I Installed a Security Plugin.

Now What?

About Me

- Working in various parts of computer industry for over 25 years.
- GSEC certification
- Part of greynoi.se security podcast.
- Work on security and privacy mostly by avocation.
- scott@geekslv.com
- @smaction

The Why and How of Attacks

- usually automated
- may or may not be a sophisticated attacker
- denial of service
- taking information
- profit
- use to attack some other site

https://

- It allows secure and private communication on the Web.
- needed for many applications and Google says so
- Use Let’s Encrypt.
- Change any passwords that were used before you installed certificate.

Force https://

- When you have https:// setup, make sure it is being used.
- .htaccess commands

```
RewriteEngine On

RewriteCond %{HTTPS} !=on

RewriteRule ^(.*)$ https://%{HTTP_HOST}%{REQUEST_URI} [L,R=301,NE]
```

Backup Plugin

- rules for all plugins apply
- good for things other than security

Logs

- Find out what logs your hosting provider gives access to.
- Check what logs are provided by your security plugin.
- You want logs to go far back as possible.
- If possible store logs on another computer.

Passwords

- long and random
- Use 2FA with passwords.
- app is better than text message
- Use a password manager.

Change the Salt in wp-config.php

- Salt is used in concert with passwords.
- manual
  - https://api.wordpress.org/secret-key/1.1/salt/
- Saltshaker plugin

Change Rights on Key Files and Directories

- In Linux rights are represented by 3 digit hex number such as 755
- find /path/to/your/wordpress/install/ -type d -exec chmod 755 {} \;
- find /path/to/your/wordpress/install/ -type f -exec chmod 644 {} \;

Keep Your Personal Devices Secure

- strong passwords
- especially a laptop that travels with you
- that includes your phone

Get A New Router

- Most router reviews never talk about security.
- If router is more than a couple of years old, the firmware is probably out of date.
- Many people do not change default values.
- Some people use insecure features like WPS.
- Others use combination modem/routers.

What To Do With a New Router

If you are really paranoid, *do the first steps behind another router.* Otherwise, just follow the list.

- Change the default router password.
- Change the default WiFi password(s).
- Use WPA2 with AES.
- Change the default WiFi network name(s).
- Turn off WPS, UPnP, NAT-PMP and Remote Administration.
- Download the latest firmware for the router.
- Turn off any features you are not using.

What To Do With a New Router (2)

- If possible, change the username for your router.
- Your modem may be a router, too.

For the truly paranoid:

Connect the WAN port of a router to be tested to a LAN port on another router (outside router). Then, from a computer connected to the outside router, scan the WAN side of the router to be tested using NMAP to look for open ports.

VPN

- for additional security and privacy
- mostly privacy
- Always use on public WiFi.
- for additional privacy 1.1.1.1

Keep Everything Up to Date

- core Files
- plugins
- your computers and devices, too

Web Application Firewall

- blocks many problems before they get to your site.
- Plugins or CDN might provide this.

Different Accounts for Different Functions

- administration
- posting and editing
- user accounts

CDN

- caches your content on multiple computers in different geographical areas
- helps protect against a DDOS attack
- Some include Web application firewalls.

It Happened

- Don’t panic!
- If you have a backup from before the attack, use it.
- Change all the passwords.
- You may lose limited data.

To avoid data loss or if this didn’t work ...

It’s Still Happening

- Make a fresh backup.
- Change SSH password.
- Change database password.
- Change all WP user passwords.
- Delete and replace all core files.
- Delete and replace all plugins.

Resources

- WordPress Security Announcements
- Facebook WordPress Security Group
- WordPress.org Hardening WordPress
- WordPress.TV/tag/security
- Routersecurity.org
- Nmap.org
- grc.com

Thank You