

Forum:[Hack Forums](#)

Thread: [How does one prevent getting their static HTML/CSS sites hacked/defaced?](#)

Turf - March 28, 2016, 12:14 am

I run a few simple, basic & static HTML/CSS websites. What are the most common & effective methods for ensuring my site doesn't get hacked / defaced / exploited / etc.?

0x7FFDF000 - March 28, 2016, 5:04 am

By purchasing a server (Dedicated / Virtual) thus eliminating shared hosting escalation
And then hardening it (Installing fail2ban, disabling SSH passwords use certs instead, config iptables block troublesome ranges, turn TCP cookies, update all daemons, remain upstream as possible, update kernel & patch kernel with grsec and pax, review at all times what goes in and out of your system with tcpdump and uninstall anything that isn't strictly needed, use chage & faillog, review all inbound logins with shit passwords (empty or otherwise), extensively review SUID/SGID binaries, harden port scanning using tcp wrappers, turn off ipv6 until it's not shit, secure apache remove shit modules install mod_security disable cgi re-write errorpages)

dont look for 'common' methods like idiotically relocating common ports
dont look for 'effective' methods like installing a one-size-fits-all solution like snort which is good on it's own but goes with more things
look for time consuming, quality, research-full methods. Laziness and shortcuts are often exploited themselves. A vulnerability within improperly-placed IPS is an actual way in.

chillingwitha9 - March 28, 2016, 6:32 am

(Mar 28, 2016 05:04 AM)0x7FFDF000 Wrote: [\[CITE\]](#) By purchasing a server (Dedicated / Virtual) thus eliminating shared hosting escalation

And then hardening it (Installing fail2ban, disabling SSH passwords use certs instead, config iptables block troublesome ranges, turn TCP cookies, update all daemons, remain upstream as possible, update kernel & patch kernel with grsec and pax, review at all times what goes in and out of your system with tcpdump and uninstall anything that isn't strictly needed, use chage & faillog, review all inbound logins with shit passwords (empty or otherwise), extensively review SUID/SGID binaries, harden port scanning using tcp wrappers, turn off ipv6 until it's not shit, secure apache remove shit modules install mod_security disable cgi re-write errorpages)

dont look for 'common' methods like idiotically relocating common ports
dont look for 'effective' methods like installing a one-size-fits-all solution like snort which is good on it's own but goes with more things
look for time consuming, quality, research-full methods. Laziness and shortcuts are often exploited themselves. A vulnerability within improperly-placed IPS is an actual way in.
what this guy said..... couldn't agree more

pashabiceps - March 28, 2016, 11:02 am

(Mar 28, 2016 05:04 AM)0x7FFDF000 Wrote: [\[CITE\]](#) By purchasing a server (Dedicated / Virtual) thus eliminating shared hosting escalation

And then hardening it (Installing fail2ban, disabling SSH passwords use certs instead, config iptables block troublesome ranges, turn TCP cookies, update all daemons, remain upstream as possible, update kernel & patch kernel with grsec and pax, review at all times what goes in and out of your system with tcpdump and uninstall anything that isn't strictly needed, use chage & faillog, review all inbound logins with shit passwords (empty or otherwise), extensively review SUID/SGID

binaries, harden port scanning using tcp wrappers, turn off ipv6 until it's not shit, secure apache remove shit modules install mod_security disable cgi re-write errorpages)

dont look for 'common' methods like idiotically relocating common ports
dont look for 'effective' methods like installing a one-size-fits-all solution like snort which is good on it's own but goes with more things
look for time consuming, quality, research-full methods. Laziness and shortcuts are often exploited themselves. A vulnerability within improperly-placed IPS is an actual way in.
That's cool and all, but you forgot to mention that hacking HIM first (who will be much more insecure) would make all that extra security on the server side useless ;)

0x7FFDF000 - March 28, 2016, 11:06 am

(Mar 28, 2016 11:02 AM)pashabiceps Wrote: [\[CITE\]](#) That's cool and all, but you forgot to mention that hacking HIM first (who will be much more insecure) would make all that extra security on the server side useless ;yes, omitted for brevity and my own attention span

pashabiceps - March 28, 2016, 11:10 am

(Mar 28, 2016 11:06 AM)0x7FFDF000 Wrote: [\[CITE\]](#) yes, omitted for brevity and my own attention span

Also checking for capabilities on binaries, not just permissions like SUID/SGID, there are around 18 caps that are equivalent to root, if exploited correctly.

