SANS TECHNOLOGY INSTITUTE

RESEARCH REVIEW JOURNAL

Volume 3

Published Cybersecurity Research From SANS.edu Graduate Students

sans.edu/research

SANS TECHNOLOGY INSTITUTE

SCIENTIA PRO PACE

Ed Skoudis

President, SANS Technology Institute

"One of the vital roles that higher education institutions play in our world is research — that is, advancing the state of human knowledge to unlock new capabilities and insights. I am proud to say that the SANS Technology Institute college, through our students and their advisors, is no slouch when it comes to advancing the state of the art of cyber security through research. In fact, our student's research, as embodied in this journal, is a great manifestation of the SANS Promise: *Everyone who completes SANS training can apply the skills and knowledge they've learned the day they return to work.* In their research captured in these pages, our students are building on what they've learned in class, extending those ideas in a very practical hands-on way, and sharing those new insights to make the world a safer, more secure place. I hope you enjoy and learn from them as much as I do!"

Dr. Johannes Ullrich

Dean of Research, SANS Technology Institute
SANS Faculty Fellow

"Conducting academic research teaches students a very deliberate problem solving methodology. This skill is often overlooked when opinions and influencer "hot takes" are substituted for carefully designed experiments and data. It allows students to have fun with a topic of their choice. They are diving into the issue and contributing to the development of the field. Practical applied research does not just help our students, but it helps all of us make better decisions. I hope you will find this research journal helpful, and please let me know what worked or didn't work for you."

TABLE OF CONTENTS

Cyber Defense

Penetration Testing and Red Teaming

Cloud Security

Industrial Control Systems Security

Security Awareness, Management, and Insights

DETECTING AND MITIGATING THE GATEKEEPER USER OVERRIDE ON MACOS IN AN ENTERPRISE ENVIRONMENT

BY ANTONIO PIAZZA

For red teamers, social engineering a macOS user into executing an application is a common way to gain code execution on a remote macOS client machine. Apple's development of their macOS built-in security mechanism, GateKeeper, has made this a more difficult task, but not impossible. It is effortless for a macOS user to bypass GateKeeper by simply right-clicking to execute a potentially malicious application. An adversary can convince the user to override GateKeeper in this manner and gain remote code execution on the user's system. In fact, many adversaries have done just that. This could lead to further exploitation of a corporate network, so quickly detecting this user activity is essential. While this is a crucial detection, endpoint security products seem to lack the capability. This research explores the detection possibilities for the GateKeeper user override. Developing a GateKeeper detection will allow corporate security teams to protect their environments from users being socially engineered into executing malware. This is an essential step in increasing the defenses of our macOS corporate environments.

Read the research: www.sans.org/u/1oLQ

Figure 15 - GateKeeper Breadcrumb: Adding Vs. Clearing

"Antonio, like others in the community, realize that there has always been a gap in the detection and mitigation tools when it comes to enterprises that utilize MacOS workstations. While MacOS implements some protection against the installation of untrusted applications, the override mechanism is widely known and utilized by individuals. His research illustrates detection opportunities, which are present before possible malicious applications are installed and later executed, providing a better way for security professionals to safeguard users and network resources, if applied at the enterprise level." – **LEE CROGNALE, FACULTY RESEARCH ADVISOR**

DOPPELGÄNGERS: FINDING JOB SCAMMERS WHO STEAL BRAND IDENTITIES

BY ASHLEY TAYLOR

Fraud is on the rise and occurs in many forms. A growing number of criminals are impersonating real companies to trick job seekers into handing over their personal information or money. These impersonated companies face risks in terms of damage to their brand identity. What can companies do to protect their brand against fraud? Information security teams often have the tools to help find impersonation fraud before it becomes a problem. Using threat intelligence and a security orchestration, automation, and response (SOAR) platform, suspicious similar domains were found, intelligence about those domains gathered, and the evidence presented to information security teams to make informed decisions on whether to block the domain. Automation reduced the time it took information security analysts to respond to similar domain alerts. Guidance is given to turn this data into an actionable program to begin building brand identity protections into any security program.

Read the research: www.sans.org/u/1oME

Figure 10. Suspicious domain name is checked against the block list and returns a Boolean value.

AUTOMATING RMF STEPS USING LIGHTWEIGHT SCRIPTS AND TOOLS

BY BRETT FRY

Many Risk Management Framework (RMF) steps and sub-tasks can be accomplished using small, lightweight tools and scripting. Only specific administrative tasks can be automated or inherited in Enterprise Mission Assurance Support Service (eMASS). This constraint results in many government organizations using different tools, creating their own standards, and often buying costly tools to capture all the information needed. This research will explore the many tools and techniques that can be leveraged to accomplish these steps and tasks using a set of scripts that focuses on efficiency and repeatability. Since RMF is not strictly a framework the United States government uses, this research will benefit the community by providing tools and techniques to generate specific information required for implementing the RMF process or data collection activities.

Read the research: www.sans.org/u/1oLB

Figure 2

Prepare04_netstat.bat Output

Protocol	Local Address	Foreign Address	State	Process ID
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	1016
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:903	0.0.0.0:0	LISTENING	4980

Figure 3

Prepare04_processes.sh Output

UID	PID	PPID	CMD
root	1	0	/sbin/init
root	2	0	[kthreadd]

HUMAN INTERFACE DEVICE FIREWALL FEASIBILITY

BY BRIAN DAVIDSON

The Human Interface Device Firewall (HID-F) will make the BadUSB attack far more challenging to succeed while avoiding privacy intrusion by using machine learning models paired with homomorphic encryption. Exploring the flaws of current BadUSB defenses will develop a series of design principles that the HID-F must follow to avoid the same pitfalls. Exploring essential features of an HID-F with research code and public code samples shows that an HID-F is a feasible new class of defensive cybersecurity applications.

