GRNET NOC

How we got pwnd
(in a pentest...6 years ago)

{ikakavas,kargig}@noc.grnet.gr

External pentest

Execute PHP code in GET request

http://XXXX.grnet.gr/nea/index.php/%22%29;phpinfo%28%29;%23

Reverse Shell with www-data privileges→found a nice backup file in a vhost

/srv/www/XXXX.grnet.gr/oldXXXX/oldroot.tar.gz

Upload static binaries (nmap, socat)→Execute network scans, use as jump point

Scan files→Find php-MySQL configs containing passwords to ZZZZ.grnet.gr→Connect to database, dump user tables containing MD5 passwords→Break MD5 passwords…

External pentest

Get userX password from world readable file. UserX had left the company 4 years ago!

```
/srv/svn/YYYYY.grnet.gr/conf/passwd
```

Connect to wiki.noc.grnet.gr with user/pass from svn→Get topology map, oob VPN CA+configs (userX password did not work for VPN)

Various other XSS, directory traversals, etc

External pentest

0-day SQL injection in www.grnet.gr (same CMS as in.gr used to have)

- Hosted in admin.grnet.gr network
- Database kept cleartext passwords
- Kept logs in the database…easy to clean trail (duh!)
- Directory traversal leading to database credentials leak
- Execute C# code via aspx⟶reverse shell

Reverse shell→scan the “admin” network→Connect to SMB, telnet to admin router

Internal Pentest

NOC network is firewalled from the outside→Add malicious device in the NOC network (no mac filtering + DHCP = partay!!) as relay

Scan NOC administrators range→find VNC (nxtest/nxtest) -> ssh capable !!

```
grep -ir passw /home/username →/home/username/Documents/LiveZilla/login.xml →Base64 encoded username+password
```

ssh with username+password→Got username access!→inject malicious ssh key in ~/.ssh/authorized_keys

Try password...worked for a) root password b) ssh-key password (!!)

Internal Pentest

ssh with ssh-key to jp.noc.grnet.gr

Add 5’ cron to overwrite .ssh/authorized_keys + reverse shell to a destination

On jp.noc.grnet.gr there were world readable files of other NOC users against a) admin.grnet.gr servers (POP3 password) b) router passwords used in automation tool -> administrator access to core backbone routers

ssh with ssh-key to vima2.grnet.gr→loopback mount VM disk→Full VM access

Client-side

Edit www.grnet.gr webpage, add malicious java payload

Send email from NOC manager to multiple NOC admins

User opens email→reverse client connection to pentesters

Found cleartext mail passwords in .netrc→use to VPN→enter NOC internal network→arp spoofing→rang a few bells and access was cut.