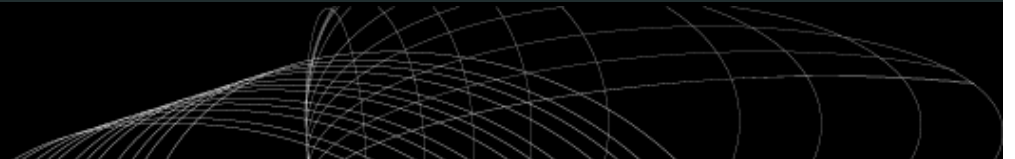


# Proof is in the Penetration

Max Caceres

Core Security Technologies



# Vulnerability Scanning or Penetration Testing?



Dave's new job  
as a Pen Tester  
wasn't anything  
at all like he'd  
expected

# Vulnerability Scanning

Look for **evidence** of

- Vulnerable software versions
- Presence or lack of patches
- Misconfiguration

# With authentication

- Do you have the right things in your registry?
- Do you have updated files?
  - DLL versions
  - Hashes

# Without authentication

- Service checks

“WARNING! You are running fingerd!”

- Banner checks

“Knock Knock! – Hi! I’m Apache 1.3.24, how are you?”

- Boss check

“Let’s see how much crap() you can handle”

# Service Check

```
port = get_kb_item("Services/finger");
```

```
...
```

```
    soc = open_sock_tcp(port);
```

```
    if(soc) {
```

```
        buf = string("root\r\n");
```

```
        send(socket:soc, data:buf);
```

```
        data = recv(socket:soc, length:65535);
```

```
        if(egrep(pattern:". *User|[lL]ogin|logged.*", string:data)) {
```

```
            ...
```

```
            security_warning(port:port, data:report);
```

```
        }
```

```
    }
```

# Banner Check

```
if(safe_checks())
{
    if(ereg(pattern:".*Server v(0\.|1\.0\.[0-4][^0-9]).*", string:r))
    {
        security_hole(port);
    }
    exit(0);
}
```

# Boss Check

```
soc = open_sock_tcp(port);  
if(!soc)exit(0); # WTF ?  
poison = crap(520) + '\r\n';  
send(socket:soc, data:poison);  
r = recv_line(socket:soc, length:4096);  
close(soc);
```

```
soc = open_sock_tcp(port);  
if(!soc)security_hole(port);  
send(socket:soc, data:'HELP\r\n');  
r = recv_line(socket:soc, length:4096);  
if(!r)security_hole(port);
```

192.168.36.23 - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites Recycle Bin Mail Print Word Pad Notepad Paint Internet Options

Address <C:\Documents and Settings\max\My Documents\ACTIVE PROJECTS\CSI Annual 2005\Nessus Report\1> Go Links >>

[\[ back to the list of ports \]](#)

### Vulnerability found on port www (80/tcp)

The remote host appears to be vulnerable to the Apache Web Server Chunk Handling Vulnerability.

If Safe Checks are enabled, this may be a false positive since it is based on the version of Apache. Although unpatched Apache versions 1.2.2 and above, 1.3 through 1.3.24 and 2.0 through 2.0.36, the remote server may be running a patched version of Apache

\*\*\* Note : as safe checks are enabled, Nessus solely relied on the banner to issue this alert

Solution : Upgrade to version 1.3.26 or 2.0.39 or newer  
See also : [http://httpd.apache.org/info/security\\_bulletin\\_20020617.txt](http://httpd.apache.org/info/security_bulletin_20020617.txt)  
[http://httpd.apache.org/info/security\\_bulletin\\_20020620.txt](http://httpd.apache.org/info/security_bulletin_20020620.txt)

Risk factor : High  
CVE : [CVE-2002-0392](#)  
BID : [5033](#)  
Other references : LAVA:2002-A-0008  
Nessus ID : [11030](#)

[\[ back to the list of ports \]](#)

My Computer

# Penetration Testing

Attempt to **compromise** security by using the same techniques of the **attacker**

- If I was an attacker, how far would I be able to go?
- How easy is it to compromise this *computer* | *network* | *application* | *system*?

# An Exploit

**Actively** takes advantage of a vulnerability to accomplish something

- Denial of Service
- Obtain private information
- Execute code

# An Exploit for a Code Execution Vulnerability

- Trigger
  - Get control of the execution flow
- Payload
  - Perform some action

# Advisory

MS05-039 Vulnerability in Plug and Play Could Allow Remote Code Execution and Elevation of Privilege

## **Affected Software:**

- Microsoft Windows 2000 SP 4
- Microsoft Windows XP SP1 and SP2
- Microsoft Windows 2003 SP1

# Exploit

- Send special request to PnP interface to write payload in memory and overflow buffer
- Redirect execution to payload in memory

# Exploit Payloads

- Shellcode
- Special functionality
  - Execute a command
  - Run VNC
  - Break out of chroot
- Generic functionality
  - Syscall Proxying
  - Metasploit's Meterpreter
  - Immunity's MOSDEF

What do we really want?