Read the research: www.sans.org/u/1oMp

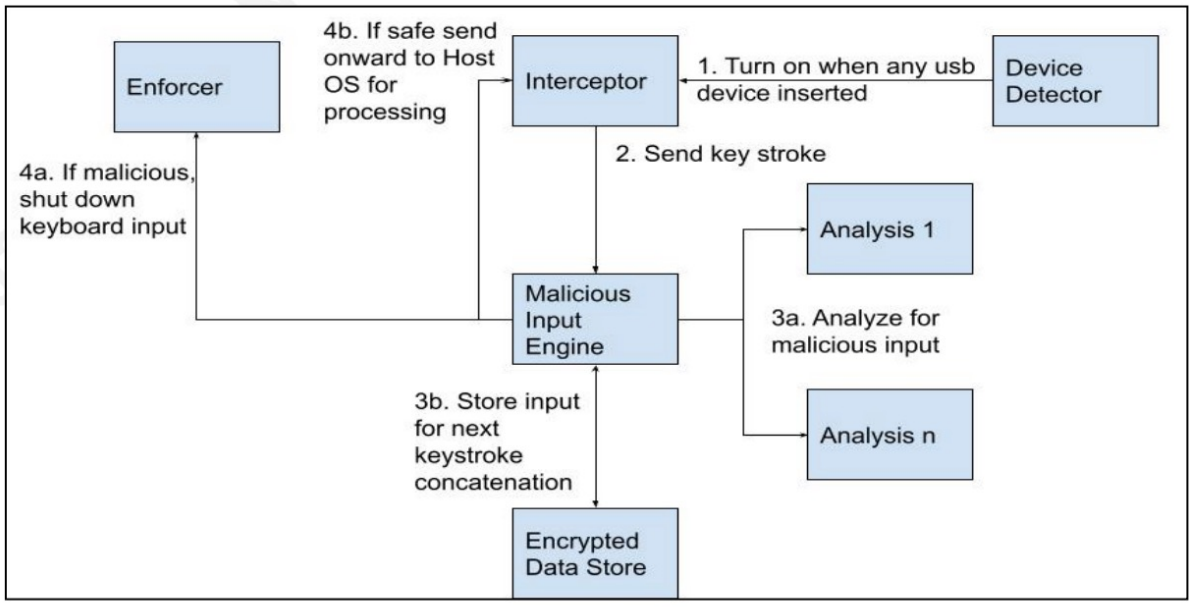


Figure 1. Human Interface Device Firewall

NO-BUDGET LIVING-OFF-THE-LAND DETECTION

BY MOSTAFA ALY

Adversaries face challenges in executing tools that give them the first entry point into an endpoint; hence they started to increasingly adopt the Living-Off-the-Land (LoL) techniques. The execution of Living off the Land techniques usually goes undetected by traditional endpoint defenses because the files used are part of the Windows Operating System, digitally signed by Microsoft. Moreover, these binaries are vital for the Windows Operating System to operate. More organizations started to depend on Windows Security Event Logging to detect such techniques. This paper explores the detection capabilities of Windows Security Event Logging in addition to PowerShell logging and Microsoft Sysmon logging against the most common Living off the Land techniques. Exploring how this can be accomplished without an extensive budget will be the focus of this paper.

Read the research: www.sans.org/u/1oN8

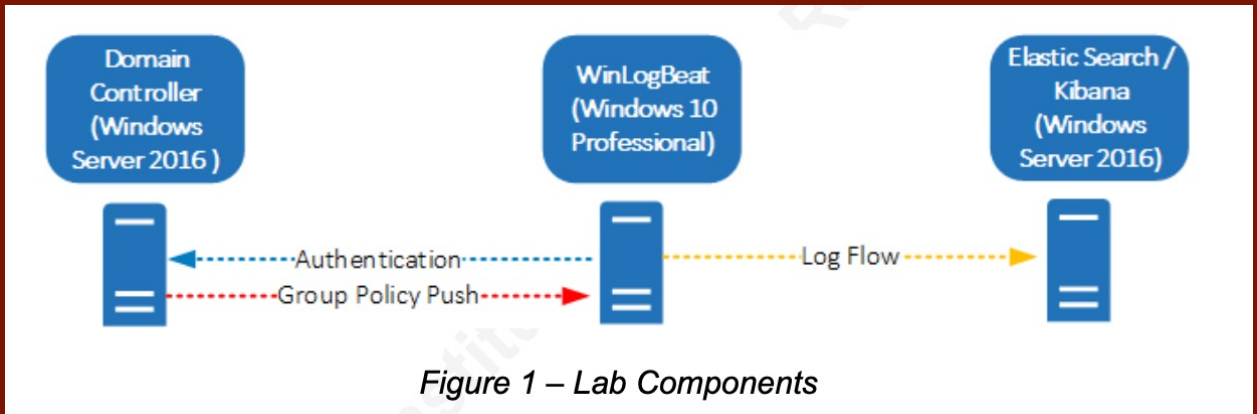


Figure 1 – Lab Components

"THINK DIFFERENT" ABOUT COMPLIANCE: IS EFFECTIVE, AUTOMATED MACOS CONFIGURATION ACHIEVABLE WITH NIST'S MACOS SECURITY COMPLIANCE PROJECT?

BY T. BOONE BERLIN

Information security compliance within the Apple macOS ecosystem is an especially challenging problem for IT practitioners. Apple's Mac computers continue to grow in enterprise deployment market share (Evans J., 2021). Simultaneously, compliance audit reporting and management is a growing concern for IT teams, managers, and executives as the threat of ransomware and other financially motivated attacks have become more prevalent in recent years. Compared to Windows, there remains a relative need for configuration management and compliance tools natively available for macOS. NIST recently released SP800-219, titled "Automated Secure Configuration Guidance from the macOS Security Compliance Project (mSCP)." It aims to provide 1) a new compliance/configuration solution for the macOS ecosystem and 2) an automated configuration tool built around mitigating the compliance challenges from Apple's annual macOS release cycle. This paper reports findings between four systems: macOS 10.15 Catalina, 11 Big Sur, 12 Monterey, and 13 Ventura. Nessus, Lynis, and mSCP tools audited each system in a "reference" new installation configuration. Then each was configured by the mSCP tool according to the CIS Level 2 Benchmark for each macOS version. Finally, each system was audited again with the trio of tools to determine the effectiveness of the mSCP tool. Results show that mSCP is an effective configuration management and audit tool. However, due to limitations within macOS and design decisions within mSCP, there is still a notable amount of manual configuration required. mSCP is a flexible command line interface (CLI) based tool and could be easily integrated into custom scripts, further automating the configuration and auditing process. However, documentation is somewhat limited and presents a learning curve.

Read the research: www.sans.org/u/1oHO

	Improvement Reported[9]			Difference in Reported Improvement[10]	
macOS	Nessus	mSCP	Lynis	Reference	Configured
10.15 Catalina	12%	82%	10	-30%	40%
11 Big Sur	16%	61%	10	-4%	41%
12 Monterey	15%	61%	10	-3%	43%
13 Ventura	14%	56%	9	-8%	33%

Table 3. Compliance Score Reporting Comparison

FIREWALL "BANG FOR YOUR BUCK": A SMALL AND MEDIUM-SIZED ENTERPRISE EDITION

BY STEVE BROWN

Information security amounts to installing host-based anti-virus software, Wi-Fi passwords, in addition to configuring permissions and native multi-factor authentication in cloud-based applications for many smaller U.S.-based businesses. Extensive and often even basic network perimeter security is overlooked. This research investigates low-cost changes to the network perimeter firewall to reduce these businesses' exposure to outsider threats significantly.

