Internet Downloaded (Fareit) Malwares in Memory

Dhruv Gajjar and Aniket Patel

January 10, 2020

Internet Downloaded (Fareit) Malwares in Memory

***Author:* - Dhruv Rohitbhai Gajjar**

***Guided by:* - Aniket Patel**

Abstract: -

The idea is to find optimum use of memory by finding various formats of storing data so as to bring storage of computers into efficient memory storage area. The normal storage corresponds to binary storage formats, which corresponds to four inputs in number format, octal may corresponds to 8 input formats (2^3) whereas hexadecimal corresponds to 16 input procedures, which allows us to have a storage area as efficient as to support 16 input procedures making it is easier for having quicker storage. The faster we store and analyse the faster we get the result.

For security purposes we do memory forensic and try to detect malware if found. Computer security is a state of well-being of information and infrastructure. Also refers to the protection of computer systems and the information a user stores or processes. User should focus on various security threats and countermeasures in order to protect their information assets.

Question arise why security? Then answer to this is its importance for protecting the confidentiality, integrity, and availability of computer systems and their resources. Computer administration and management have become more complex which produces more attack avenues. Evolution of technology has focused on the ease of use while the skill level needed for exploits has decreased. Network environments and network-based applications provide more attack paths.

Confidentiality: - it is ensuring that information is accessible only to those authorized to have access. Authenticity: - identification and assurance of the origin of information. Integrity: - ensuring that the information is accurate, complete, reliable, and is in its original form. Availability: - ensuring that the information is accessible to authorized persons when required without delay. Non-Repudiation: - ensuring that a party to a contract or a communication cannot deny the authenticity of their signature on a document.

storage but also other purposes in computers and other digital electronics devices. There are two main kinds of semiconductor memory, volatile and non-volatile. Examples of non-volatile memory are flash memory (used as secondary memory) and ROM, PROM, EPROM and EEPROM memory (used for storing firmware such as BIOS). Examples of volatile memory are primary storage, which is typically dynamic random access memory (DRAM), and fast CPU cache memory, which is typically static random access memory (SRAM).

What is Forensics?

Forensic science is the application of science to criminal and civil laws, mainly on the criminal side during criminal investigation, as governed by the legal standards of admissible evidence and criminal procedure. Forensic scientists collect, preserve, and analyze scientific evidence. In addition to their laboratory role, forensic scientists testify as expert witness in both criminal and civil cases and can work for either the prosecution or the defense.

RAM Artifacts: -

Network connections: -

A computer network is a digital telecommunications network which allows nodes to share resources. In computer networks, computing devices exchange data with each other using connections (data links) between nodes. These data links are established over cable media such as optic cables, or wireless media such as Wi-Fi.

Running processes: -

There are dozens of processes running on your system, some for programs that you are interacting with graphically, some for commands that you have started at a shell prompt, some running in the background and some that perform system tasks. Each process is identified by a unique ID, known as the PID or process ID.

Usernames and passwords: -

Username referred to as an account name, login ID, nickname, and user ID, username or user name is the name given to a user in a computer or computer network.

A password, sometimes called a passcode, is a memorized secret used to confirm the identity of a user.

Dynamic link libraries (DLL): -

DLL is Microsoft's implementation of the shared library concept in the Microsoft Windows and OS/2 operating systems. These libraries usually have the file extension DLL, OCX (for libraries containing ActiveX controls), or DRV (for legacy system drivers). The file formats for DLLs are the same as for Windows EXE files that is, Portable Executable (PE) for 32-bit and 64-bit Windows, and New Executable (NE) for 16-bit Windows. As with EXEs, DLLs can contain code, data, and resources, in any combination.

Contents of open window: -

OpenWindows was a desktop environment for Sun Microsystems workstations which combined SunView, NeWS, and X Window System protocols. OpenWindows was included in later releases of the SunOS 4 and Solaris operating systems, until its removal in Solaris 9 in favor of Common Desktop Environment (CDE) and GNOME 2.0.

Open registry keys of process: -

The Windows Registry is a hierarchical database that stores low-level settings for the Microsoft Windows operating system and for applications that opt to use the registry. The kernel, device drivers, service, Security Accounts Manager, and user interface can all use the registry. The registry also allows access to counters for profiling system performance.

