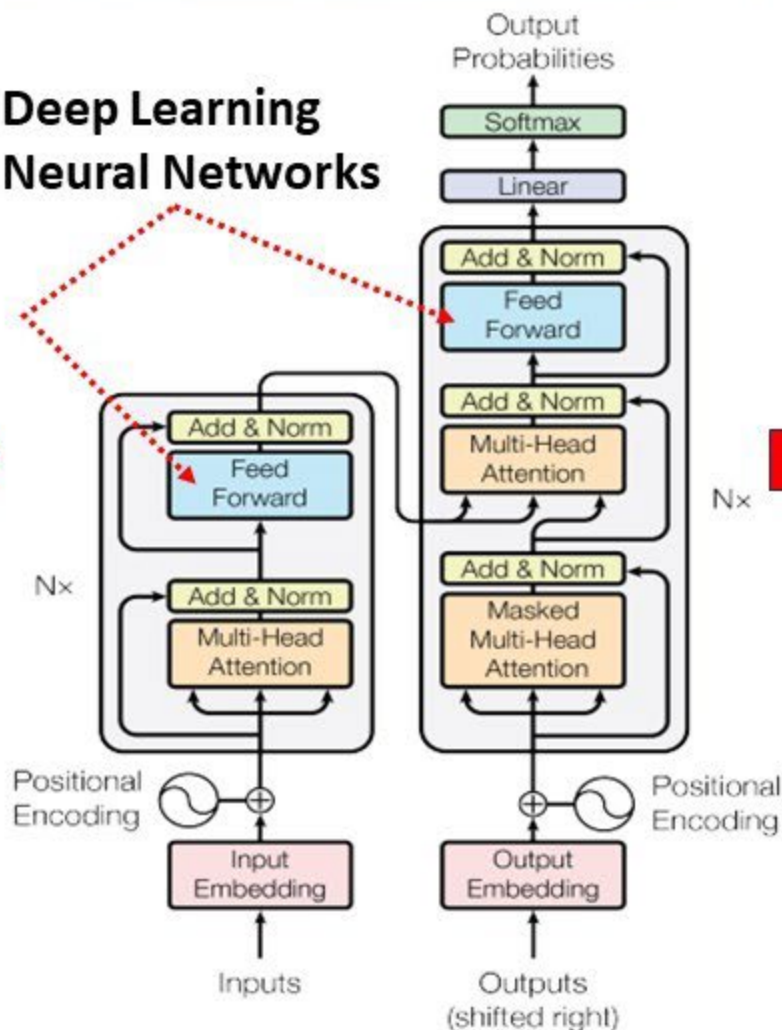


Figure 1: The Transformer - model architecture.

1. **Transformer** architecture for language understanding and generation.
2. It breaks down **input text** into smaller units called **tokens**.
3. **Tokens** are converted into numerical vectors known as **embeddings**.
4. **Embeddings** capture word meanings and relationships.
5. **Self-attention** mechanisms analyze contextual dependencies.

# Today's ChatGPT → Tomorrow's "Model - T"



CHATGPT  
TODAY

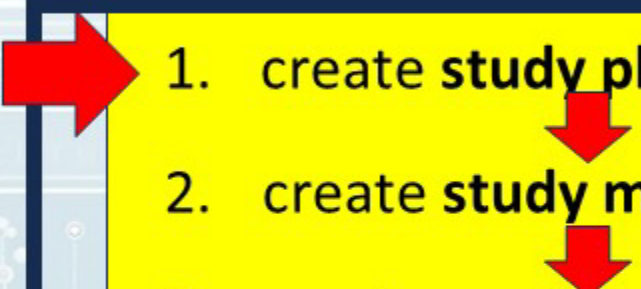
TOMORROW



## We used ChatGPT as AI tool for teaching Cybersecurity

1. create **study plan** for DLG's CVAP CompTIA Security+ program
2. create **study material** to help prepare for the certification exam
3. create practice **exam questions** to help prepare for the certification exam
4. create a **Capture The Flag (CTF)** – in early prototyping phase
5. create a **90-question Security+ exam**
6. create a **summer cybersecurity program** for high school teachers – ready to go

