Global Scientific JOURNALS

GSJ: Volume 9, Issue 11, November 2021, Online: ISSN 2320-9186
www.globalscientificjournal.com

Various New Domains in the Field of Technology

G. Anandhi[1] and M Nawaz Brohi*
[1]*Senior Facilitator*
Regenesys Business School, Navi Mumbai
giri_anandhi@hotmail.com
*Department of Creative Computing
Bath Spa University, Academic Center
Rak-UAE
mnbrohi@bathspa.ae

*Corresponding author: M Nawaz Brohi, Department of Creative Computing, University of Bath Spa Academic Center, Ras Al Khaimah-United Arab Emirates. mnbrohi@bathspa.ae 00971504229890.

Abstract - This current period can be termed as the advanced stage in the Information technology. IT is becoming a big change agent in different aspect of business and society. Information Technology tools are definitely a catalyst in resolving economic and social issues. The World is becoming technically advanced, markets are stronger, and new technologies are emerging at an astronomical pace. The backbone of these technological advances are the seamless connectivity. The digital transformation continues, to build a more interconnected society. The data is shared and used by more platforms than ever – in the datacenter, on the cloud and on internet of things (IoT) devices and this would increase in the future. However, benefit comes with a cost. The topic of discussion is on the data susceptibility due to the seamless connectivity.

Keywords: Bit Cracker**,** Tracer, Osquery, CimSweep, Skydive, Nscan, Detours, OPNsense, osquer, Diario.

I. Introduction

Cyber Security is the protection of computer systems and networks from information leakage, theft or damage to their hardware, software, or data. Computer forensic refers to digital forensic which is the fusion of network forensics, internet forensics, social media forensics.

Machine and application virtualization technologies are the focus of attention.

The transformation from traditional services towards various cloud services has its underlying drawbacks. The benefits of virtualization and data storage. The security issues that come with the advantages should not however be ignored. Of course, virtualization is an advantage for consumers because security is one of the features that are taken care to lesser extent. A key feature of virtualization is live migration (LM) that allows transfer of virtual machine from one physical server to another without interrupting the services running in virtual machine. Live migration facilitates workload balancing, fault tolerance, online system maintenance, consolidation of virtual machines etc.

The technical field is becoming smarter, due to the support on computer systems, the Internet and wireless network standards such as Bluetooth and Wi-Fi, and due to the growth of "smart" devices, including smartphones, televisions, and the various devices that constitute the "Internet of things". In this regards it is noteworthy to discuss the tools that are highly used in the domain.

II. Facts of Latest introduced techniques

A. Open-Source Firewall: OPNsense

This is an easy-to-use and easy-to-build FreeBSD based firewall and routing platform. It includes most of the features that are available in expensive commercial firewalls. It brings rich set of commercial offerings with the benefits of open and verifiable sources.

B. Offline Digital Forensics Tool for Binary Files

This tool is used for offline digital forensics and malware analysis as it shows all raw bytes of a file and ASCII representations. It can be used on different file types, TXT, PNG, Compiled C code and also for a packet capture file. It has three columns: one to show the byte count on the far left, in the middle the hexadecimal bytes of the file and on the right the ASCII representations of the of the hexadecimal bytes.

Bit Cracker is the first open course BitLocker password cracking tool. It has a full-disk encryption feature available in recent Windows versions (Vista 7, 8.1 and 10) Pro and Enterprise. It is a mono-GPU password cracking tool for memory units encrypted with the password authentication mode of BitLocker.

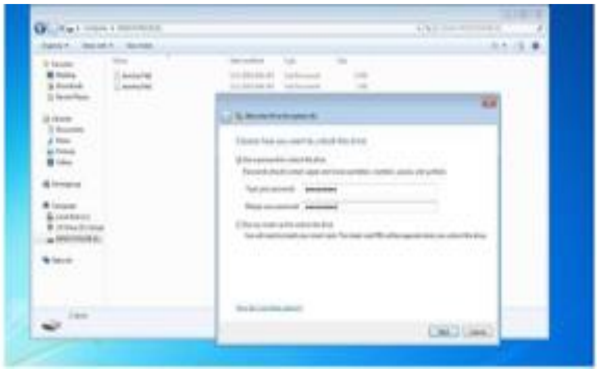

Figure 1: Bit Cracker structure

Tracer is an open-source GPS tracking system for various GPS tracking devices. This Maven project is written in Java and works on most platforms with installed Java Runtime Environment. This supports more than 80 communication protocols from popular vendors. It includes web interface to manage tracking devices online. It is the best free and open-source GPS tracking system software that offers self-hosting real time online vehicle fleet management and personal tracking.

