Golden Ticket Attack

Golden Ticket Attacks target the Kerberos authentication protocol, which is widely used in Windows environments for securely authenticating users and services. A successful attack grants the attacker unlimited access to the system or network.

How a Golden Ticket Attack Works:

- Key Distribution Center (KDC) is compromised.
- Once inside the KDC, the attacker extracts the cryptographic keys to create and verify Kerberos tickets.
- The attacker forges a special Kerberos ticket known as a "golden ticket" to impersonate users and gain access to any network resources.
- The attacker can embed the golden ticket within the compromised network, ensuring persistent access even if their initial entry point is discovered and closed.
- Unrestricted Access: With the golden ticket, the attacker can access, modify, or exfiltrate data, install malware, and perform other malicious actions on the network.

Mitigating Golden Ticket Attacks:

1. Protecting and monitoring the Key Distribution Center (KDC) and domain controllers to prevent unauthorized access.
2. Implementing strong network segmentation and access controls to limit lateral movement by attackers.
3. Enforcing strict account and password policies to reduce the risk of credential theft.
4. Regularly monitoring network activity for signs of suspicious or unauthorized behavior.
5. Employing the principle of least privilege, ensuring that users and accounts have only the necessary permissions to perform their tasks.
6. Implementing multi-factor authentication (MFA) to make it more difficult for attackers to gain access to critical systems.

www.thecentexitguy.com

Centex Technologies

CENTEX TECHNOLOGIES

13355 Noel Road,Suite #1100
Dallas, TX 75240

Phone: (972) 375 - 9654

501 N. 4th Street,
Killeen, TX 76541

Phone: (254) 213 - 4740

1201 Peachtree ST NE,
400 Colony Square #200
Atlanta, GA 30361

Phone: (404) 994 - 5074

Capital Factory, 701
BrazosStreet, Suite 500
Austin, TX 78701

Phone: (512) 956 - 5454