# We used ChatGPT as AI tool for teaching Cybersecurity

- 
1. create **study plan** for DLG's CVAP CompTIA Security+ program
  2. create **study material** to help prepare for the certification exam
  3. create practice **exam questions** to help prepare for the certification exam
  4. create a **Capture The Flag (CTF)** – in early prototyping phase
  5. create a **90-question Security+ exam**
  6. create a **summer cybersecurity program** for high school teachers – ready to go

# #1 create **study plan** (entire 11 weeks)

1

**Prompt:** Generate a weekly study plan for 15 hours per week for 11 weeks that cover all the major topics of Darril Gibson's "CompTIA Security+ Get Certified Get Ahead: SY0-701 Study Guide" that includes time to study at least 40 pages per week, complete at least 5 hours of homework / lab projects per week, conduct at least 4 hours per week of independent study and 2 hours of class time every week.

2

## ChatGPT

Certainly, here's a **revised** weekly study plan for 15 hours per week for 11 weeks, with Week 11 as the final week:

### Weeks 1-2: Introduction and Threats, Attacks, and Vulnerabilities

- Class Time: 2 hours
- Independent Study: 2 hours
- Reading: Chapters 1-2 (80 pages)
- Homework/Lab: Complete relevant exercises

### Weeks 3-4: Architecture and Design

- Class Time: 2 hours
- Independent Study: 2 hours
- Reading: Chapter 3 (40 pages)
- Homework/Lab: Complete relevant exercises

### Weeks 5-6: Implementation and Operations and Incident Response

- Class Time: 2 hours

- Independent Study: 2 hours
- Reading: Chapters 4-5 (80 pages)
- Homework/Lab: Complete relevant exercises

### Weeks 7-8: Governance, Risk, and Compliance and Cryptography and PKI

- Class Time: 2 hours
- Independent Study: 2 hours
- Reading: Chapters 6-7 (80 pages)
- Homework/Lab: Complete relevant exercises

### Weeks 9-10: Identity and Access Management and Networking

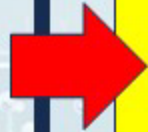
- Class Time: 2 hours
- Independent Study: 2 hours
- Reading: Chapters 8-9 (80 pages)
- Homework/Lab: Complete relevant exercises

### Weeks 11: Security Assessment and Testing and Malware and Social Engineering

- Class Time: 2 hours
- Independent Study: 2 hours
- Reading: Chapters 10-11 (80 pages)
- Homework/Lab: Complete relevant exercises
- Review and practice exams

## We used ChatGPT as AI tool for teaching Cybersecurity

1. create **study plan** for DLG's CVAP CompTIA Security+ program
2. create **study material** to help prepare for the certification exam
3. create practice **exam questions** to help prepare for the certification exam
4. create a **Capture The Flag (CTF)** – in early prototyping phase
5. create a **90-question Security+ exam**
6. create a **summer cybersecurity program** for high school teachers – ready to go



# #2 generate more detailed **study plan** – to identify topics

**Prompt:** Generate a weekly study plan for 15 hours per week for 11 weeks that cover all the major topics of Darril Gibson's "CompTIA Security+ Get Certified Get Ahead: SY0-701 Study Guide" that includes time to study at least 40 pages per week, complete at least 5 hours of homework / lab projects per week, conduct at least 4 hours per week of independent study and 2 hours of class time every week.

## ChatGPT

Certainly, here's a **revised** weekly study plan for 15 hours per week for 11 weeks, with Week 11 as the final week:

### Weeks 1-2: Introduction and Threats, Attacks, and Vulnerabilities

- Class Time: 2 hours
- Independent Study: 2 hours
- Reading: Chapters 1-2 (80 pages)
- Homework/Lab: Complete relevant exercises

### Weeks 3-4: Architecture and Design

- Class Time: 2 hours
- Independent Study: 2 hours
- Reading: Chapter 3 (40 pages)
- Homework/Lab: Complete relevant exercises

### Weeks 5-6: Implementation and Operations and Incident Response

- Class Time: 2 hours

- Independent Study: 2 hours
- Reading: Chapters 4-5 (80 pages)
- Homework/Lab: Complete relevant exercises

### Weeks 7-8: Governance, Risk, and Compliance and Cryptography and PKI

- Class Time: 2 hours
- Independent Study: 2 hours
- Reading: Chapters 6-7 (80 pages)
- Homework/Lab: Complete relevant exercises

