Authentication Based Attacks

Tools in Kali Linux

Module #27

Kali Linux: Authentication Definition?

Authentication is the act of confirming the trust of one's identity. This might involve confirming the identity of a person, program, or hardware, such as verifying XYZ is a government employee, as well as his laptop is issued by the government agency.
As a Penetration Tester, it is valuable to be able to gain the trust of a system and bypass security as an authorized entity.

The Certified Information Systems Security Professional (CISSP) curriculum classifies authentication based on three factor types, as follows:

- Something you know, such as a PIN or password
- Something you have, such as a smart card
- Something you are, such as a fingerprint

Kali Linux: Authentication Definition?

The most common method by which people confirm their identity is using something they know, such as a password.

We have already seen various ways to crack passwords while attacking host systems. Cracking a password will get you access to some systems however, many targets will leverage multifactor authentication, meaning a combination of authentication steps to prove one's identity.

Kali Linux: Authentication Definition?

It is common that user authentication involves the use of a username and password combination. It becomes cumbersome for a user to enter this information every time authentication is required.

To overcome this, single sign-on was created as a means to authenticate one to a central authority that is trusted by other websites. The central authority will verify trust on behalf of the user or device, so the user can access multiple secured systems without having to be prompted at each security gateway.

A common trusted authority is a Windows domain controller, providing authentication for internal users to intranet resources. In such cases, compromising a trusted authority or account with high privileges could mean access to many other internal resources in this type of system.

Kali Linux: Attacking session management?

With regards to web applications, a session is the length of time users spend on a website.

Best practice is managing authorized sessions (that is, what you are permitted to access), based on how people and devices authenticate as well as, controlling what and how long resources are available during the active session.

This makes authentication a key aspect of managing authorized sessions.

Kali Linux: Attacking session management?

The goal for a Penetration Tester is to identify accounts that are permitted access to sessions with high-level privileges, and unlimited time to access the web application.

This is why session management security features, such as session timeout intervals and SSL certificates, were created.

Tools available in Kali can identify flaws in how sessions are managed, such as capturing an active session on a web application post user logout, and using that session for another person (also known as a session fixation attack).

Kali Linux: Attacking session management?

Session management attacks can occur using vulnerabilities in applications or how users access and authenticate to those applications.

Common ways attackers do this is through cross-site scripting or SQL injection attacks to a web server.

Attackers can also take advantage of session cookies in web browsers or vulnerabilities in web pages to achieve similar results.

Kali Linux: Clickjacking?

Clickjacking is a technique where an attacker tricks a user into clicking something other than what they believe they are clicking.

Clickjacking can be used to reveal confidential information, such as the login credentials, as well as permitting an attacker to take control of the victim's computer. Clickjacking usually exposes a web browser security issue or vulnerability using embedded code or script that executes without the victim's knowledge.

One example of performing clickjacking is having the hyperlink text to a trusted site different than the actual site. The average user doesn't verify hyperlinks prior to clicking, or notices changes associated with common clickjacking attempts, making this a very effective form of attack.

Kali Linux: Clickjacking?

In the following example, the user will see Visit us on Facebook.com however, when they click on the text, they will actually be redirected to www.badfacebook.com .

Visit Us on Facebook.com

Clickjacking can be more malicious and complicated than changing hyperlinks. Attackers who use clickjacking normally embed iFrames into a webpage. The content of the iFrames contains data from the target website and usually placed over a legitimate link making it difficult to detect.

Kali Linux: Hijacking web session cookies?

Cookies are a small piece of data sent from a website and stored on a user's web browser while the user is accessing the website. The website can use a cookie to verify the user's return to the site and obtain details about the user's previous activity.

This can include what pages were accessed, how they logged in, and what buttons were pressed. Anytime you log into a website, such as Facebook, Gmail, or Wordpress, your browser assigns you a cookie.

Kali Linux: Hijacking web session cookies?

Cookies can include tracking history from users for long periods of time, including behavior on a website years ago.

Cookies can also store passwords and form values a user has previously filled, such as their home address or credit card number.

A session token is delivered from a web server anytime a host authenticates. The token is used as a way to recognize among different connections. Session hijacking occurs when an attacker captures a session token and injects it into their own browser to gain access to the victim's authenticated session. Essentially, it is the act of replacing an attacker's unauthorized cookie with a victim's authorized cookie.

Kali Linux: Hijacking web session cookies?

Some limitations of session hijacking attacks:

- Stealing cookies is useless if the target is using https:// for browsing, and end-to-end encryption is enabled. Adoption has been slow; however, most secured websites provide this defense against session hijacking attacks.

- Most cookies expire when the target logs out of a session. This also logs the attacker out of the session. This is a problem for some mobile apps that leverage cookies that don't expire, meaning an attacker could gain access for life if a valid session token is captured.

Thank You