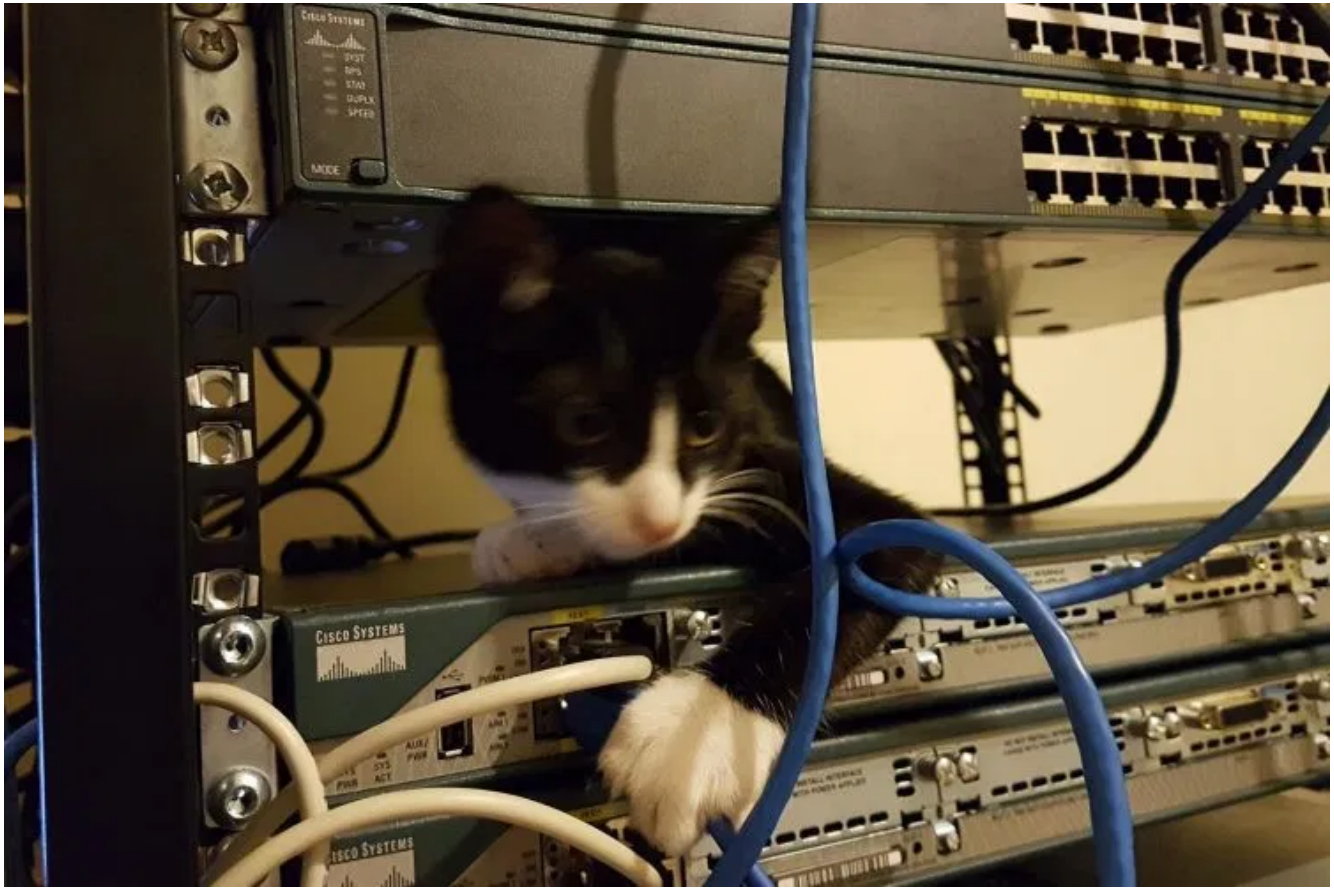
So Long, and Thanks for All the Fish

JUST SOME RANDOM THOUGHTS ABOUT THE MEANING OF LIFE, THE UNIVERSE, AND EVERYTHING

MENU



NetCat attack (CVE-2019-11184): steal encrypted SSH keystrokes exploiting DDIO

RECENT POSTS

Win32/StealthFalcon malware uses Windows Background Intelligent Transfer Service (BITS) to communicates to its C&C servers