### Weeks 9-10: Identity and Access Management and Networking

- Class Time: 2 hours
- Independent Study: 2 hours
- Reading: Chapters 8-9 (80 pages)
- Homework/Lab: Complete relevant exercises

### Weeks 11: Security Assessment and Testing and Malware and Social Engineering

- Class Time: 2 hours
- Independent Study: 2 hours
- Reading: Chapters 10-11 (80 pages)
- Homework/Lab: Complete relevant exercises
- Review and practice exams

1



# #3 single out one topic to generate example **study material**

1

**Prompt:** Expand on Week 9 to include what topics should be studied

**ChatGPT Response:** To provide a more detailed breakdown for Week 9, focusing on Identity and Access Management as part of your CompTIA Security+ study plan, **we can include specific topics that are essential for understanding this area.** Here's an expanded view of what should be covered:

## **Week 9: Identity and Access Management**

**Objective:** Gain a thorough understanding of the mechanisms and principles behind identity management and access control systems.

### **Class Time (2 hours)**

- **Session 1 (1 hour): Introduction to Identity Management**
  - Overview of identity lifecycle (provisioning, management, deprovisioning)
  - Discussion of identity as a security layer in various architectures

- **Session 2 (1 hour): Access Control Systems**
  - Types of access controls: DAC, MAC, RBAC, ABAC
  - Examples of each type of control in practice

### **Reading (Chapter 8 – approx. 40 pages)**

- **Main Focus:**
  - Authentication methods and technologies, including **Kerberos**, SAML, OAuth, and OpenID Connect.
  - Detailed look at how these protocols manage identities and provide secure access.

### **Homework/Lab (1 hour) ...snip...snip....**

### **Additional Study Topics: ...snip...snip.**

### **Review and Practice ...snip...snip...**

This detailed plan ensures a comprehensive understanding of Identity and Access Management, including theoretical concepts, practical implementations, and current technologies used in the field. If you have specific areas within these topics that you'd like to focus more deeply on or any other related topics to add, let me know!

# #4 generate **study material** for the topic

1

## **ChatGPT Prompt: Explain Kerberos**

### **ChatGPT Response:**

Kerberos is a network authentication protocol designed to provide secure authentication for users and services over a non-secure network, such as the internet. It was developed by MIT as an open-source project and has become widely used in various computing environments, particularly in enterprise networks.

2

## **Here's a high-level explanation of how Kerberos works:**

- Authentication Server (AS):** The authentication process begins with an Authentication Server (AS). When a user wants to access a service, they send a request to the AS.
- Authentication:** The AS verifies the user's identity and issues a Ticket Granting Ticket (TGT) if the user's credentials are correct. The TGT is encrypted and can only be decrypted by the Ticket Granting Server (TGS).
- Ticket Granting Server (TGS):** The user then sends the TGT to the TGS, requesting access to a specific service.
- Service Ticket:** If the TGT is valid, the TGS issues a Service Ticket for the requested service. The Service Ticket is also encrypted and can only be decrypted by the service itself.
- Accessing the Service:** The user presents the Service Ticket to the desired service. The service decrypts the ticket and verifies its authenticity. If the ticket is valid, the user is granted access to the service.

3

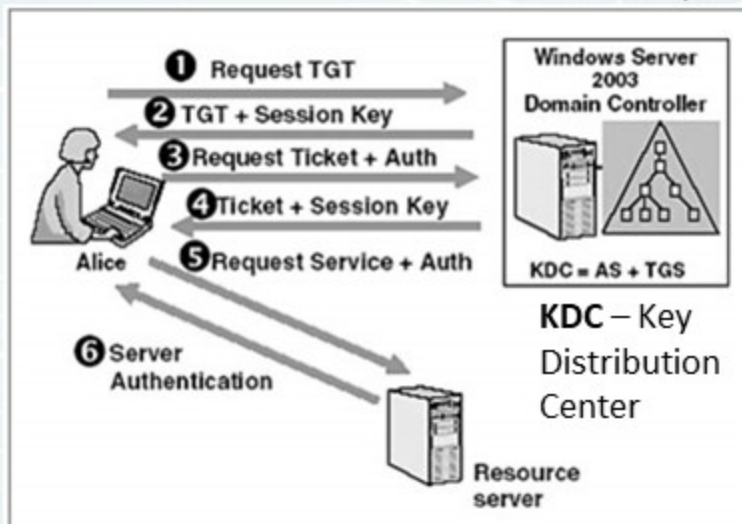
## **Key characteristics and benefits of Kerberos:**

**Single Sign-On (SSO):** Once a user has obtained a TGT, they can request service tickets for multiple services without needing to re-enter their credentials. This provides a seamless and secure SSO experience.