Read the research: www.sans.org/u/1oN3

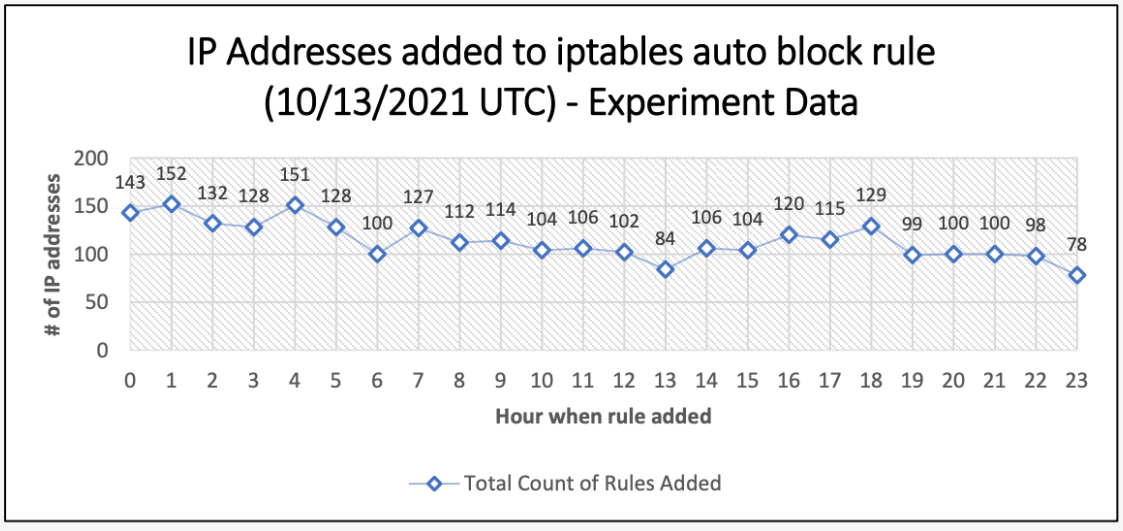


Figure 10: IP Addresses added to iptables auto-block rule (10/13/2021 UTC) - Experiment Data

DETECTING APPLICATION LAYER DDOS ATTACKS USING TLS FINGERPRINTING

BY ALEJANDRO AUCESTOVAR

Application layer DDoS attacks are some of the most complex and devastating attacks on the modern internet. Unlike their lower-layer counterparts, application-layer DDoS attacks utilize the widely accepted TLS encryption, commonly used across the internet, to their advantage so that identification and mitigation do not happen easily. Previous research has had different levels of success at identifying DDoS attacks and differentiating them from legitimate human traffic as well as legitimate flash flood events. Adding TLS fingerprinting details of a client/server communication to the identification methodology previously used and tested by researchers will increase fidelity in identifying application-layer DDoS attacks. The combined identification methodology and JA3 fingerprinting technique were tested against the Canadian Institute of Cybersecurity's DDoS dataset created in 2019. TLS Fingerprinting successfully identified illegitimate traffic by providing details of the user/client operating system, browser information, and application components.

Read the research: www.sans.org/u/1oN3

.50.9	13.35.78.80	107.23.199.168	
Average	11.797731	11.751489	
Std Dev	24.871305	24.747548	
.50.8	162.248.19.151	54.235.104.182	
Average	2.983623	3.108598	
Std Dev	9.324346	9.569274	
.50.6	54.200.193.43	104.19.198.151	
Average	6.018451	11.670449	
Std Dev	18.930571	24.603402	

Table 3. Request Interval Sequence Statistics for Legitimate Users

BOOKMARK BRUGGLING: NOVEL DATA EXFILTRATION WITH BRUGGLEMARK

BY DAVID PREFER

Modern web browsers like Chrome, Edge, Safari, and Firefox are ubiquitous, and built-in synchronization capabilities have long since become a standard feature. For even longer, browsers have enabled users to save and edit bookmarks and the names and links stored for each. Where bookmarks were once confined to the device that saved them, this research describes how the ability to synchronize bookmarks across devices introduces a novel vector for data exfiltration and other misuses. As a part of this effort, Brugglemark is a basic PowerShell script that has been created to demonstrate the practical application of the findings presented. Potential countermeasures will also be explored in this paper.

Read the research: www.sans.org/u/1oM0

BROWSER	VERSIONS TESTED
Chrome Stable Channel	99.0.4844.74, 99.0.4844.82, 100.4896.60, 100.0.4896.75, 100.0.4896.88, 100.0.4896.127, 101.0.4951.54, 101.0.4951.64, 102.0.5005.63
Chrome Beta Channel	103.0.5060.42, 103.0.5060.53
Edge Stable Channel	99.0.1150.39, 99.0.1150.46, 100.0.1185.44, 101.0.1210.32, 101.0.1210.39, 102.0.1245.39
Brave Stable Channel	1.37.114 Chromium: 100.0.4896.88, 1.37.116 Chromium: 100.0.4896.127
Opera Stable Channel	85.0.4341.28, 85.0.4341.75, 86.0.4363.23

Table 1. Browser versions tested.

"We could say that there is much in the technological world that changes continually. We could also say that at the same time, there isn't as much of what doesn't change. When these two perspectives collide, however, unintended security ramifications can be very intriguing.

In this paper David describes how he leveraged the ever-present web browser to discover a unique method of data exfiltration via browser bookmarks. Not only did David discover this novel method for data exfiltration, but he went above and beyond by writing a proof-of -concept tool that uses PowerShell for automation of the exfiltration.

I have no doubt that his work will be relevant for many more years to come due to the static and persistent nature of web browsers (many things change, but some remain the same in almost perpetuity)." – **BRYAN SIMON, FACULTY RESEARCH ADVISOR**

ANTIMALWARE SCAN INTERFACE BYPASSES: EVADING DETECTION TO PERFORM POST EXPLOITATION ACTIVITIES

BY CHRISTOPHER NOURRIE

During red team engagements and penetration tests, one of the initial challenges that penetration testers and red teamers must overcome is the antimalware scan interface (AMSI) integrated with most endpoint security solutions. AMSI was designed to add a layer of defense to Windows operating systems by analyzing and preventing the execution of malicious files. AMSI presents a challenge to penetration testers and red teamers as many of the tools utilized to conduct offensive engagements are detected by AMSI as malicious files. Since the introduction of AMSI, public releases of AMSI bypass techniques have been temporarily successful. AMSI is periodically updated with signatures to identify malicious files and to address well-known bypass techniques. This research analyzes how AMSI works, and the techniques red teamers and penetrations testers leverage to develop new AMSI bypass techniques to conduct post-exploitation activities.

