


Security Threats and Attack Vectors



Dale Meredith

@dalemeredith | www.daledumbsitdown.com

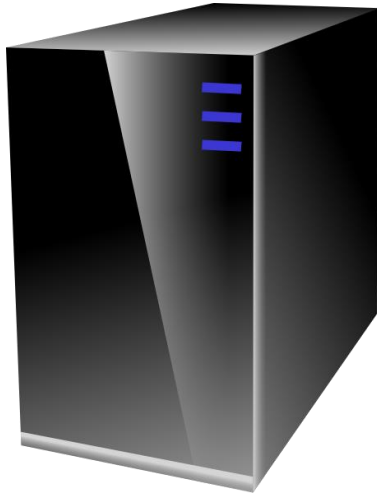


We live in a society exquisitely dependent on science and technology, in which hardly anyone knows anything about science and technology.

— Carl Sagan



Understanding What You Face



- Security threats
- Attack vectors
- IPv6

Security Threats

“What Could Possibly Be a Threat in My Network?”

Security Threats

Hosts

Natural

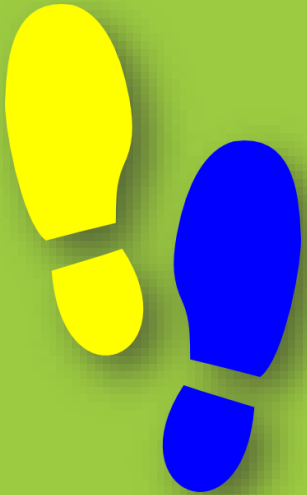
Physical

Applications

Human

Network

Hosts



Footprinting



Physical Security



Passwords



Malware

Hosts



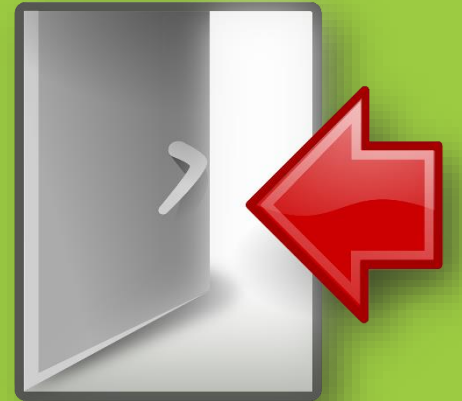
Denial of Service



Unauthorized
Access



Privilege Escalation



Back Doors

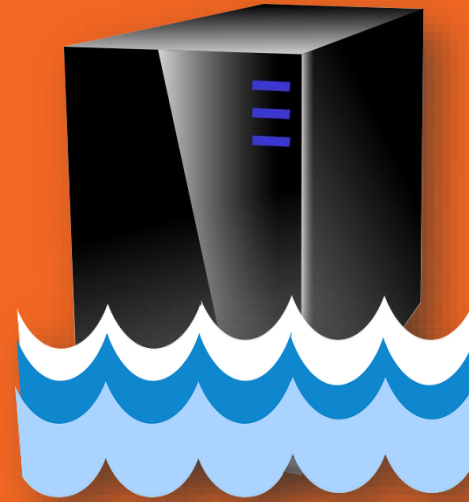
Natural



Earthquakes



Hurricanes



Floods



Natural Disasters

Physical



Theft



Impact



Power



End of Life

Applications



Configuration

```
A problem has been detected and Windows has been shut down to prevent damage to your computer.

The problem seems to be caused by the following file: SPOMDCON.SYS
PAGE_FAULT_IN_NONPAGED_AREA

If this is the first time you've seen this stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any Windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.

Technical information:
*** STOP: 0x00000050 (0xFB3094C2,0x00000001,0xFBFE7617,0x00000000)
*** SPOMDCON.SYS - Address FBFE7617 base at FBFE5000, DateStamp 3d6d267c
```

Buffer Overflow

```
<!DOCTYPE html>
<html>
<!--
Created 16-10-2014
-->
<head>
<title>Sample</title>
</head>
<body>
<p>Sample text</p>
</body>
</html>
```

The HTML code above produces the following below

← → ↻ file:///k.html

Sample text

Lazy Coding

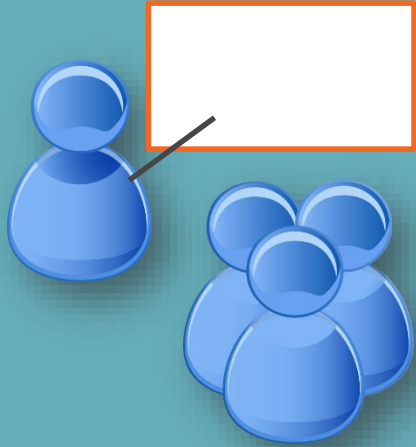


Data/Input
Validation

Human



Malicious
Employees



Lack of Training



Social Networking



Hackers

Network



Sniffing /
Eavesdropping



ARP Poisoning



DoS



Spoofing

Top Security Vectors

Cloud

Mobile

Ransomware

Virus/Worms

Advanced
Persistent Threats

Botnets

Top Security Vectors

Phishing

Web Applications

Insiders

IoT

Threat Categories

Network Threats

- ☐ Information gathering
- ☐ Sniffing / Eavesdropping
- ☐ Spoofing
- ☐ Firewall / IDS attacks
- ☐ Passwords
- ☐ ARP / DNS poisoning
- ☐ Session / MiTM
- ☐ DoS
- ☐ Compromised-keys

Host Threats

- ☐ Unauthorized access
- ☐ Privilege escalation
- ☐ Backdoors
- ☐ Physical
- ☐ Malware
- ☐ Footprinting
- ☐ Profiling
- ☐ Passwords
- ☐ DoS

Application Threats

- ☐ Phishing
- ☐ SQL injection
- ☐ Error handling
- ☐ Cryptography attacks
- ☐ Data/Input validation
- ☐ Auth attacks
- ☐ Misconfigurations
- ☐ Information disclosure
- ☐ Buffer overflows

Where Do Most Attacks Come From?

External

Foreign Countries

Internal

Attack Vectors

“Shields! Red Alert!”

How Many Attack Vectors Are You Aware Of?

- VM & Cloud environments
- Unpatched OS/software
- Social networking
- Internal users
- Hackivism
- Malware
- Botnets
- Security staffing
- Lack of security policies
- Compliance with regulations/laws
- Complexity of network infrastructure
- Mobile devices

How Many Attack Vectors Are You Aware Of?

- Botnets
- Security staffing
- Lack of security policies
- Compliance with regulations/laws
- Complexity of network infrastructure
- Mobile devices
- Ransomware
- Advanced Persistent Threats
- Phishing
- Web Applications
- IoT

IPv6

New and “Improved” IP?

How Many Attack Vectors Are You Aware Of?

- Auto configuration
- Incompatibility of logging systems
- Default activation
- Shortcuts
- Bigger headers
- 4to6 translation
- Multiple IP's per device
- Network discovery

Summary



- Security threats
- Attack vectors
- IPv6