Security: Kali Linux Forensics Tools, SSH Primer and ?Yelp, but for MAGA? Mad About Holes

By *Roy Schestowitz*
Created *15/03/2019 - 2:48am*
Submitted by Roy Schestowitz on Friday 15th of March 2019 02:48:32 AM Filed under Security [1]

- **Kali Linux Forensics Tools [2]**

  Kali Linux is a powerful Operating system especially designed for Penetration Tester and Security Professionals. Most of its features and tools are made for security researchers and pentesters but it has a separate ?Forensics? tab and a separate ?Forensics? mode for Forensics Investigators.
  Forensics is becoming very important in Cyber Security to detect and backtrack Black Hat Criminals. It is essential to remove Hackers? malicious backdoors/malwares and trace them back to avoid any possible future incidents. In Kali?s Forensics mode, Operating System doesn?t mount any partition from System?s hard drive and doesn?t leave any changes or fingerprints on host?s system.

  Kali Linux comes with pre-installed popular forensics applications and toolkits. Here we?ll review some famous open source tools present in Kali Linux.

- **What is SSH (Secure shell protocol)? [3]**

  SSH stands for Secure Shell which is a security protocol based on the application layer. We use the SSH to securely access the remote servers and Desktops to execute various commands. In short, we can control the complete system remotely, if we have login information and SSH server access. Because The Secure Shell (SSH) is a cryptographic network protocol designed to replace the Telnet and access the remote system even on the unsecured remote shell by encrypting data before sending.

- **Security Researcher Discovers Flaws In Yelp-For-MAGAs App, Developer Threatens To Report Him To The Deep State[4]**

  Even a cursory look at past stories we've done about how companies treat security researchers who point out the trash-state of their products would reveal that entirely too many people and companies seem to think shooting the messenger is the best response. I have never understood the impulse to take people who are essentially stress-testing your software for free, ultimately pointing out how the product could be safer than it is, and then threatening those people with legal action or law enforcement. But, then, much of the world makes little sense to me.

  Such as why a Yelp-for-MAGA people should ever be a thing. But it absolutely is a thing, with conservative news site 63red.com releasing a mobile app that is essentially a Yelp-clone, but with the twist that its chief purpose is to let other Trump supporters know how likely they are to be derided when visiting a restaurant. This is an understandable impulse, I suppose, given the nature of politics in 2019 America, though the need for an app seems like overkill. Regardless, the app was released and a security researcher found roughly all the security holes in it.

- **?Yelp, but for MAGA? turns red over security disclosure, threatens researcher[5]**

  But the safe space for 63red founder Scott Wallace was violated quickly when French security researcher Elliot Alderson discovered some fundamental security flaws in Safe's architecture?making it not so safe.

  Because the application is build in React Native, a JavaScript- and JSX-based scripting language that basically turns Web apps into "native" Apple iOS and Android applications, the entire architecture of the application is available to anyone who downloads and unpacks it. And in that code, Alderson discovered a few things: [...]

Security

Source URL: http://www.tuxmachines.org/node/121723

Links:
[1] http://www.tuxmachines.org/taxonomy/term/59
[2] https://linuxhint.com/kali_linux_forensics_tools/
[3] https://www.how2shout.com/what-is/what-is-ssh-secure-shell-protocol.html
[4] https://www.techdirt.com/articles/20190314/10143841796/security-researcher-discovers-flaws-yelp-for-magas-app-developer-threatens-to-report-him-to-deep-state.shtml
[5] https://arstechnica.com/information-technology/2019/03/yelp-but-for-maga-turns-red-over-security-disclosure-threatens-researcher/