Read the research: www.sans.org/u/1oMf

```
C:\Users\morty\Desktop\temp>AmsiTrigger.exe -i asbb_original.ps1 -f 1
[+] "Add-Type $Win32

$LoadLibrary = [Win32]::LoadLibrary("am" + "si.dll")
$Address = [Win32]::GetProcAddress($LoadLibrary, "Amsi" + "Scan" + "Buffer")
$p = 0
[Win32]::VirtualProtect($Address, [uint32]5, 0x40, [ref]$p)
$Patch = [Byte[]] (0xB8, 0x57, 0x00, 0x07, 0x80, 0xC3)
[System.Runtime.InteropServices.Marshal]::Copy"
```

Figure 8. Leveraging AMSITRigger.exe to identify malicious strings in a PowerShell script

HOW SECURE IS YOUR HEALTH INFORMATION? ELECTRONIC MEDICAL RECORD VULNERABILITY DISCOVERY

BY CHRIS PATTERSON

Electronic Medical Record (EMR) System vulnerabilities provide an easy target for hackers to steal valuable personal data. With an average cost to a healthcare provider of $9.23 million per hacking incident (Ponemon Institute, 2021), EMR vendors need to work with security researchers to review, discover, and patch these vulnerabilities before attackers exploit them. While the security community has made some efforts to disclose vulnerabilities, these efforts are often sporadic and rely on niche feature sets to be enabled. Security researchers' limited time and resources need to be focused on the most used and most likely to be exploited targets in these EMR applications. This whitepaper utilizes vulnerability exploitation in a popular open-source EMR application to provide specific areas for researchers to focus efforts on securing the applications that protect this valuable data.

Read the research: www.sans.org/u/1oMJ

Full Name	Date of Birth	External ID
aAbMylJH, tJgir Gar	1955-11-25	54283
AacBjNhgMHJ, XVBZDrwnguU	1926-08-12	35106
aAHydzk, zKPOBwZcTnMevb	1973-12-07	23608
AaiEDYzFGPsdq, KeQlEhYGHDnS	1948-05-09	40487
aAljxB, cPmUvsVAe	1988-10-19	43702
AajFYR, lYzyHGDQXSs	1984-10-29	51412
AajxglpUZbnuY, gXPpDiNsu	1978-07-31	33567
AakHoyCzEb, KErgUQPFBYZcw	1990-09-27	45597
aAMpUODPh, WihbjKY	1957-11-26	32358
aAmWzb, oLZnW	1934-02-19	44139

Patient Finder Screen After Appendix C Script Execution

NATION-STATES: THEY'RE JUST LIKE US. EMULATING COMMON TACTICS, TECHNIQUES, AND PROCEDURES

BY GEOFF HORVATH

When attacking private organizations, nation-states often employ a variety of methodologies to gain initial access to networks, access files, exfiltrate information, and perform post-compromise tasks. These methodologies often are thought of as sophisticated, bespoke threat vectors requiring vast resources to perform. When defending against these capabilities, private organizations often think of themselves as unable to accurately model the threat or believe they are too small of a fish to be concerned. In many high-profile instances, this was, in fact, not the case. Small organizations, with their limited resources, are also targets of nation-states as they can provide access to information resources of larger organizations. By observing and analyzing tactics, techniques, and procedures (TTPs) utilized by these attackers, organizations can implement defensive measures to mitigate the threat posed by these actors and improve an organization's information security level. Many of the tools and methodologies used by nation-states are not unique to those organizations but still follow along the same lines of a commercial penetration test or a cyberattack by a nongovernmental entity. By understanding the common threats posed by nation-states, an organization can also construct a more robust digital security awareness program. Knowing how the adversaries act enables organizations to anticipate future threats and understand that nation-states are not insurmountable obstacles or threats but, in many cases, can be treated like any other cyber-criminal.

Read the research: www.sans.org/u/1oMu

	Spear Phishing	Social Engineering	Watering Hole	Compromised Credentials	Remote Access	CVE Exploits
Metasploit Community/Pro	X	X	X	X	X	X
Cobalt Strike	X			X	X	X
Infection Monkey				X	X	
APT Simulator			X	X	X	
Social Engineering Toolkit	X	X	X			

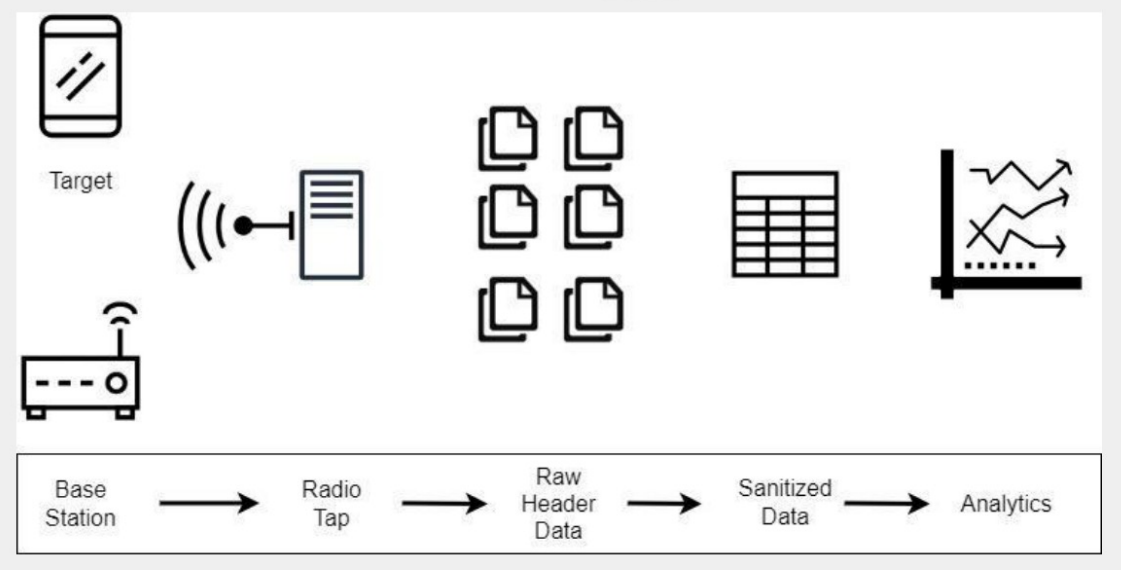
Comparison of Open-Source Tools to Nation-State Actions

ESTABLISHING PATTERN OF LIFE BASED ON PASSIVE COLLECTION OF WIFI TRANSMISSIONS

BY JASON LEVERTON

WiFi has become a staple service with the growth of home networking, smart devices, IoT, and several devices that utilize WiFi to function. Recent attempts have been made to enhance devices due to the privacy concerns of passive WiFi collection. Location services, subject identification, or population enumeration were easily captured prior to address randomization. However, more targeted collections methods are still available in specific applications. Certain characteristics inherently exist in the WiFi protocol that allows attribution to be made, which can be used to identify subjects, their usage on the spectrum, and even give away their physical colocation in a target area. This paper will explore the mechanisms that exist through the passive collection of WiFi signals to build a subject's Pattern of Life (PoL) that persists even through privacy enhancements of address randomization. This research will identify the attributions that remain available for passive capture and that can be used as a tool for enhanced surveillance on a subject. Conversely, the research will inform potential defensive postures to increase OPSEC and PERSEC while utilizing WiFi.

