JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Attacking AAA Protocols and Systems

Security Architecture & Tool Sets

Attacking AAA Protocols and Systems

- Directory, authentication, and SSO systems are great targets for attacks to go after
- Attackers use specific vulnerabilities and misconfigurations to target the AAA protocol itself or how a server implements the protocol
- Attempting system compromises of domain controllers and AAA systems is common

Attacking LDAP

- Target unencrypted LDAP traffic to capture traffic for replay attacks
  - Use secure binding to prevent this
- Target improper access controls to harvest directory information or to modify directory
  - Setup good access controls
- Perform LDAP injection against vulnerable web applications that interface with directory
  - Validate web-based input and use least privilege
- Conduct Denial-of-Service against LDAP to cause services to fail which rely on it
  - Design scalable LDAP for redundancy

RADIUS

- Authentication commonly used for network devices and VPNs can be attacked by…
  - Session replay of server or client responses
  - Compromising shared secret key from client machines
  - Brute-force share secret key from a stolen password
  - Denial-of-Service to prevent user authentication

Kerberos

- Relies on central key distribution center (KDC)

- Compromise of KDC allows impersonation as any user
- Common attacks:
  - Stealing administrator account credentials
  - Kerberos ticket reuse
    - Pass-the-ticket allows impersonation for ticket lifespan
    - Pass-the-key allows reusing secret key to get new tickets
  - Ticket Granting Ticket (TGT) attacks
    - “Golden Ticket” allows creation of new tickets, account changes, and creation of new accounts/services

Active Directory

- Core identity store and AAA service for Microsoft Windows domains
    - Many exploits built for clients, servers, and AD

- Many Windows domains contain older systems still…
    - or are at least backward configurations still activated which makes them vulnerable to attack

- Very common target for attackers

Attacks on Active Directory

- Malware focused on stealing credentials
  …or Phishing or social engineering
- Malware focused on Windows server exploit
- Focus on attacking older services like NTLM, LANMAN, NetBIOS, unsigned LDAP, or SMB
- Privilege creep of service accounts
- Overuse of domain admin credentials
- Privilege escalation attacks

OAuth, OpenID, OpenID Connect

- OAuth and OpenID are implemented by each service provider leading to configuration flaws
- Open redirects are a common attack
  - Redirects and forwards aren’t validated
  - Untrusted user input can be sent to web apps
  - Users can be redirected to untrusted websites
  - Potential for phishing, pharming, or bypassing of website security
- Original account information will not be compromised, but your web application may allow in untrusted users

OAuth, OpenID, OpenID Connect

- OpenID attacks have been directed at vulnerabilities in the protocol itself
  - Example:
    - Attackers forged request to gain arbitrary logins

- OAuth2 is vulnerable to cross-site request forgery (CSRF) attacks
  - Attack attempts to get user to click a link so that their browser performs an action as the user

- OpenID Connect provides extra encryption and signing to prevent many of these exploits