Fern Wi-Fi Cracker is a wireless security auditing and attack software program written using Python language and Python Qt GUI library. This program is able to crack and recover WEP/WPA/WPS keys and also run-on other network-based attacks on wireless or Ethernet based networks.

C. Big Game Hunting

Ransomware attacks are defined by a new strategy called ’big game hunting’. This targets larger organizations with a low tolerance for down-time like manufacturing, healthcare and government firms. This ransomware group invests time and effort in researching targets to access potential return on investment of a campaign. This has innovated new methods on targets to pay ‘double extortion’ schemes which combine IT system ransoms with additional threat to publish an organization’s confidential information online if payment is not forthcoming.

D. OS Instrumentation Framework

Osquery exposes an operating system as a high-performance relational database. This allows to write SQL-based queries to explore operating system data. With osquery, SQL tables represent abstract concepts such as running processes, loaded kernel modules, open network connections, browser plugins, hardware events or file hashes.

E. Android Security Virtual Machine

AndroidL4b is based on ubuntu-mate that includes the collection of latest frameworks, tutorials and labs from different security geeks and researchers for reverse engineering and malware analysis. The tools directory contains tools and frameworks. Labs, documents and source codes are in the lab’s directory.

Detours is a software package for monitoring and instrumenting API calls on Windows. Detours has been used by many ISVs and is also used by product teams at Microsoft.

F. Windows Remote Incident Response

CimSweep is a suite of CIM/WMI-based tools that enable the ability to perform incident response and hunting operations remotely across all versions of Windows. This may also be used to engage in offensive reconnaissance without the need to drop any payload to disk. Windows Management instrumentation has been installed and its respective service running by default since Windows XP and Windows 2000 and is supported in the latest versions of Windows including Windows 10, Nano Server and Server 2016. Agent-based defensive tools are extremely powerful but require deployment of the agent to each system. Agent-based solutions are expensive and not foolproof it can be detected by determined attackers. This enables the acquisition of time-sensitive data without the need of an agent to deploy it.

G. Open-Source Real Time Network Topology and Protocols Analyzer

Skydive aims to provide a comprehensive way of understanding what is happening in the network infrastructure. Its agents collect topology information and flows and forward them to a central agent for further analysis. All the information is stored in an Elastic search database. This is SDN-agnostic but provides SDN drivers in order to enhance the topology and flows information. Currently only Neutron driver is provided. The topology probes currently implemented are: OVSDB, Net LINK, NetNS, and Ethtool. The flow probe currently implemented is slow.

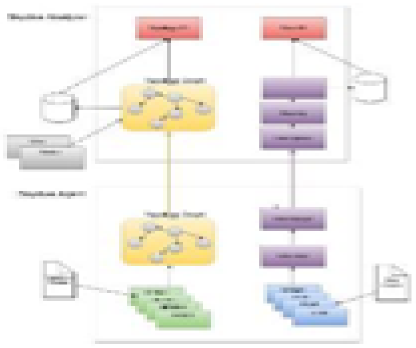

Figure 2: Architecture of Open-Source Real Time Network Topology and Protocols Analyzer

Bro is an open-source network traffic analyzer. It is primarily a security monitor that inspects all traffic on a link in depth for signs of suspicious activity. Bro supports a wide range of traffic analysis tasks outside of security domain including performance measurements and helps with troubleshooting. The benefit that the site gets from deploying Bro is a set of log files that record a network's activity in high-level terms. These logs include not only record of the connection in the wire, but also application layer transcripts such as HTTP sections with their requested URIs, key headers, MIME sessions and server responses, DNS requests with their replies, SSL certificates, key content of SMTP sessions and much more. Bro writes all the information into well-structured tab-separated log files suitable for post processing with external software. Users can choose from a set of alternative output formats and back ends to interface directly with external databases. In addition to logs, Bro comes with built-in functionality for a range of analysis and detection tasks, including extracting files from HTTP sessions, detecting malware by interfacing to external registries, reporting vulnerable versions of software seen on the network, identifying popular web applications, detecting SSH brute-forcing, validating SSL certificate chains and much more.