Read the research: www.sans.org/u/1oNd



Collection Data Flow

SCANNING WORDPRESS PLUGINS FOR VULNERABILITIES

BY ADI WONG

WordPress is the most used Content Management System (CMS) for websites that runs 42.8% of all Internet Websites (w3tech, Oct 2021). WordPress users range from individual users to large corporations who use it to run a blog site, e-commerce store, company website, and more. One of the reasons for its popularity is the availability of themes and plugins developed by third parties that allow the website owner to add functionality easily without knowing how to code. At the same time, there has been an increasing trend of finding vulnerabilities from these third-party plugins. This paper will explore and compare the result of finding WordPress vulnerabilities on previous plugins with known Common Vulnerabilities and Exposures (CVE) vulnerabilities using a Static Application Security Testing (SAST) and WordPress specific scanner, WPScan. This paper will compare the effectiveness of a SAST to proactively find vulnerabilities against WPScan which detects vulnerabilities reactively as they need to be reported in its database to find a match.

Read the research: www.sans.org/u/1oMO

Review Priority	Category	Security Hotspot Rules Triggered	Count
HIGH	auth	Hard-coded credentials are security-sensitive	7
		Setting loose POSIX file permissions is security-sensitive	119
	sql-injection	Formatting SQL queries is security-sensitive	1
	xss	Creating cookies without the "HttpOnly" flag is security-sensitive	98
		Disabling Vue.js built-in escaping is security-sensitive	16
MEDIUM	dos	Using slow regular expressions is security-sensitive	229
	rce	Dynamically executing code is security-sensitive	34
	weak-cryptography	Manual generation of session ID is security-sensitive	1
		Using pseudorandom number generators (PRNGs) is security-sensitive	720
		Using weak hashing algorithms is security-sensitive	506

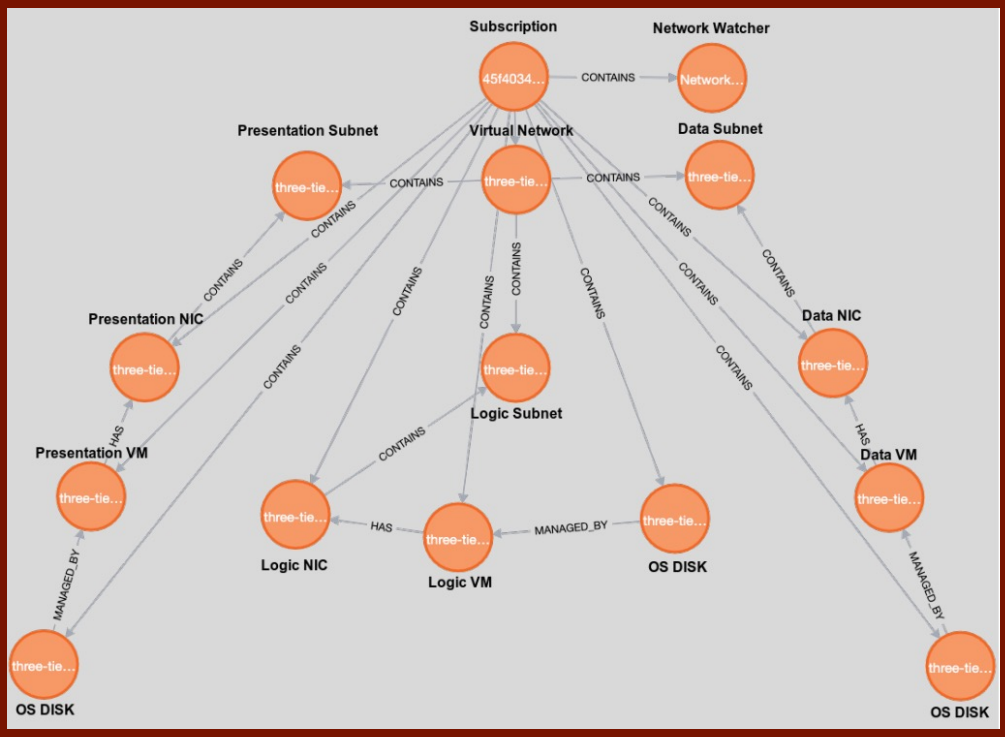
Table 3 – SonarQube – Security Hotspot Categorization and Count of Triggers Count

ENTERPRISE OBSERVABLE SECURITY: A HOLISTIC APPROACH USING AZURE

BY JOSE MARIA POLANCO CANUL

The information security industry has been plagued with many technical and social challenges that have made securing environments seemingly impossible. In this paper, a holistic approach toward managing complex environments is proposed called Enterprise Observability using Azure as an example. The focus of this proposal is to improve attack surface management in complex environments, allow security professionals to understand the behavior of their environments, and leverage the platform to improve security operations.

Read the research: www.sans.org/u/1oM5



Enterprise Observability Graph Visualization

"Jose's research into Enterprise Observability lays the foundation for creating an understanding of an Azure environment to make assessment efforts repeatable with the contextual information to be as accurate as possible. While the paper is Azure-centric, these concepts can be extended to other public cloud environments as well." – **JOHN HALLY, FACULTY RESEARCH ADVISOR**

IS YOUR CLOUD ENVIRONMENT SECURE? HOW DO YOU KNOW?

BY KIEL VAUGHN

The adoption and utilization of cloud environments continue to proliferate for businesses of all sizes. Organizations realize numerous benefits upon integrating cloud services, including ease of use, flexibility, and lack of large upfront expenditures. However, several drawbacks exist, including the lack of understanding of the nuanced differences between managing traditional data centers and cloud environments. This drawback often leads to disaster, as numerous highly publicized data breaches have resulted from misconfigurations of cloud resources. Fortunately, there are multiple tools available to help combat this problem. This research analyzes three cloud auditing tools — AWS Config, Prowler, and Scout Suite, to determine which provides the best value to organizations.

Read the research: www.sans.org/u/1oLV

Tool Analysis Summary

Assessed Criteria	AWS Config	Prowler	Scout Suite
Installation	4	4	4
False Positives	5	5	4
Audit Completeness/False Negatives	5	4	2
Clarity of Results	3	4	3
Flexibility	5	4	2
Unique Features	5	5	2
Total Score	27	26	17

Note. These ratings utilize each tool's latest version as of August 17, 2022.