**We want to prevent  
exploitation**

Really don't care about "managing"  
vulnerabilities or patches

# Things We Do To Prevent Exploitation

1. Eliminate vulnerability
2. Reduce connectivity
3. Detect intrusion attempt
4. Detect successful intrusion

# I. Eliminate Vulnerability

- Apply patch
- Reconfigure software
- Turn off service
- Uninstall software
- Disconnect computer

## 2. Reduce Connectivity

- Firewalling
- Segmentation
- End-Point Security

# 3. Detect Intrusion Attempt

- Detect exploit trigger in transit
  - Signature based NIDS, NIPS, Content Filters, AV
- Detect payload in transit
  - Signature based NIDS, NIPS, Content Filters, AV
- Detect network anomalies
  - Anomaly based NIDS, NIPS

# Signature for Exploit Trigger in Transit

```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS
$HTTP_PORTS (msg:"WEB-IIS ISAPI .printer
access"; flow:to_server,established;
uricontent:".printer"; nocase;
reference:arachnids,533;
reference:bugtraq,2674; reference:cve,2001-
0241; reference:nessus,10661;
reference:url,www.microsoft.com/technet/securit
y/bulletin/MS01-023.msp; classtype:web-
application-activity; sid:971; rev:10;)
```

# Signature for Payload in Transit

```
alert ip $EXTERNAL_NET $SHELLCODE_PORTS ->
$HOME_NET any (msg:"SHELLCODE Linux shellcode";
content:"|90 90 90 E8 C0 FF FF FF|/bin/sh";
reference:arachnids,343; classtype:shellcode-
detect; sid:652; rev:9;)
```

## 4. Detect Successful Intrusion

- Detect payload communication
  - Signature and anomaly NIDS / NIPS
- Detect payload executing on host
  - HIDS / HIPS
- Detect unauthorized / abnormal change
  - HIDS, policy enforcement, change monitoring

# Signature for Payload Communication

```
alert tcp $HOME_NET !21:23 -> $EXTERNAL_NET any
(msg:"ATTACK-RESPONSES Microsoft cmd.exe
banner"; flow:established; content:"Microsoft
Windows"; content:"|28|C|29| Copyright 1985-";
distance:0; content:"Microsoft Corp.";
distance:0; reference:nessus,11633;
classtype:successful-admin; sid:2123; rev:3;)
```

# Detect Payload Executing on Host

- API / System Call hooking
  - Systrace, McAfee Enterscept, Cisco Security Agent
- File tampering
  - Tripwire
- Host based anomaly detection

# Prevent Payload from Executing

- Mandatory Access Control
  - SELinux, Novell AppArmor, Trusted Solaris
- W<sup>X</sup>, PaX, DEP
  - OpenBSD, Linux, Windows XP SP 2