**Mutual Authentication:** Both the user and the service authenticate each other, ensuring that both parties are who they claim to be. This prevents unauthorized access.

**Strong Encryption:** Kerberos relies on strong encryption to protect the authentication process and the tickets exchanged between the AS, TGS, and services. This makes it highly resistant to eavesdropping and replay attacks.

**Ticket Expiration:** Tickets have a limited validity period, reducing the risk of unauthorized access in case a ticket is intercepted.



# #5 generate **study material** suitable for a high school teacher

**Prompt:** Explain Kerberos to a high school teacher with no cybersecurity background

1

**ChatGPT:** Certainly! Explaining Kerberos to someone with no cybersecurity background can be challenging, but I'll provide a simple and **relatable analogy** to help a high school teacher understand the basic concept of Kerberos authentication.

2

**Imagine you have a magic ticket that you use to enter a secret club.**

This magic ticket is like your "authentication token" in the digital world. The club, in this case, represents a computer system, server, or network that you want to access securely.

**Here's how the Kerberos authentication process works in this analogy:**

**1. Getting the Magic Ticket (Authentication):** Before you can enter the **secret club** (access the computer system), you need to get your magic ticket. To do this, you go to the ticket office (a special server) and provide your name (your username) to the ticket seller (the server).

**2. Getting Your Personal Magic Ticket (Ticket Granting Ticket or TGT):** The ticket seller knows you, so they give you a **special "personal magic ticket"** called a Ticket Granting Ticket (TGT). This TGT is like a key that can be used to get other tickets without having to reveal your name each time.

**3. Requesting Access to the Club (Access to the Computer System):** Now, when you want to enter the club (access the computer system), you don't need to go back to the ticket office. Instead, you show your TGT to the **club's doorman** (the computer system).

**4. Getting the Club Entry Ticket (Service Ticket):** The doorman recognizes your TGT and gives you a **temporary "club entry ticket"** (Service Ticket). This ticket allows you to enter the club (access the computer system) without showing your TGT again.

**5. Accessing the Club (Accessing the Computer System):** With the club entry ticket (Service Ticket), **you can enter the club** (access the computer system) and enjoy its resources and services.

**6. Leaving the Club (Logging Out):** When you're done, you leave the club (log out of the computer system), and your club entry ticket (Service Ticket) **becomes invalid**.


**In this analogy, Kerberos acts like the ticket office and manages the authentication process to ensure that only authorized users can access the computer system.** The TGT and Service Ticket are temporary, secure tokens that allow users to access resources without exposing their sensitive information (like passwords) every time they want to access something.

**Kerberos authentication provides a secure way for users to prove their identity to computer systems and access resources without constantly revealing their secrets, just like having a magic ticket to enter a secret club.**





## We used ChatGPT as AI tool for teaching Cybersecurity

1. create **study plan** for DLG's CVAP CompTIA Security+ program
2. create **study material** to help prepare for the certification exam
- 
 3. create practice **exam questions** to help prepare for the certification exam
4. create a **Capture The Flag (CTF)** – in early prototyping phase
5. create a **90-question Security+ exam**
6. create a **summer cybersecurity program** for high school teachers – ready to go

# #6 generate practice exam question for Kerberos

**1 Prompt:** create a scenario-based practice exam question for **Kerberos** with four choices. Indicate which is the **best choice**. Then explain why the **other options are incorrect**.

**2 ChatGPT Answer:** Your company is planning to implement a centralized authentication service for its network infrastructure. The IT team is tasked with selecting the most suitable authentication protocol. The requirements include strong security, support for single sign-on (SSO), and seamless integration with existing Windows-based systems. Additionally, the company wants to minimize the risk of transmitting plaintext credentials over the network. **Which of the following authentication protocols would be the BEST choice for meeting these requirements?**

- A. RADIUS
- B. LDAP
- C. Kerberos**
- D. NTLM

**3** →

**4 Explanation:**

**C. Kerberos:** In this scenario, the best choice for the authentication protocol is Kerberos. Kerberos is a widely adopted authentication protocol that meets the specified requirements. It provides strong security through the use of tickets, supports single sign-on (SSO) for seamless user experience, and integrates well with existing Windows-based systems, particularly Active Directory. Additionally, Kerberos mitigates the risk of transmitting plaintext credentials over the network by using mutual authentication and encryption.