HEAD IN THE CLOUD? CLOUD APPLICABILITY OF THE NIST CYBERSECURITY FRAMEWORK

BY RAYMOND MINIFIELD

The NIST Cybersecurity Framework is the gold standard by which organizations evaluate their cybersecurity controls. The NIST Cybersecurity Framework was developed in 2014 with a minor revision in 2018. The threat landscape has changed dramatically over the past decade, with threat actors becoming more refined in their methods. The technology landscape has also evolved, and cloud computing platforms such as AWS and Azure did not exist a decade ago. With these significant changes in the cybersecurity domain, does the NIST Cybersecurity Framework still help organizations to prevent and reduce cybersecurity risk effectively?

Read the research: www.sans.org/u/1oMa

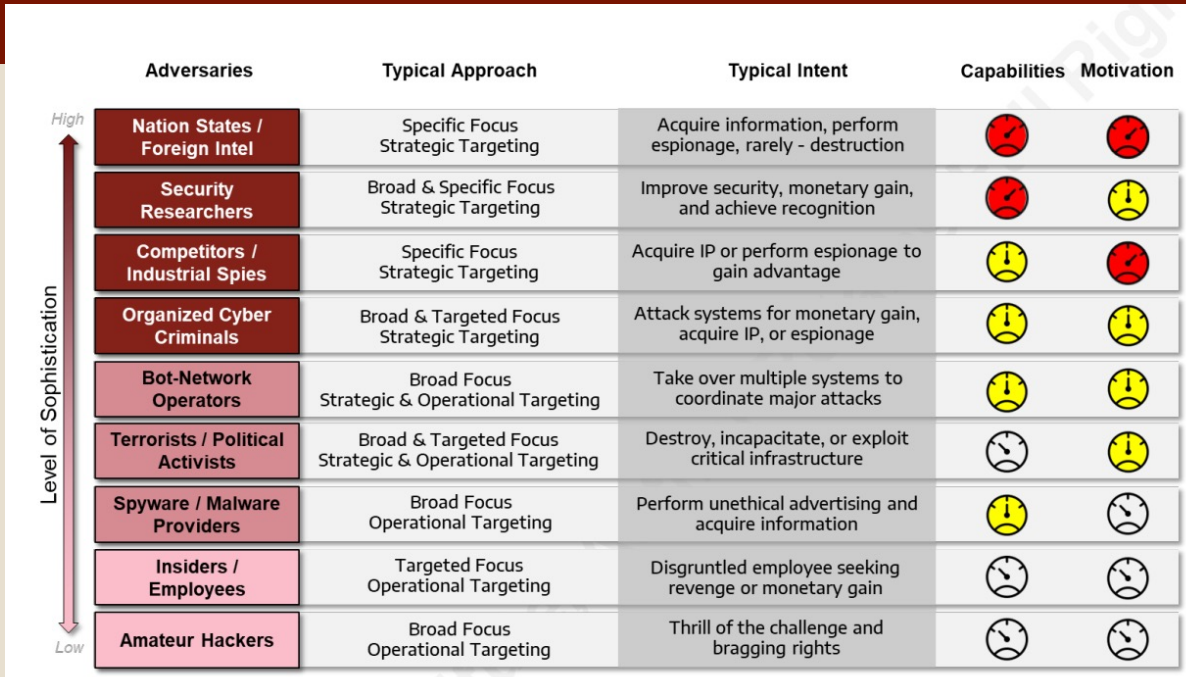


Figure 1: Categorization of Cyber Adversaries

IMPLEMENTING SCALABLE SECURITY FOR DEVICES WITHOUT 802.1X SUPPORT

BY UMER KHAN

Enterprises often implement 802.1x to control access to wired and wireless networks by authenticating computers using username/password or a digital certificate, but MAC Authentication Bypass (MAB) is used for devices that do not support enterprise 802.1x capability such as printers, industrial control systems, and operating technology machines. MAB is difficult to maintain and devices that use it are often permitted unrestricted network access without other security mitigations. Since MAC addresses are easy to impersonate, this authentication mechanism by itself is ineffective and easy to bypass, thereby granting attackers easy access to enterprise networks. This research analyzes how to implement MAB in a more scalable fashion and how to enhance it with security mitigations such as device fingerprinting for device validation and automated access control lists to restrict network resources a MAB-authenticated device can access.

Read the research: www.sans.org/u/1oLG

"The topic of Umer's paper is critical for organizations with devices that don't support the 802.1x protocol for accessing the network. His approach to addressing this challenge was very pragmatic--it relied on accessible, free, and open-source tools for controlling how such devices connect to the network and minimizing the risk they pose to other information resources. Security professionals can refer to Umer's research to quickly understand what they can achieve when tackling such challenges in a scalable way."

– LENNY ZELTSER, FACULTY RESEARCH ADVISOR

Physical or virtual network firewalls	"Router ACLs" on SVIs	Port Access Control Lists (PACLs)
Work at VLAN / layer-3 boundaries only (inter-VLAN traffic)	Work at VLAN / layer-3 boundaries only (inter-VLAN traffic)	Works at every switch port (all traffic goes through them)
Require possible move of devices to "appropriate" VLAN, re-IP-addressing	Require possible move of devices to "appropriate" VLAN, re-IP-addressing	Can be applied without having to "move" or "re-IP" a device
Require "VLAN change" and shut/no-shut on the port	Require "VLAN change" and shut/no-shut on the port	Can be applied without having to "change VLAN" and shut/no-shut port
Provide best inspection and logging abilities (stateful; based on deep packet inspection, etc.)	Inspection / logging nowhere near as good as a (mostly layer 3 and layer 4)	Inspection / logging nowhere near as good as (mostly layer 3 and layer 4)
Require adding a "hop" / bottleneck to the network. Scale challenges.	Scale without impact in performance	Scale without impact in performance
VLANs have scaling limitations (too many spanning tree instances, etc.)	VLANs have scaling limitations (too many spanning tree instances, etc.)	Work fine with a small number of VLANs
Do not depend on PACL support in switches	Do not depend on PACL support in switches	Switches must support PACLs and have large enough TCAMs

TABLE 1: COMPARISON OF NETWORK SEGMENTATION OPTIONS FOR MAB-AUTHENTICATED DEVICES.

NETWORK ACCESS CONTROL AND ICS: A PRACTICAL GUIDE

BY RONALD GROHMAN

Industrial Control Systems (ICS) are the lifeblood of the organizations that use them, often requiring one-hundred percent uptime. This requirement makes securing them and the networks they operate on extremely challenging, as increased security often increases the risk of interruption. Due to the nature of their function, Industrial Control Systems tend to be left untouched and in place until they physically break. Resulting in decadesold equipment operating on modern infrastructure with modern security risks. Those things combined with OT staff, who are often not trained in security or basic IT functions, means getting buy-in for anything that increases risk or changes their job function becomes near impossible. However, it is still possible to implement complex network access control systems safely and effectively and architect them in a way usable by plant engineers (OT staff) without the need for extensive security or IT training.