September 13, 2019

Simjacker: a brand new mobile vulnerability exploited by surveillance companies for espionage operation

September 12, 2019

Some thoughts about Browser Fingerprinting

September 12, 2019

NetCat attack (CVE-2019-11184): steal encrypted SSH keystrokes exploiting DDIO

September 11, 2019

Written by Andrea Fortuna • on September 11, 2019 • in Cybersecurity

Intel chipset can be exploited to sniff SSH passwords as they're typed over the network.

In 2011, Intel introduced a feature called Data-Direct I/O (DDIO) its server processors that allowed network cards and other peripherals to connect directly to a CPU's last-level cache, increasing input/output bandwidth and reducing latency and power consumption.

> *Data-Direct I/O (DDIO) is a performance-enhancing technology on recent Intel server-grade processors. Instead of reading/writing from/to slow memory, DDIO allows peripherals to read/write from/to the fast (last-level) cache. DDIO was specifically introduced to improve the performance of server applications in fast networks.*

Researchers from the **Vrije Universiteit Amsterdam** and **ETH Zurich** **discovered** that attackers can abuse DDIO to obtain keystrokes and other types of sensitive data that flow through the memory of vulnerable servers, especially in data centers and cloud environments that have both DDIO and remote direct memory access enabled to allow servers to exchange data: for example a server leased by a malicious hacker could abuse the vulnerability to attack other customers on.

CATEGORIES

Select Category

RECENT COMMENTS

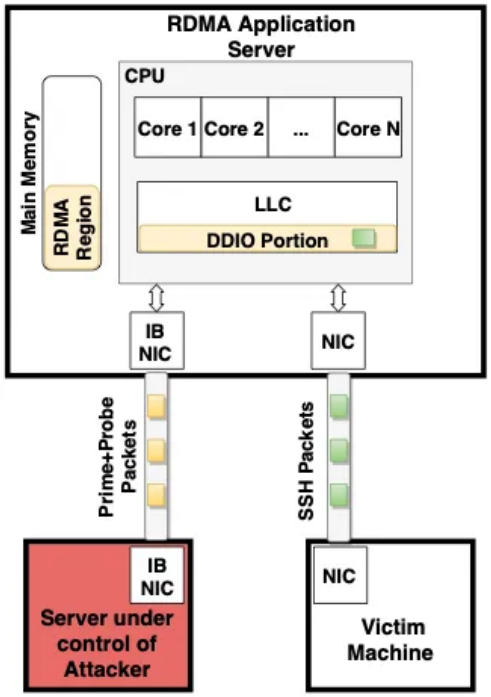
Cybersecurity: DNS Tunneling – Elite Homework on DNS tunneling techniques in cyberattacks

simjacker, anda bisa dimata-matai hanya dengan modal kartu sim - High3 Blog on Simjacker: a brand new mobile vulnerability exploited by surveillance companies for espionage operation

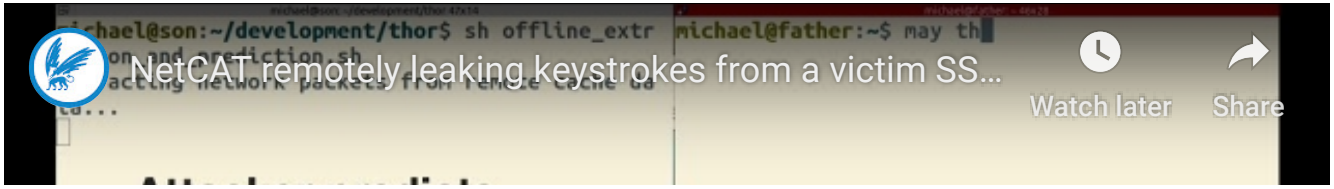
Andrea Fortuna on How to make a "Ultra-Geek" Linux Workstation