**5 Why the other options are incorrect:**

**A. RADIUS:** While RADIUS (Remote Authentication Dial-In User Service) is commonly used for centralized authentication in network environments, it is primarily designed for remote access authentication and lacks native support for SSO and integration with Windows-based systems like Active Directory.

**B. LDAP:** LDAP (Lightweight Directory Access Protocol) is a protocol used for querying and modifying directory services such as Active Directory. While LDAP can be used for authentication, it does not provide native support for SSO and may require additional components to achieve seamless integration and strong security.

**D. NTLM:** NTLM (NT LAN Manager) authentication is an older authentication protocol used in Windows environments. While it may be supported by existing Windows systems, it lacks the advanced security features and SSO capabilities provided by Kerberos. Additionally, NTLM has known security vulnerabilities, such as susceptibility to pass-the-hash attacks.

**6 Therefore, in this scenario, Kerberos is the best choice** for meeting the requirements of strong security, support for SSO, seamless integration with existing Windows-based systems, and minimizing the risk of transmitting plaintext credentials over the network.

But every once in a while, ChatGPT gets the answer to the test question ... **“wrong”**.

But even there, we learn something more about the power of ChatGPT as follows!

## ChatGPT Post Chapter 2 Questions (6-15)

### Question 8:

You need to provide a junior administrator with appropriate credentials to rebuild a domain controller after it suffers a catastrophic failure. Of the following choices, what type of account would BEST meet this need? Explain the best answer and why the other answers are incorrect.

- A. User Account
- B. Generic account
- C. Guest account
- D. Service Account

**Student assignment was to give ChatGPT practice exam questions from our textbook to see how it did.**

## ChatGPT Post Chapter 2 Questions (6-15)

Question 8:

1

You need to provide a junior administrator with appropriate credentials to rebuild a domain controller after it suffers a catastrophic failure. Of the following choices, what type of account would BEST meet this need? Explain the best answer and why the other answers are incorrect.

- A. User Account
- B. Generic account
- C. Guest account
- D. Service Account

### ChatGPT Response: 2

The type of account that would BEST meet the need to provide a junior administrator with appropriate credentials to rebuild a domain controller after a catastrophic failure is:

**D. Service Account**

### Explanation: 3

**Service Account:** A service account is specifically designed to run services, tasks, or applications on a system. In the context of rebuilding a domain controller, a service account with the necessary permissions and rights would be suitable for carrying out the required tasks without exposing unnecessary privileges. It provides a more controlled and secure way to grant access for specific tasks.

### Why the other options are not the best: 4

- A. User Account:** While it's possible to use a user account, it may have unnecessary permissions and may not be as securely managed as a service account. Using a user account can expose more privileges than needed for the task.
- B. Generic Account:** A generic account is typically a shared account used by multiple users. Using a shared account for such a critical task introduces accountability issues and makes it difficult to trace actions to individual administrators. It's generally not recommended for security reasons.
- C. Guest Account:** Guest accounts are typically used for providing temporary and limited access. They are not suitable for the kind of privileged and critical tasks involved in rebuilding a domain controller.

## ChatGPT Post Chapter 2 Questions (6-15)

Question 8:

1

You need to provide a junior administrator with appropriate credentials to rebuild a domain controller after it suffers a catastrophic failure. Of the following choices, what type of account would BEST meet this need? Explain the best answer and why the other answers are incorrect.

- A. User Account
- B. Generic account
- C. Guest account
- D. Service Account

**ChatGPT Response:**

2

The type of account that would BEST meet the need to provide a junior administrator with appropriate credentials to rebuild a domain controller after a catastrophic failure is:

**D. Service Account**

**Explanation:**

3

**Service Account:** A service account is specifically designed to run services, tasks, or applications on a system. In the context of rebuilding a domain controller, a service account with the necessary permissions and rights would be suitable for carrying out the required tasks without exposing unnecessary privileges. It provides a more controlled and secure way to grant access for specific tasks.

