Sysadministrivia

Linux, Lagers, and Late Nights

S1E9: "I Can Smell You (and You Smell Horrible)"

Posted 2016-06-21 13:04
Modified 2017-02-11 18:39
Comments 0

Navigation

Previous Episode	Next Episode
S1E8: "On the Origin of Processes"	S1E10: "(F|H)ired!"

Log

Recorded (UTC)	Aired (UTC)	Editor
2016-06-09 03:06:18	2016-06-21 13:04:00	aaron k.

Verification

Format	SHA256	GPG	Audio File
MP3	`433146155ce4149af6f425785a316908f4f471ab90612c7455ec4bfe2ebc0af0`	click	click
OGG	`091ff24f08cde9bf5bc21310b7dccab117fbed481afaa4e8ba39610d3c735b10`	click	click

Quicklisten:

“Everyday OPSEC” (operations security), packet sniffing, and a neat trick to hide pentesting equipment.

- News
- Notes
- Sysbadministration Award
- Errata
- Music

News

Starts at **6m00s**.

- (During intro) There is apparently a Twitter database dump from a compromise, and apparently there is a large amount of celebrity accounts reporting compromised. Apparently, however, it is pretty old.
- CentOS 6.8 was released.
- A Florida man was caught jamming mobile signal.
  - The FCC totally manhandled him. Protip: don’t mess around with FCC affairs.
- The US military still uses 8” floppies for some functionality.
- The FOSSCON 2016 CFP is open
  - Registration and other info is available here.
- The LinkedIn database leak is available.
  - Always be careful when popping various personal information on compromise-checkers, but you may find this handy.
  - This is also handy.
  - If you want to try getting into password cracking, the dumps can (at the time of episode release) can be found via several links mentioned here. It’s also available via a magnet link.
- A dog charity org has paid the ransom to a ransomware, at a haggled price.
- (Mentioned during Discussion) Paden mentions this (which are SUPPOSEDLY used in civil forfeitures- keep reading). Important to note is in the 5th and 14th Amendments, the government shall not deprive anyone of “life, liberty, or property, without due process of law…”- an exception to this is civil forfeiture, which I mention, but that can only be valid in the case where the monies, property, etc. being seized is suspect of being evidence/involved in a crime.

Notes

Starts at **12m08s**.

I was drinking the same rum as before. Jthan was drinking a Dry Dock Apricot Blonde. Paden sung praises about Matilda.

- Good OPSEC for the everyday Joe (“Going Dark”)
  - I’m fairly certain the HOPE talk I reference is this one. It’s 3 hrs though- if someone wants to watch through and find the time he discusses this, let me know!

- In addition to Tor, I mention:
  - I2P
  - Lantern
  - cjdns (and related, the Hyperboria network)

- Packet sniffing! **(24m20)**
  - We fail to mention this early enough, but **WE DO NOT CONDONE ATTACKING NETWORKS YOU DO NOT OWN OR DO NOT HAVE PROPER AUTHORIZATION TO PERFORM THESE ACTIONS ON**.
  - Jthan mentions using Python to do packet sniffing. I also mention Scapy (but that is moreso used for packet creation, manipulation, etc.)
  - When we talk about sniffing SIP packets, I mention a STUN server/proxy.
  - Paden also mentions reassembling SIP in Wireshark.
  - Port mirroring is generally considered the “appropriate” way of sniffing traffic if using it for “legitimate” purposes (i.e. debugging network issues).
  - I mention tcpreplay, and Wireshark, and my personal favourite for capturing packet dumps: tcpdump.
  - Passive sniffing tends to be used by tools like p0f, in which your machine can simply listen to packets being broadcasted on the network and identifying hosts etc. without throwing up any red flags on any NIDS (Network Intrusion Detection System) or NIPS (Network Intrusion Prevention System).
  - For bluetooth, there’s some pretty awesome bluesnarfing tools.
  - You can sniff Zigbee…
  - and EDGE/GSM…
  - and run your own spoofed (or legitimate for in-house use) mobile carrier.
  - Possible mitigation:
    - Turn off ANY connection (bluetooth, ethernet port, NFC chip, Wi-Fi card, etc.) not being used.
    - RFID can be blocked by various technology.
    - As Paden brings up, the only real protection/mitigation you can have is **persistently examining** your network and technicians. Yes, that means physically- with your eyes and feet. Because these things (and these, and these, these, these…) exist.
    - I can’t seem to find the Deviant Ollam talk I reference about incentivizing higher vigilance with monetary reward. If anyone knows where to find it, let me know! I can’t seem to remember the title.

- A woman in China uses 3D-printed heels to hide pentesting gear **(48m34s)**
  - You can find a write-up here, but the really interesting thing is this Reddit thread where she answers a lot of technical questions as to the design of the shoes- her posts are pretty interesting/informative as well. You can find a series of photos showing off the scheme here.

Sysbadministration Award

In this segment, we highlight system administration mistakes. Think of them as the IT equivalent of the Darwin Awards. **(52m37s)**

There was a ransomware fail in which the victim toasted three of their backups- because they hooked them up to the running infected system.

Errata

- Jthan is wrong (starting 55m26s)- he absolutely said that someone shouldn’t be mocked for their use of a language not natively their own. See S1E5. The conversation thread starts at 11m37s, and the important parts are 13m00s, 14m24s, and especially lulzy starting at 15m18s. So much for being “open-minded”, Jthan. :P

Music

Music Credits

Track	Title	Artist	Link	Copyright/License
Intro	Secrets to Yourself	WJLP	click	CC-BY-NC 3.0
Outro	Mellow Acid	CyberSDF	click	CC-BY 3.0

(All music is royalty-free, properly licensed for use, used under fair use, or public domain.)

Author r00t^2
Categories Season One

Comments

There are currently no comments on this article.