?Criminal - March 28, 2016, 1:05 pm

In this case your theoretical attacker would attempt to take specifically your hosting account and reset the vps/dedis ssh password and log in as root or take the entire hosting company over and reset anyones server at their hearts content depends on their skill level but the general rule of thumb is if its a static site with just pure HTML theres not anything an attacker can do to the web application it self so the user is usually targeted think client side attacks, aside from what 0x7FFDF000 mentioned another thing you can add is IP whitelisting to your box so only specific IP's can SSH into your server. There was this static site generator I saw on reddit netsec awhile back I actually might try it out static blogs are definitely much more secure then running wordpress and roll with the risk of having someone pop a shell I remember the first time I ran wordpress awhile ago I was seeing chinese ip ranges in the access_logs doing automated brute attacks so theres definitely a risk there but of course with a proper hardened set up even bots bruting you shouldn't matter but most people run vanilla installs these days. Oh yeah one last thing I wanted to add theres usually no point to target a static site in the first place aside from I guess defacing it to attention whore OR if you run web apps on the same box they can probably check insertuserdirectorynamehere/domains/ and check for config files with SQL creds and dump dbs from sites that contain actual user data but aside from that can't see a valid reason why you'd be targeted.

Frosteh - March 30, 2016, 12:44 am

If you have a purely static content site which does not take user input in any form then you're not going to have any webapp vulnerabilities.

However the below information is good general security practice stuff for hardening hosting. I would also add to this that you use a good domain provider and hosting provider which ideally provides you with 2 factor authentication so no one can one shot your site by grabbing a single super admin password.

Consider limiting remote access via SSH to specific IPs if possible or wrap the whole thing in a VPN so you need to auth onto a VPN LAN before getting access to any of the non-web ports on the box for management.

All security practices you use for hardening the server itself you also want to consider doing for the computers that remotely connect to manage it, any computer given access. Any saved credentials on those computers become targets just as valuable as the webserver itself.

Security is always best in layers so failure in one layer doesn't lead to popping the server.

(Mar 28, 2016 05:04 AM)0x7FFDF000 Wrote: [\[CITE\]](#) By purchasing a server (Dedicated / Virtual) thus eliminating shared hosting escalation

And then hardening it (Installing fail2ban, disabling SSH passwords use certs instead, config iptables block troublesome ranges, turn TCP cookies, update all daemons, remain upstream as possible, update kernel & patch kernel with grsec and pax, review at all times what goes in and out of your system with tcpdump and uninstall anything that isn't strictly needed, use chage & faillog, review all inbound logins with shit passwords (empty or otherwise), extensively review SUID/SGID binaries, harden port scanning using tcp wrappers, turn off ipv6 until it's not shit, secure apache remove shit modules install mod_security disable cgi re-write errorpages)

dont look for 'common' methods like idiotically relocating common ports

dont look for 'effective' methods like installing a one-size-fits-all solution like snort which is good on it's own but goes with more things

look for time consuming, quality, research-full methods. Laziness and shortcuts are often exploited themselves. A vulnerability within improperly-placed IPS is an actual way in.

DjHaxorz - March 31, 2016, 11:14 am

Use a linux distro, such as SUN OS, and host your server from there. That-a-way, all of the tricks used to exploit vulnerabilities will be completely incompatible with your OS without the user knowing.

ImHeyo - March 31, 2016, 12:18 pm

(Mar 28, 2016 05:04 AM)0x7FFDF000 Wrote: [\[CITE\]](#) By purchasing a server (Dedicated / Virtual) thus eliminating shared hosting escalation

And then hardening it (Installing fail2ban, disabling SSH passwords use certs instead, config iptables block troublesome ranges, turn TCP cookies, update all daemons, remain upstream as possible, update kernel & patch kernel with grsec and pax, review at all times what goes in and out of your system with tcpdump and uninstall anything that isn't strictly needed, use chage & faillog, review all inbound logins with shit passwords (empty or otherwise), extensively review SUID/SGID binaries, harden port scanning using tcp wrappers, turn off ipv6 until it's not shit, secure apache remove shit modules install mod_security disable cgi re-write errorpages)

dont look for 'common' methods like idiotically relocating common ports

dont look for 'effective' methods like installing a one-size-fits-all solution like snort which is good on it's own but goes with more things

look for time consuming, quality, research-full methods. Laziness and shortcuts are often exploited themselves. A vulnerability within improperly-placed IPS is an actual way in.

Lel do all what he said and you're done.

Also if you're using a CMS make sure it's up to date, i've pwned many wordpress sites that had very old versions ...

pashabiceps - March 31, 2016, 2:31 pm

(Mar 31, 2016 11:14 AM)DjHaxorz Wrote: [\[CITE\]](#) Use a linux distro, such as SUN OS, and host your server from there. That-a-way, all of the tricks used to exploit vulnerabilities will be completely incompatible with your OS without the user knowing.

I seriously hope you're joking :)