**Why the other options are not the best:**

4

**A. User Account:** While it's possible to use a user account, it may have unnecessary permissions and may not be as securely managed as a service account. Using a user account can expose more privileges than needed for the task.

**B. Generic Account:** A generic account is typically a shared account used by multiple users. Using a shared account for such a critical task introduces accountability issues and makes it difficult to trace actions to individual administrators. It's generally not recommended for security reasons.

**C. Guest Account:** Guest accounts are typically used for providing temporary and limited access. They are not suitable for the kind of privileged and critical tasks involved in rebuilding a domain controller.

**CHATGPT Answer: D – Service Account**

**ChatGPT disagrees with textbook answer and doesn't back down.**

**Textbook Answer: A – User Account**

5

**ChatGPT response as to why it must disagree with the textbook:**

6

If the textbook suggests a user account as the answer for providing a junior administrator with credentials to rebuild a domain controller after a catastrophic failure, it may be due to different perspectives or context. ...snip . Here are some reasons why a user account might not be the optimal choice, and why I suggested a service account... etc

**ChatGPT was asked – how the question could've been better phrased:**

7

The original question was clear in its intent, but to ...snip..., **you might consider adding specific details to the question that highlight these aspects. Here's how you could rewrite the question:**

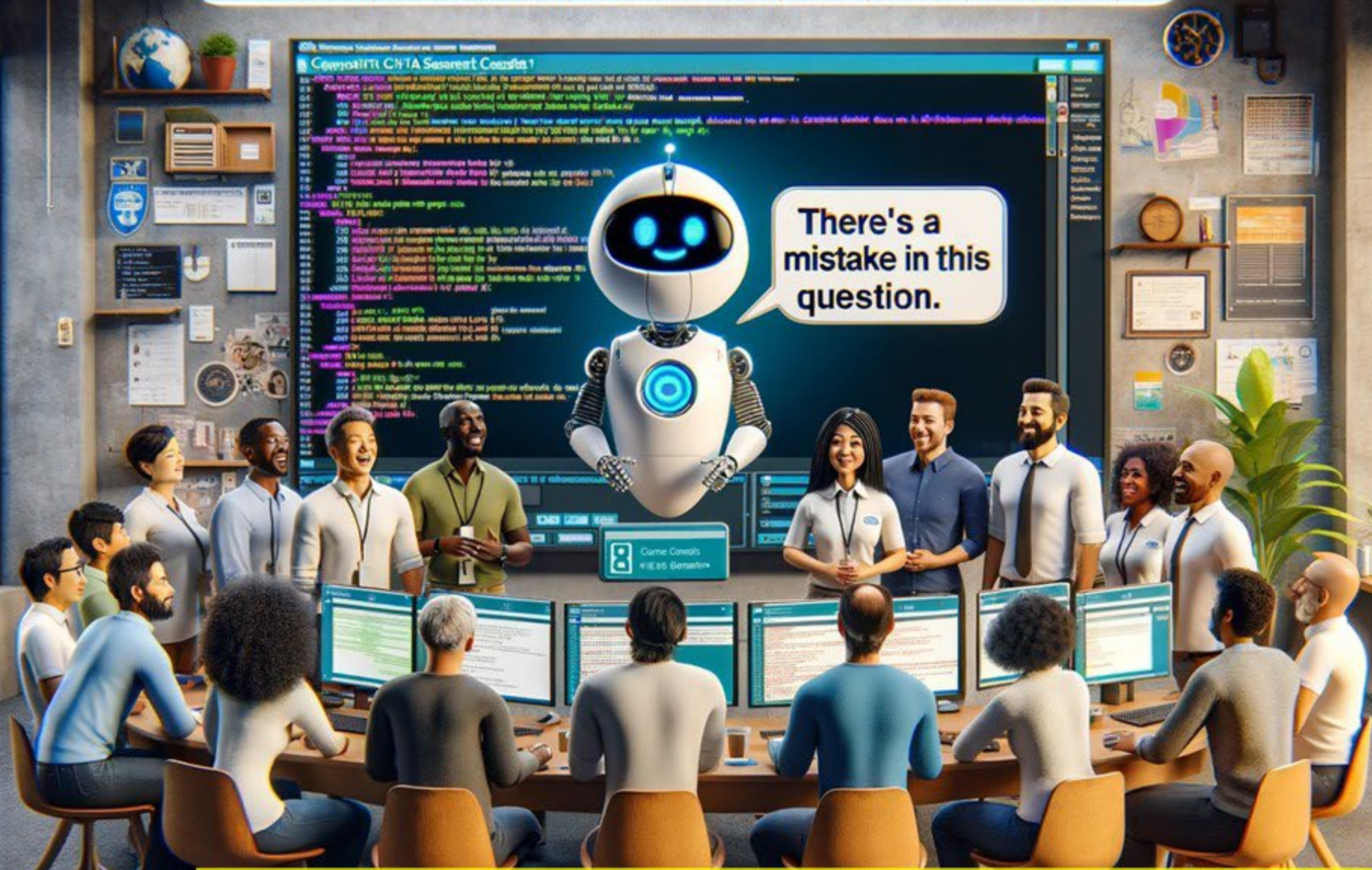
"You are tasked with delegating the rebuild of a domain controller after a catastrophic failure to a junior administrator. You need to provide them with ...snip...snip..."

