Remote Exploitation

The following doc illustrates finding and owning vulnerable network. Might you know well, it is possible to configure/monitor Cisco router using web page. With command: "**ip http server**" you enable web interface, which is by default, but it requires authentication only if you set: "**ip http authentication enable/local**", which is not set by default. **Http HEAD** of the Cisco web page with requiring authentication and without it looks like this:"

- Request:

"HEAD / HTTP/1.0
Connection: close"

- Response from authentication enabled server:

"HTTP/1.0 401 Unauthorized
Date: Fri, 20 Nov 2009 01:54:26 GMT
www-authenticate: Basic realm="level_15_access"
Connection: close
Accept-ranges: none
Server: cisco-IOS"

- Response from authentication disabled server:

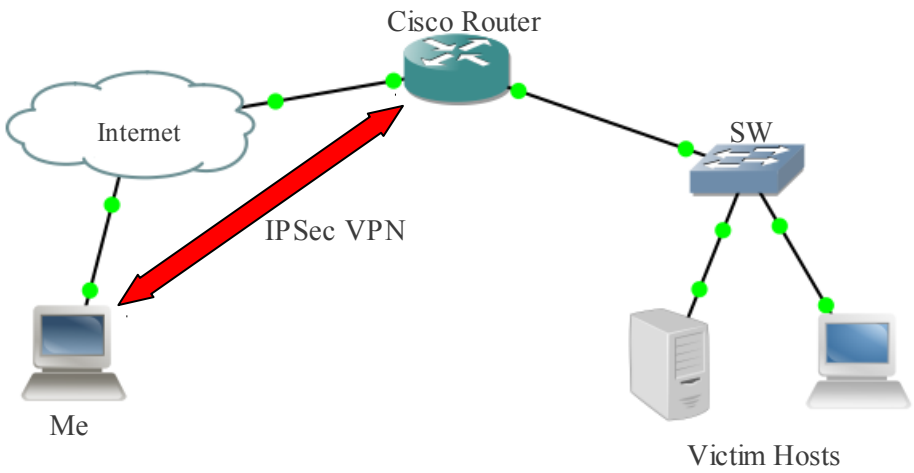
"HTTP/1.0 200 OK
Transfer-encoding: chunked
Accept-ranges: none
Expires: Sun, 30 May 1993 20:24:50 GMT
Server: cisco-IOS
Last-modified: Sun, 30 May 1993 20:24:50 GMT
Connection: close
Cache-control: no-store, no-cache, must-revalidate
Date: Sun, 30 May 1993 20:24:50 GMT
Content-type: text/html"

Interesting parts between this two responses are that, when authentication is disabled, we get **HTTP/1.0 200** response, and to filter from other web applications, we compare Server field response to cisco-IOS.

For wide scanning created simple perl script. Script scans a range of IP addresses for open 80 port, gets HEAD and checks if Server eq **cisco-IOS** and response is **HTTP/1.0 200**, prints the IP address. You can find enough unsecured routers with this method. Web page may launch SDM application, which is GUI way of configuring router, or a single web page, field to enter command, and under the field command output. Both ways wont ask login credentials. After scanning for a while, get some routers.

The next step is setting **VPN** to reach victims local network. I choose configuring router as Cisco easy VPN servers and use VPNC as client. When configuring vpn server, you have to define routes with access-list that will be accessible for clients. With "**show ip route"** I get the list of routes available from this router, and matched all in access-list**.**

Topology



After running VPNC I was able to reach victims local subnets. Left only finding vulnerable host/servers and exploit them. Scanning remote subnet with Nessus would give a pretty good result, but I scanned only for open 445 ports, and used Metasploit to exploit.

Metasploit CLI

```
msf > db_create
[*] Creating a new database instance...
[*] Successfully connected to the database
[*] File: /home/toko/.msf3/sqlite3.db
msf > db_connect
[*] Successfully connected to the database
[*] File: /home/toko/.msf3/sqlite3.db
msf > db_nmap -p 445 -sS 10.12.1-2.0-255
msf > db_autopwn -p -e –b
```

Metasploit will scan hosts for open 445 port and puts them into database. "**db_autopwn -p -e –b"** will execute all matched exploits. For payload it`ll use meterpreter bind shell on random port.

It took some time but at the end, I got about 20 active sessions. List of worked exploits:

- windows/smb/ms06_040_netapi
- windows/smb/ms05_039_pnp
- windows/smb/ms04_011_lsass
- windows/smb/ms03_049_netapi
- windows/smb/ms08_067_netapi

You can upload Trojans on exploited hosts, add user for RDP, if host has additional route that router don't, Metasploit can add route through session, and so on. But I thought it was enough at this point and this is the end of my attack.

So, from my little experience, finding good exploit and searching for vulnerable hosts is a good way, but you may get better result finding points where usually people don't pay attention, unless it`s 0day exploit ☺.

Thanks for reading, and make sure you don't harm others with your knowledge.

Author: CCNA
IRC: irc.hacking.ge #ghc
Date: 05/12/2009
OS: OpenSuSe 11.2
Mail: tokozedg@gmail.com
Greets: xokaido, hex, Hektor
Softwares used:

- Metasploit 3.4: http://www.metasploit.com/
- Angry IP Scanner 3.0: http://www.angryip.org
- VPNC: http://www.vpnc.org/