

A

1

CSRF requests contain the session cookies which are automatically added by browser. That’s why servers treat the requests as genuine.

2

TLS is easier to deploy since security is implemented by application. OS that provides TCP/IP stack does not need to change. IPsec requires an update to OS, which is time taking and not always feasible (e.g. on old and unsupported hardware).

3

Divert attacker’s attention away from critical systems.

Collect information about the attacker behaviours.

Engage the attacker to stay on the system long enough for administration to respond.

B

1

* Identify a vulnerability in target site.
* Exploit that to inject malicious <script> to site database.
* A user visits the vulnerable site. Attacker’s <script> is bundled in the response sent to user.
* In victim’s browser, the script runs and **redirects** the user to a phishing page.

2

It securely carries the data/messages created by upper layers (HTTP, SMTP etc.). All packets are encrypted and authenticated.

3

When it is desirable to monitor a critical machine (e.g. a server) rather than whole subnet. Host based can work better in cases when network traffic is encrypted, it can detect both internal and external intrusions, and has access to more detailed system logs, which are not visible to NIDS.

4

Default should be drop/deny all packets.