**By adding details about security best practices and the need for individual accountability and auditability, the question steers the answer towards the use of a specific user account with appropriate privileges, which is the standard approach in IT administration for such tasks.**

This may be one reason why some past students who have taken the certification (and passed it on their first attempt) have complained about some of the test questions feeling like “trick” questions ...  
**because even ChatGPT got confused!**

So maybe in the future CompTIA might ...





**In the scene, the creators of the CompTIA Security+ exam are engaging with ChatGPT, which points out an error in a test question and offers a correct alternative, highlighting a collaborative moment of insight and correction.**

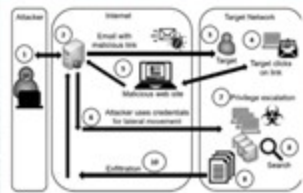


Figure 6.2: Steps in an attack

ChatGPT 4o created this step-by-step from Figure 6.2 which was given to it.

**Attacker (Step 1):** The attacker prepares to launch the attack. They start by setting up the infrastructure needed to deliver the malicious payload.

**Email with Malicious Link (Step 2):** The attacker sends an email containing a malicious link to the target. This step is designed to be convincing to increase the chance of the target clicking on the link.

**Target Receives Email (Step 3):** The target, an individual within the organization, receives the email. The email appears legitimate to avoid raising suspicion.

**Target Clicks on Link (Step 4):** The target clicks on the link, which redirects them to a compromised or malicious website.

**Malicious Website (Step 5):** The malicious website may exploit vulnerabilities in the target's web browser or prompt the target to download malware. This site is designed to look legitimate to avoid raising suspicion.

**Attacker Uses Credentials for Lateral Movement (Step 6):** If the malware successfully infects the target's device, it may capture the target's credentials. The attacker uses these credentials to move laterally across the network, gaining access to other systems and data.

**Privilege Escalation (Step 7):** The attacker escalates their privileges to gain higher levels of access within the network. This step involves exploiting additional vulnerabilities to gain administrative or root access.

**Search (Step 8):** With elevated privileges, the attacker searches the network for valuable information. They might look for sensitive data, financial information, intellectual property, or other valuable assets.

**Data Collection (Step 9):** The attacker collects the valuable data they have gathered. This data can then be compiled and used for various purposes, such as financial fraud, or selling the data on the dark web.

## Can Understand & Explain Complex Diagrams to Students

This step-by-step process highlights the typical flow of a targeted email attack, emphasizing the importance of cybersecurity measures at each stage to prevent such breaches.

This step-by-step process highlights the typical flow of a targeted email attack, emphasizing the importance of cybersecurity measures at each stage to prevent such breaches.