III. A package for capturing and analyzing network flow data and intra flow data for network research, forensics and security monitoring

Joy is a BSD-licensed libpcap based software package for extracting data features from live network traffic or packet capture (pcap) files, using a flow-oriented model similar to that of IPFIX or Net flow, and representing those data features in JSON. It contains analysis tools that can be applied to these data files. It can be used to explore data at scale, especially security and threat relevant data. It is used in order to make the output easily consumable by data analysis tools. The JSON output files are verbose, reasonably small and respond to compression. This can be configured to obtain intra flow data, (ie) data and information about events that occur within the network flow including:

- The sequence of lengths and arrival times of IP packets up to configurable number of packets.
- The empirical probability distribution of the bytes within the data portion of a flow, and the entropy derived from the value.
- The sequence of lengths and arrival times of TLS records.
- Other non-encrypted TLS data such as the list of offered cipher suites, the selected cipher suite and the length of the client Key Exchange field.
- The name of the process associated with the flow, for flows originate or terminate on the host on which pcap is running.

IV. Nscan: Fast Internet wide scanner

Nscan is a fast Network scanner optimized for internet wide scanning purposes and inspired by Masscan and Zmap. It has its own tiny TCP/IP stack and uses Raw sockes to send TCP SYN probes. It does not need to set SYN Cookies so it does not waste time checking is a received packet is a result of its own scan. This makes Nscan faster than other similar scanners. This has a feature that allows to extend the scan by chaining found ip:port to another script where they might check for vulnerabilities, exploit targets, look for Proxies/VPNs.

Diario is a tool developed by 11 paths that focuses on scanning and analyzing office documents in a static maintaining the privacy of the content of user documents. It does not process or store the private content of the document. It treats the structure and characteristics to detect malicious code inside it. From GINSEG we can access and analyze the tool.

Conclusion

With limitless emerging technologies, all possessing their own positive and negative characteristics, it is impossible to monitor them all. Technology, in the past century has taken an explosive leap into society as a whole, engulfing our lives and organizations. Such technologies as machines for assembly lines, computers and of course just recently high-speed internet connections.

References:

1. Lee, B. W.-M. (2012). Android Application Development Cookbook. In Android Application Development Cookbook: 93 Recipes for Building Winning Apps. Indiana: John Wiley & Sons, Inc
2. Accenture, Ninth Annual Cost of Cybercrime Study, 2019
3. Android Architecture 2019[R/OL]. http://www.cnmsdn.com/html/201003/1268713218ID2058_2 .html
4. http://www.usnews.com/opinion/blogs/world-report/2013/01/14/estonia-shows-how-to-build-a-defense-against-cyberwarfare
5. A Cybersecurity Agenda for the 45th President. (2017, January 5).
6. Z.A. Baig, P. Szewczyk, C. Valli, P. Rabadia, P. Hannay, M. Chernyshev, M. Johnstone, P. Kerai, A. Ibrahim, K. Sansurooah, et al., Future challenges for smart cities: Cyber-security and digital forensics, Digital Investigation 22 (2017) 3–13.
7. Carlini, J. (2017, August 6). Geneva Convention in Cyberwarfare?
8. Kumar, N.A. 2018. Collateral learning of mobile computing: an experience report. In Proceedings of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education (pp. 27-32). ACM. https://doi.org/10.1145/3197091.3197106
9. MacDermott, A., Baker, T. and Shi, Q. (2018) 'Iot Forensics: Challenges for the Ioa Era', in 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), pp. 1–5
10. Rücker, T. M., Pinkwart, N. 2018. "How else should it work?" A grounded theory of pre-college students‟ understanding of computing devices. ACM Transactions on Computing Education (TOCE), 19(1), 1-23. https://doi.org/10.1145/3226592