Evaluating the effectiveness of the security system as a whole is a complex task

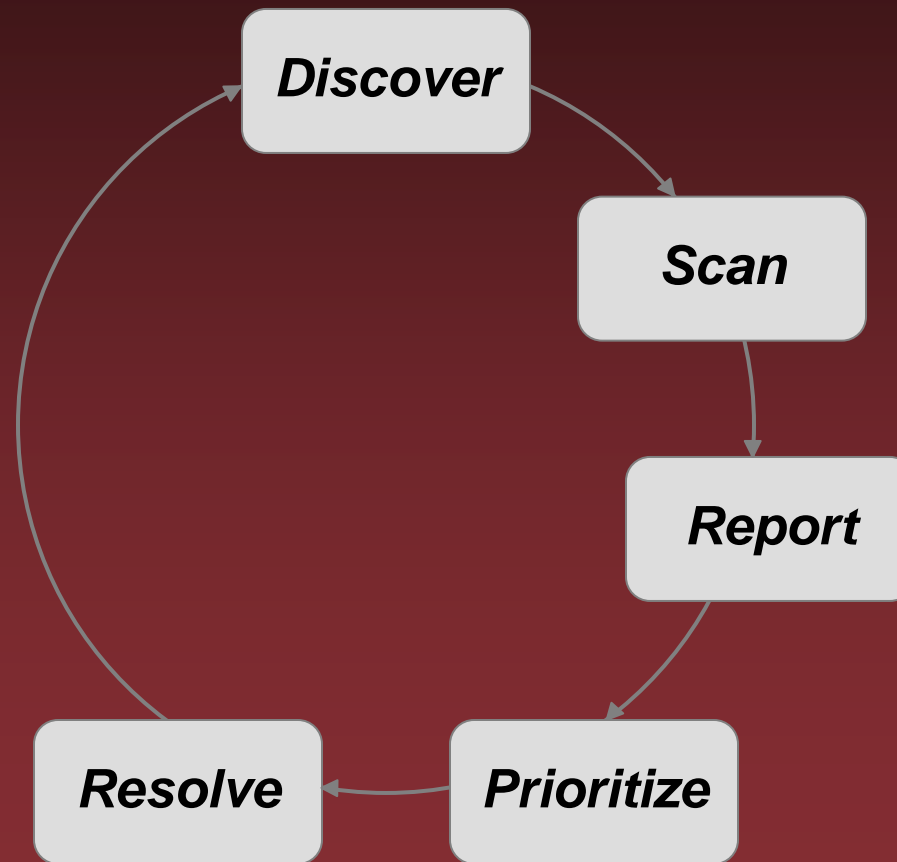
# Benefits of Penetration Testing

- Evaluates effectiveness of overall security program
- Clarity of results, easy to demonstrate risks to others
- Focuses remediation where it is needed first
- Can validate remediation actions beyond patching

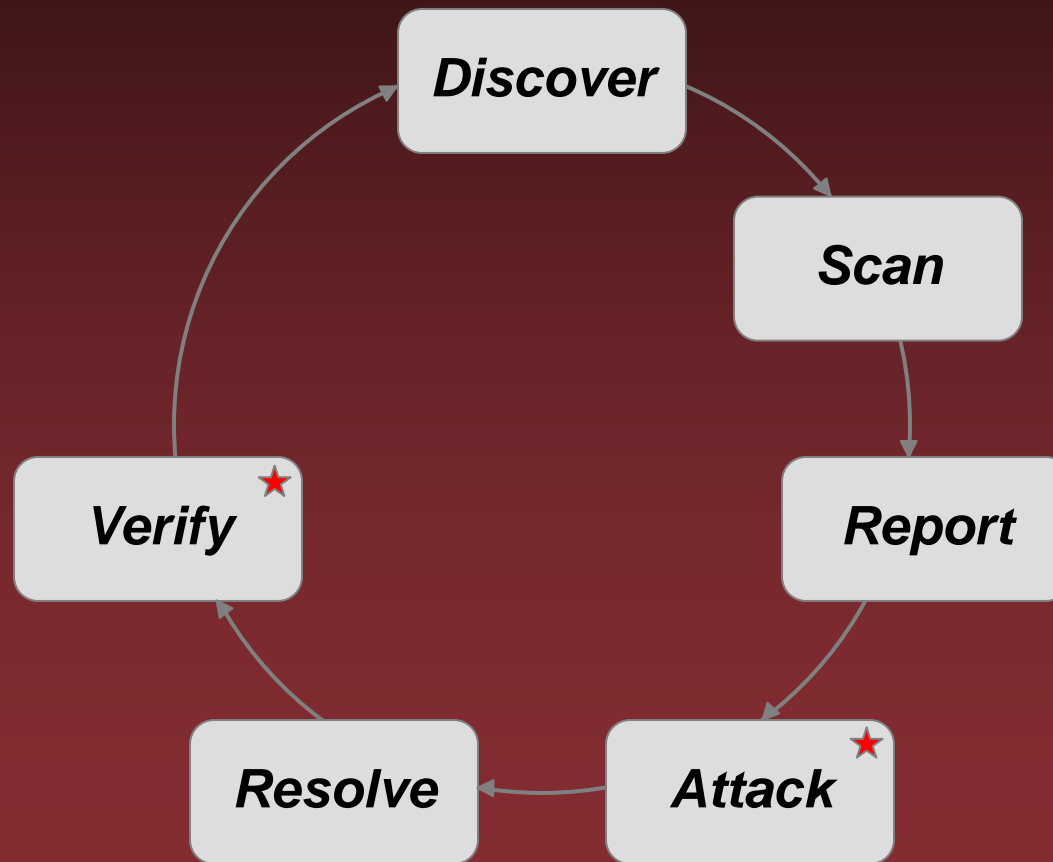
# Pen Testing or Vuln Scanning?

- Vulnerability Scanning is very efficient but does not really represent threat and suffers from false-positives
- Use **real** attacks to evaluate defenses and to complement vulnerability management

# Vulnerability Management



# Augmenting Vuln Management



# Pen Testing and Vuln Scanning

- VS is great for base lining and knowing what you have on your network
- PT is great for prioritizing vulnerabilities and only option for evaluating all defenses

Q & A

Come see us at  
<http://coresecurity.com>

Thank You!

[max\\_at\\_coresecurity.com](mailto:max_at_coresecurity.com)