### Analysis and Assessment of John Doe's eWeekly Reports

eWeekly 240324 SelfScore=6 DirScore=6 L...  
Date of Submission: 240324 Sunday  
Last Day of Reporting Period: 240429 Sunday  
Student's Name: [Redacted]  
Total Hours Worked (1 to Week): 15  
Self Assessment Score (1 to 5): 6  
Projected Mentor/Director Score (1 to 5): 5  
Milestone Score (1 to 5): 6

1. Weekly Major Accomplishments:

- Monday: 3 hours: Today I spent a lot of time just looking at the model and trying to figure out how I could make it better. Again, progress is still being made, but just at a very slow pace. I figured the maybe how to do with how weak my computer is, and how much memory the model is taking up inside the machine. I'll look into how I can optimize the code further so it fits my laptop's capabilities. I also worked on the documentation, focusing on the fundamentals of machine learning.
- Tuesday: 3 hours: Another 5000 episodes started at a very low -21 mean, and I'm spending a lot of time just looking into ways for me to improve the learning pace. Other than that, I am making slow progress with the documentation because most of my time was spent investigating the code.
- Wednesday: 3 hours: Another 10000 episodes, the model is still inconsistent, and I progress when compared to games are progressing. It is now taking a progress being made of ML and RL.
- Thursday: 3 hours: This indicates the first win after about 50000+ episodes. I wonder why that is because Kasperly in his blog said that his model achieved consistent wins after only 8000 episodes, whereas mine is still inconsistent, where some games would go incredibly well and some would fall miserably. But the positive score is, again, a sign of progress so I think I'll let it continue.

**General Overview:** John Doe has provided a detailed account of his weekly progress in the development and documentation of a machine learning model. The reports span over three weeks, where Long reflects on major accomplishments, challenges, and lessons learned, while continuously improving both his code and documentation.

**Accomplishments:** **Progress in Model Development:** John Doe managed to improve the model's performance from an average score of -21 to achieving sporadic wins with a positive score, showcasing gradual but significant improvements. This indicates persistent and focused efforts on model tuning and optimization.

**Documentation:** Throughout the reporting period, John Doe dedicated significant time to producing comprehensive documentation that explains both the theoretical underpinnings and practical implementations of his project. This effort culminates in three detailed documents aimed at encapsulating the entire project scope and development nuances.

**Challenges and Solutions:** **Computational Limitations:** Limited computational resources potentially using more efficient algorithms as the model complexity increases.

**Inconsistent Model Performance:** Despite achieving some positive scores, the model displayed inconsistency in performance. John Doe plans to explore hyperparameter tuning and different batch sizes to enhance model consistency and performance.

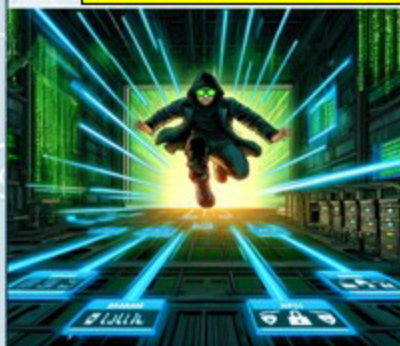
**ChatGPT Prompt:** Score each eWeekly from 1 (Awful) to 10 (Awesome).  
**ChatGPT Response:** Week 1 (7) - Week 2 (6) - Week 3 (8)

## Help "Study" Student Weekly Progress Reports and Provide Initial Assessments

### Chapter 5: SECURING HOSTS AND DATA (Phase 1)



## Create Illustrations from Written Instructions



VM Escape by ChatGPT



Data Loss Prevention by ChatGPT



Data Encryption by ChatGPT

### The next steps in the integration of AI and Cybersecurity inside of our 3D virtual campus

## Help Create "Ethical Hacking" Track inside 3D Virtual Campus



Security+ Certification "Bootcamp" inworld

Hands-on Ethical Hacking micro-projects inworld

# Recapping

1. **Disruptive Gamechanger**: ChatGPT has amplified and accelerated AI plus Cybersecurity project-based learning inside DHX by nearly an order-of-magnitude. CVAP – partnership with **University of Cincinnati** as Dept Labor funded program.
2. **AI Digital Instructor**: ChatGPT helps students complete our Smart Pong AI project in Deep Learning AI despite starting with very little AI experience.
3. **AI Digital Tutor**: ChatGPT helps veterans pass the CompTIA Security+ certification exam on 1<sup>st</sup> attempt despite no prior Cybersecurity experience.
4. **Ask**: CVAP is in our last year. We want to “pass the baton” to continue this “battle-tested” AI-powered, 3D-virtual AI & Cyber campus approach **beyond our DLG**.

**Thank you! Are there any questions?**

**Presenter: Dr. Rob Williams, DLG**  
**[Rob.Williams@discoverylabglobal.com](mailto:Rob.Williams@discoverylabglobal.com)**