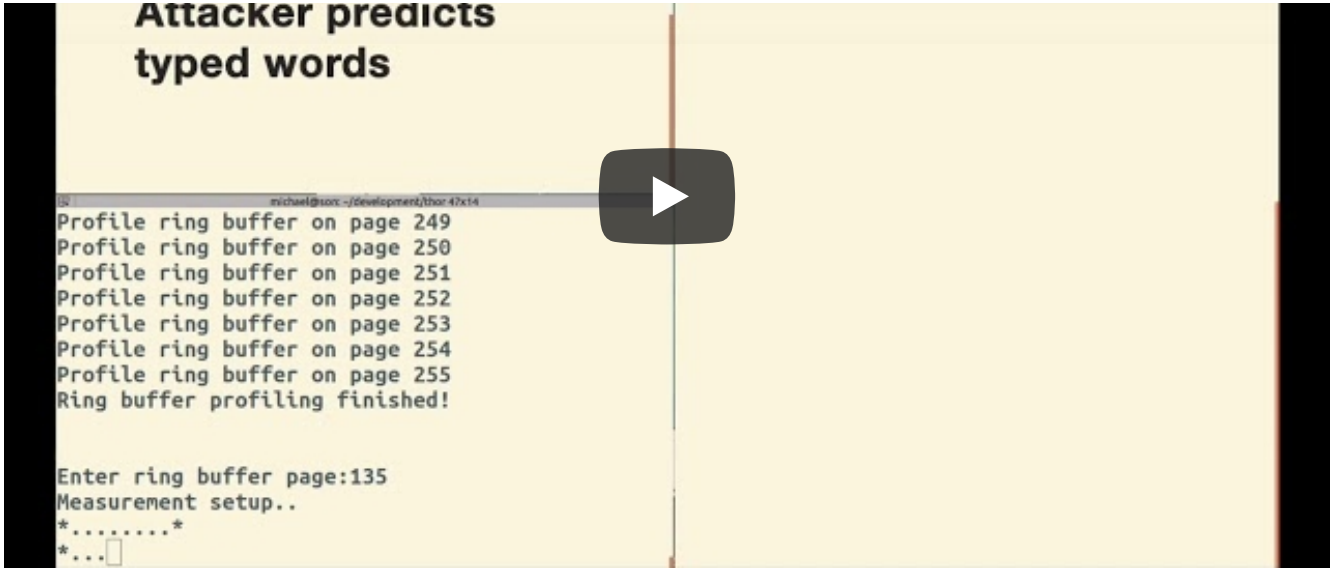
Juan on How to make a "Ultra-Geek" Linux Workstation

> *In our attack, we exploit the fact that the DDIO-enabled application server has a shared resource (the last-level cache) between the CPU cores and the network card. We reverse engineered important properties of DDIO to understand how the cache is shared with DDIO. We then use this knowledge to leak sensitive information from the cache of the application server using a cache side-channel attack over the network. To simplify the attack, similar in spirit to* ***Throwhammer****, we rely on Remote Direct Memory Access (RDMA) technology. RDMA allows our exploit to surgically control the relative memory location of network packets on the target server.*



Process Injection Teknikleri - Process Hollowing ve Atombombing - Manalysiz on RunPE: a practical example of Process Hollowing technique





> *The attacker controls a machine which communicates over **RDMA** to an application server that supports DDIO and also services network requests from a victim client. **NetCAT** shows that attackers can successfully spy on remote server-side peripherals such as network cards to leak victim data over the network.*
>
> ***https://www.vusec.net/projects/netcat/***

References

- https://www.vusec.net/projects/netcat/

Related posts

Share this:

Like this:

Loading...

TAGS

CYBERSECURITY INTEL VULNERABILITY

PRINT

Andrea Fortuna

CVE-2019-15846 - Seriously? Another RCE in Exim?

COMMENTS

Enter your comment here...

This site uses Akismet to reduce spam. Learn how your comment data is processed.