Attack Types

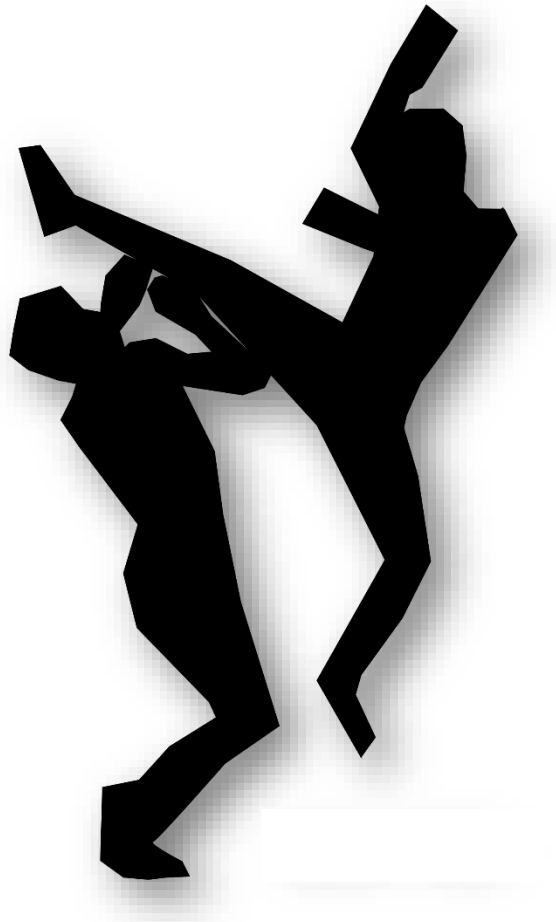
Dale Meredith

@dalemeredith | www.daledumbsitdown.com

Invincibility lies in the defense, the possibility of victory in the attack

— Sun Tzu

Categories of Attacks



- Application attacks
- Misconfiguration attacks
- Shrink-wrap code attacks
- O/S attacks
- Entry Points

Application Attacks

Causes

- Time
- Features
- QA
- Add-on

Results

- Buffer overflows
- Cross-site scripting
- Active content
- DoS and SYN
- SQL Injection

Other App Attacks

- Session hijacking
- Man in the Middle
- Directory traversal

Misconfiguration Attacks

Targets

- Web servers
- Application platforms
- Frameworks
- Databases
- Hardware

Shrink-wrap Code Attacks

```
    $computername = $env:computername
    $username = 'AdminAccount1'
    $password = 'topSecret@99'
    $desc = 'Automatically created local admin
account'
    $computer =
[ADSI]"WinNT://$computername,computer"
    $user = $computer.Create("user", $username)
    $user.SetPassword($password)
    $user.Setinfo()
    $user.description = $desc
    $user.setinfo()
    $user.UserFlags = 65536
    $user.SetInfo()
    $group =
[ADSI]("WinNT://$computername/administrators,group
")
    $group.add("WinNT://$username,user")
```

- Lazy developers take short cuts
- Fine tune scripts
- Build-in scripts

O/S Attacks

Gaining access via vulnerabilities

O/S vulnerabilities via defaults

O/S attacks via non-updated systems

Entry Points for an Attack

Remote Network	Local Network	Social Engineering
Dial-Up Network	Stolen Equipment	Physical Entry

Summary

- Application attacks
- Misconfiguration attacks
- Shrink-wrap code attacks
- O/S attacks
- Entry Points