Read the research: www.sans.org/u/1oMY

Figure 11 - IND Shared Attributes

assetDeviceType	EtherNet/IP Node
assetId	20207
assetIpAddress	10.3.44.73
assetMacAddress	00:00:bc:37:cd:4b
assetName	10.3.44.11
assetProductId	1747-L551/C C/11 - DC 3.46
assetProtocol	CIP
assetSerialNumber	0xBC37CD4B
assetSwRevision	3.011
assetVendor	Rockwell Automation/Allen-Bradley

IMPLEMENTING SECURITY CONTROLS TO IOT WIRELESS TECHNOLOGIES

BY BRIAN HERRON

Business leaders and risk management decision-makers are unaware of how the Internet of Things (IoT) increases the threat surface to business assets and devices. Emerging network technologies such as Thread and Zigbee are creating unmonitored, bi-directional connections into business networks due to the rise of IoT integration into devices found in businesses today. Designed for minimal processor requirements and low power consumption, implementing security controls on individual IoT devices is not possible. Utilizing segmentation and open-source border routers increases a company's security posture by restricting lateral movement and enabling visibility of how these devices interconnect to the business' data networks. Following the Center for Internet Security Controls methodology, these techniques provide an effective strategy to mitigate potential risks of implementing IoT in business environments

Read the research: www.sans.org/u/1oMz

	Zigbee with Segmentation and WebThings		
CIS Control	Control Title	Segmentation	COTS
1	Inventory and Control of Enterprise Assets	Partial*	Minimal
2	Inventory and Control of Software Assets	None	None
3	Data Protection	Minimal*	Minimal
4	Secure Configuration of Enterprise Assets and Software	Partial*	None
8	Audit Log Management	Significant*	None
12	Network Infrastructure Manangement	Significant*	None
13	Network Monitoring and Defense	Significant*	None
	*utilizing non-certified Zigbee gateway		

	Thread with Segmentation and OTBR		
CIS Control	Control Title	Segmentation & OTBR	COTS
1	Inventory and Control of Enterprise Assets	Significant	Minimal
2	Inventory and Control of Software Assets	Partial	None
3	Data Protection	Significant	Minimal
4	Secure Configuration of Enterprise Assets and Software	Partial	None
8	Audit Log Management	Significant	None
12	Network Infrastructure Manangement	Significant	None
13	Network Monitoring and Defense	Significant	None

BUILDING AN INTELLIGENT, AUTOMATED TIERED PHISHING SYSTEM: MATCHING THE MESSAGE LEVEL TO USER ABILITY

BY GEOFFREY PARKER

Phishing campaigns and the procedures to run them have remained unchanged since the dawn of the modern era of security awareness training platforms in 2012. The present model uses templates sent at random, assigned based on the level of difficulty of the template, not the user. This study creates a new phishing model, method, and process in which the system matches the phishing message difficulty level to the user's skill level. The new design factors the current aptitude of the user and the level of the message difficulty. The system is intelligent, automated, dynamic, and platform-agnostic to scale for the size of the enterprise. Analysis of the tiered system produced statistically significant results indicating that the system improves the user's ability to detect phishing. The system systematically builds the user's skill level and commensurately decreases the risk of falling victim to phishing attacks. There are no other known documented systems like this that are in use at this time. The study discusses forward looking observations on how practitioners could further enhance this new system when used with User Behavior Analytics and Risk Scoring.

Read the research: www.sans.org/u/1oNi

A possible console view of your campaigns

Campaign	Target Group	Tier	Message Difficulty	User Count	Action
Advanced 0%	0% PPP	1	Very Hard (5 star) ★★★★★	2832	Clone
Very Good 1-10%	1-10% PPP	2	Hard (4 star) ★★★★	2300	Clone
Intermediate 11-50%	11-50% PPP	3	Medium hard (2-3 star) ★★★	520	Clone
Beginner 51-99%	51-90+% PPP	4	Easy (1 star) ★	430	Clone

Figure 6. A sample console view of tiered phishing campaigns

"Geoffrey's paper exemplifies what we are attempting to accomplish with our research project. Geoffrey took a real-world problem and applied the rigor necessary to solve it. His problem was particularly challenging because it involved some of security's social and human aspects. But Geoffrey managed to find a measurable and reproducible solution."

– JOHANNES ULLRICH FACULTY RESEARCH ADVISOR

INOCULATING THE MASSES: EVALUATING CYBERSECURITY AWARENESS TRAINING

BY SHAY CHRISTENSEN

Like a disease, cybercrime is spreading across the world. The sums of money lost to these criminals seem to be increasing daily. Many technical solutions are on the market to detect and prevent the latest threats. However, these solutions don't prevent adversaries from exploiting the most common attack vector, the human. Many large organizations have budgets and teams responsible for training their employees to detect and evade phishing emails and other threats. The problem lies in the large portion of the population who doesn't have access to this regular training. This study will examine the landscape of available free training options and compare them against the most prevalent threats the average person faces.

Read the research: www.sans.org/u/1oLL

Training Program	Phishing Awareness	BEC/EAC Passphrase	Malware Patching	The Why?	The How?	The What?	Average Score
CDSE	Excellent	Good	Good	Good	Good	Good	**3.16**
Cyber Exchange	Fair	Fair	Fair	Poor	Fair	Good	**2**
ESET	Excellent	Good	Fair	Excellent	Excellent	Excellent	**3.5**
HHS	Excellent	Excellent	Fair	Good	Good	Good	**3.16**
Curricula	Excellent	Excellent	Fair	Excellent	Excellent	Good	**3.5**
CISA	Excellent	Fair	Excellent	Good	Good	Good	**3.16**

Table Summary of Program Scores

CONTINUOUS DIAGNOSTICS AND MITIGATION: EVOLVING FEDERAL DEFENSES WITH COST-EFFECTIVE AND MAINTAINABLE DATA INTEGRATION SOLUTIONS

BY ANDREW DAVIDOW

Civilian federal agencies have struggled to implement the Continuous Diagnostics and Mitigation program over the past decade. Billions of dollars have been spent, and the cybersecurity tools have been deployed. Yet, there are challenges in getting the data from those tools into the new CDM Dashboard powered by Elasticsearch and Kibana. Filebeat and Logstash can solve this problem. The data from two CDM tools, HCL BigFix and Tenable.sc were collected using Filebeat and Logstash and stored in Elasticsearch. This approach is simple, maintainable, feasible, and cost-effective.

