Securing Network Access with Open Source Solutions

Nick Owen
BSidesAtlanta
@wikidsystems
nowen@wikidsystems.com
Why increase your remote access?

Because more remote access == less breaches

Rotman/Telus Survey 2009
Is this your Network?

- Lots of firewall rules
- Multiple password datastores
- Lots of protocols
- Static passwords
Our Goal: Securely allow access to the network with simplicity and flexibility.
Authentication
Static Passwords

The most frequent password: '123456', followed by 'password'
Password reuse
Passwords are clearly a 20th Century Technology
Certs & Keys

• Certificates
  – Offline brute-force of passphrase
  – Is there a passphrase?
  – Integration across apps is the real problem

• SSH Keys
  – Love them, but there are audit issues
  – Is there a passphrase?
  – No key expiration system
One-time passwords

- A number of Open Source options:
  - WiKID, Opie, FreeToken, OTP Auth
- Passwords work everywhere
- Just need to change the back-end
Integration

Do you work with???
Flexibility comes from Protocols

- Radius
- LDAP
- TACACS+
- SAML
- etc
Why I like Radius

• Simple. Server, Port, Shared Secret
• It's a pretty standard standard
• All commercial VPN products support it
• Can do ACL
• Freeradius is an excellent product
• Even MS supports proxy radius auth now!
Two tricks to rule the world
PAM rules!

• Once you grok PAM, you get:
  • SSH
  • Sudo
  • Login
  • SFTP
  • Etc, etc, etc
PAM Radius

- Edit `/etc/raddb/server`:
  
  ```
  radiusserverIPaddress  shared_secret  1
  ```

- Edit `/etc/pam.d/sshd` (for example)
  
  ```
  auth sufficient /lib/security/pam_radius_auth.so
  ```
Pam radius example

#%PAM-1.0
auth include system-auth
auth sufficient /lib/security/pam_radius_auth.so
account include system-auth
account sufficient /lib/security/pam_radius_auth.so
password include system-auth
session optional pam_keyinit.so force revoke
session include system-auth
SSH

• Create an SSH Gateway box
  – All users auth using 2 Factor to the GW
  – Use keys out from Gateway for SSO
  – No password file on Gateway boxes
  – No remote root access
  – Sudo requires 2\textsuperscript{nd} OTP

• Use the command line token :)
When Auditors Attack!
OpenVPN

Create an /etc/pam.d/openvpn file
Add to client.conf or client.opvn:
auth-user-pass

Add to server.conf:
plugin /usr/share/openvpn/plugin/lib/openvpn-auth-pam.so
openvpn
Postgresql

Edit the pg_hba.conf:

`host  all    all    192.168.0.0/24      pam postgresql`

Edit your `/etc/pam.d/postgresql`

What about MySQL?
Remote Desktop

- FreeNX, NoMachine, Tacix, NeatX (google)
- Remote X, VNC, RDP, desktop sharing and session shadowing
- Tunneled through SSH
- Auth via pam: /etc/pam.d/sshd
- Quite Fast
Apache!

- Http-auth, & most web apps
- CMSs
- Web-DAV
- Webmail
- Wordpress
- PHPBB, Etc, etc
Apache Radius Example

Install mod-auth-radius
$ sudo apt-get install libapache-mod-auth-radius

In your httpd.conf add:
AddRadiusAuth radius_server:1812 shared_secret 5
AddRadiusCookieValid 60

Remember Radius is port 1812 *UDP*
Apache Radius Example con't

Enter this into your apache2.conf:

```
<location>
	Options Indexes FollowSymlinks
	AuthType Basic
	AuthName "WiKID RADIUS authentication"
	AuthBasicAuthoritative Off
	AuthBasicProvider radius
	AuthRadiusAuthoritative on
	AuthRadiusActive On

Require valid-user
</location>
```

Restart Apache!
### Wordpress Admin

#### Manage Plugins

<table>
<thead>
<tr>
<th>Plugin</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Akismet</td>
<td>Akismet checks your comments and will use it. You can review the template. See also: WP Static_blog.</td>
</tr>
<tr>
<td>Hello Dolly</td>
<td>This is not just a plugin, it's actually Armstrong: Hello, Dolly.</td>
</tr>
<tr>
<td>HTTP Authentication</td>
<td>Authenticate users using HTTP.</td>
</tr>
</tbody>
</table>

**Bulk Actions**

- **Activate**
- **Delete**
- **Version** 2.2.6 | By Matt M
- **Version** 1.5.1 | By Matt M
- **Version** 2.2 | By Daniel W
Protect wp-login

<FilesMatch "wp-login\.php$">
    Satisfy all
    AuthType Basic
    AuthBasicProvider xradius
    AuthName "Username and WiKID one-time passcode."
    AuthXRadiusAddServer "192.168.1.171:1812" "secret"
    AuthXRadiusTimeout 7
    AuthXRadiusRetries 2
    require valid-user
</FilesMatch>
Protect wp-admin

<Location "/wordpress/wp-admin/"
Satisfy all
AuthType Basic
AuthBasicProvider xradius
AuthName "Username and WiKID one-time passcode."
AuthXRadiusAddServer "192.168.1.171:1812" "openid_secret"
AuthXRadiusTimeout 7
AuthXRadiusRetries 2
require valid-user
</Location>
Fixing HTTPS

PKI in the browser doesn't really work

TOFU/POP – Trust on First Use/Persistance of Pseudonym

Requires the cooperation of the Browsers, which is not there yet
Prevent MITM attacks with Mutual HTTPS Auth

- In WiKID, add a “Registered URL” to the domain
- The Server will store a hash of the site's SSL cert.
- When the user requests an OTP, the token gets the hash and compares the two
- If OK, it launches the browser to the URL
Pretty Lame Diagram

VPN, SSH, HTTPS Gateway

Desktop, Mail, Web

SSH, RDP, VNC, HTTPS

2FA Server

RADIUS, LDAP, etc

Auth/Radius Server

Desktop, Mail, Web

SSH, RDP, VNC, HTTPS

2FA Server

RADIUS, LDAP, etc

Auth/Radius Server

VPN, SSH, HTTPS Gateway
Join the cause!

• If Info Sec pros aren't leading the way to increased security, who will?
• Static passwords are teh suxxor
• Demand two-factor authentication!
• Contribute!
Any questions?

nowen@wikidsystems.com
@wikidsystems