Read the research: www.sans.org/u/1oMk

Computer Na	CPU	RAM	MAC Address	IP Address	IPv6 Address	OS
b65eb28d3baa	860 MHz Core i5-6300U	15776 MB	02-42-ac-11-00-02	172.17.0.2	<none>	Linux Ubuntu 20.04.4 LTS (3.10.0-116
BF-10-0-4-INV	2800 MHz Xeon	9984 MB	08-00-27-6f-a8-d7	10.10.4.3	fe80:0:0:0:d518:d7e:	Win2019 10.0.17763.3113 (1809)
BF-10-0-4-SERV	2800 MHz Xeon	16000 MB	08-00-27-de-0e-6b	10.10.4.2	fe80:0:0:0:e53f:80f6:	Win2019 10.0.17763.3113 (1809)
centos8-workstation	3100 MHz Core i7-8705G	1824 MB	[+] 00-0c-29-92-c2-59	[+] 10.10.21.16	fe80:0:0:0:20c:29ff:f	Linux CentOS Stream 8 (4.18.0-394.el
d66d55104b4d	2800 MHz Core i5-6300U	15776 MB	02-42-ac-11-00-04	172.17.0.4	<none>	Linux Ubuntu 20.04.4 LTS (3.10.0-116
debian9-workstation	3100 MHz Core i7-8705G	2016 MB	00-0c-29-17-e2-da	10.10.21.17	fe80:0:0:0:20c:29ff:f	Linux Debian 9.13 (4.9.0-18-amd64)
elk-vm	2700 MHz Core i7-6820HQ	31328 MB	00-0c-29-61-ba-56	10.10.2.2	fe80:0:0:0:43b:faf7:3	Linux Ubuntu 18.04.6 LTS (5.4.0-122-
ol1	2900 MHz Core i5-6300U	15776 MB	02-42-ac-11-00-20	172.17.0.32	<none>	Linux Oracle Enterprise Server 8.6 (3.

A cropped view of the HWAM report in Web Reports

A FORENSIC ANALYSIS OF ANDROID MOBILE PRIVATE BROWSING ARTIFACTS

BY WARREN THOMPSON

The adoption of mobile devices and functionality continues to grow daily. Simultaneously, there has been an increase in privacy awareness and the desire for anonymity while browsing the internet. This research paper aims to explore the effectiveness of private browsing at mitigating the generation and persistence of filesystem-based artifacts on Android-based mobile devices. Four popular browsers used by advocates of private browsing were studied: Chrome, Firefox, DuckDuckGo, and Tor Browser. In some cases, the results were in line with expectations. In others, the results were alarming. The research shows that gaining access to a full disk image, including unallocated disk space, could allow an individual to access private browsing history, as well as the screenshots of websites visited in specific cases. In all cases, persistent filesystem-based artifacts were generated. In summary, private browsing is not as private as popularly perceived.

Read the research: www.sans.org/u/1oMT

	Search term	domain_histogram.txt	Domain.txt	email_domain_histogram.txt	email_histogram.txt	email.txt	json.txt	url_searches.txt	url_services.txt	sqlite.db	url_historgram.txt	url.txt	Base VM Delta
BASE	checkboxolympics.com	-	-	-	-	-	-	-	-	-	-	-	-
	guardian.co.tt	-	-	-	-	-	-	-	-	-	-	-	-
	wikirecreation.com	-	-	-	-	-	-	-	-	-	-	-	-
	burymewithmymoney.com	-	-	-	-	-	-	-	-	-	-	-	-
	JoePandaRocks@hotmail.com	-	-	-	-	-	-	-	-	-	-	-	-
	JoePandaRocks@yahoo.com	-	-	-	-	-	-	-	-	-	-	-	-
	Hotmail.com	1	1	1	1	1	-	-	-	-	-	-	5
	Yahoo.com	89	345	1	2	6	2	1	89	-	-	341	876
	Twitter.com	2	17	-	-	-	3	-	2	-	5	19	48
	Connection search_research_test	-	-	-	-	-	-	-	-	-	-	-	-
	Convict search_research_test	-	-	-	-	-	-	-	-	-	-	-	-
	Symptom search_research_test	-	-	-	-	-	-	-	-	-	-	-	-
	Deprive search_research_test	-	-	-	-	-	-	-	-	-	-	-	-
	Flood search_research_test	-	-	-	-	-	-	-	-	-	-	-	-
	Nightmare search_research_test	-	-	-	-	-	-	-	-	-	-	-	-
	Craftsman search_research_test	-	-	-	-	-	-	-	-	-	-	-	-
	Tolerate search_research_test	-	-	-	-	-	-	-	-	-	-	-	-
	Flow search_research_test	-	-	-	-	-	-	-	-	-	-	-	-
	Spill search_research_test	-	-	-	-	-	-	-	-	-	-	-	-
	unanimous_email_research_test	-	-	-	-	-	-	-	-	-	-	-	-
	continental_email_research_test	-	-	-	-	-	-	-	-	-	-	-	-
	TOTAL	92	363	2	3	7	5	1	91	-	5	360	929

Bulk_extractor results for Base VM before browsing activity

CUTTING-EDGE RESEARCH FROM SANS.EDU CYBERSECURITY BACHELOR'S STUDENTS

EXTRACTING 'HTTP CONNECT' REQUESTS WITH PYTHON

by Jesse La Grew

Published: 2022-11-14 LINK

QUICK ANSWERS IN INCIDENT RESPONSE: RECMD.EXE

by Logan Flook

Published: 2022-06-02 LINK

TERRAFORMING HONEYPOTS. INSTALLING DSHIELD SENSORS IN THE CLOUD

by Dustin Lee

Published: 2022-06-15 LINK

Lead

Join the next generation of cybersecurity leaders

SANS.edu

Master of Science in Information Security Engineering

Rigorous, challenging, and rewarding, the 36-credit Master of Science in Information Security Engineering (MSISE) program prepares working InfoSec professionals to advance to positions of leadership – whether for a commercial enterprise or a government or military entity.

GIAC Certifications

Earn 9 industry-recognized GIAC certifications throughout the program, validating the skills you've gained.

Leadership Skills

Prepare to lead through a career-focused curriculum that develops both technical expertise and management and communication skills.

Depth of Knowledge

Build your professional reputation by contributing to our collection of graduate student white papers, considered for publication in the SANS Reading Room and leading industry journals.

Career-focused Electives

Customize your degree with an optional focus area.

- Cloud Security
- Cyber Defense Operations
- Incident Response
- Industrial Control Systems
- Penetration Testing
- Security Management

APPLICATIONS ACCEPTED QUARTERLY

The SANS Technology Institute is accredited by The Middle States Commission on Higher Education (1007 North Orange St, 4th Fl, MB #166, Wilmington, DE 19801 - 267.284.5000), an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

Funding Options

Corporate Tuition Assistance

SANS.edu meets the requirements for most corporate tuition assistance programs.

Funding for Veterans

All our academic programs are eligible for U.S. and Canadian veterans' education benefits.

Interest-free Payment Plan

Eligible graduate students can fund their tuition in monthly installments with no interest.

Income Share Agreement (ISA)

Eligible undergraduates can apply to pay little or no tuition until after they are employed.

Questions?
We're happy to help.

Email: info@sans.edu
Call: (301) 241-7665

Updated 11.1.22