Open files for process: -

OpenedFilesView displays the list of all opened files on your system. For each opened file, additional information is displayed: - handle value, read/write/delete access, file position, the process that opened the file, and more… Optionally, you can also close one or more opened files, or close the process that opened these files.

Memory resident malware: -

Memory-resident malware is a type of malware that inserts itself into a computer or device in a particular way, loading its own program into permanent memory. This causes unique problems for security systems and professionals trying to maintain the integrity of a system and its security tools.

RAM Analysis: -

Memory analysis tools should be employed to collect networking connections and process information (registry and file information). Two popular memory forensic tools used to collect such information are Volatility, which is free and open-source, and HBGray, which is proprietary.

What is Malware?

Malware, or malicious software, is any program or file that is harmful to a computer user. Types of malware can include computer viruses, worms, Trojan horses and spyware. These malicious programs can perform a variety of different functions such as stealing, encrypting or deleting sensitive data, altering or hijacking core computing functions and monitoring users' computer activity without their permission.

How it Works?

Malware authors use a variety of physical and virtual means to spread malware that infect devices and networks. For example, malicious programs can be delivered to a system with a USB drive or can spread over the internet through drive-by downloads, which automatically malicious programs to systems without the user's approval or knowledge. Phishing attacks are another common type of malware delivery where emails disguised as legitimate messages contains malicious links or attachments that can deliver the malware executable to unsuspecting users. Sophisticated malware attacks often feature the use of a command-and-control server that allows threat actors to communicate with the infected systems, exfiltrate sensitive data and even remotely control the compromised device or server.

Emerging strains of malware include new evasion and obfuscation techniques that are designed to not only fool users but security administrators and anti-malware products as well. Some of these evasion techniques rely on simple tactics, such as using web proxies to hide malicious traffic or source IP addresses. More sophisticated threats include polymorphic malware, which can repeatedly change its underlying code to avoid detection tools, anti-sandbox techniques, which allow the malware to detect when it is being analyzed and delay execution until after it leaves the sandbox, and file less malware, which resides only in the system's RAM in order to avoid being discovered.

Types of Malware: -

Virus: - Spread with User Action.

Worms: - Spread Automatically.

Trojan: - Disguised as Legitimate Software.

Rootkit: - Hides Deep within PC.

Adware: - Monitor Your Activity.

Ransomware: - Encrypts Files and Demands Ransom.

Remote Access: - Control PC from a distance.

Exploit Kit: - Hunts Software Vulnerabilities.

What is Fareit Malware?

Threat Type: Spyware.

Destructiveness: No.

Encrypted: Yes, but blinded in soft wares (For example: - TeamViewer).

In The Wild: Yes.

Infection channel: Download from the internet.

Fareit is a malware family of information stealers used to download other malware such as ZEUS/ZBOT onto infected system. Its variants typically steal user names and passwords on stored in web browsers web browsers. In addition, these steal email credentials and ftp credentials such as the following: -

Directory List, Password, Port Number, Server Name, Server Type, User Name.

Users can get this malware by visiting malicious sites that host Fareit Variants.

Technical Details: -

Memory Resident: Yes

Payload: Connects to URLS/IPS

Other System Modifications: -

This spyware adds the following registry entries as part of its installation routine.

HKEY_CURRENT_USER\SOFTWARE\WINRAR

HWID="{GUID}"

How to detect malware in memory?

To detect memory-resident malware, it is essential that traditional antivirus is supplemented by technologies that facilitate volatile system memory (RAM) capture and continuous behavioral monitoring.

Organizations should look to Network (NIDS) and Host-based (HIDS) Intrusion Detection, as well as Endpoint Analytics, to help identify indicators of compromise (IOCs).

Once memory-resident malware has been detected, further analysis is required to enhance response efforts and help configure security systems to pinpoint similar attacks in the future.

Forensic analysis of memory-resident malware can be achieved with a tool such as AccessData FTK Imager, which can capture a copy of an infected device's memory contents for analysis.

Once a dump of the memory has been taken, it can then be transferred to separate workstation for analysis. This ensures that the original system, which may be needed as evidence, is fully preserved. The workstation should not be connected to a network.

With a copy of the system's memory, the Volatility Foundation's memory forensics framework can then be used to help analyse its contents. An initial starting point could be to examine active network connections from the host.

A subsequent action could be to run a plugin such as mal find to identify suspicious executables based on characteristics such as virtual address tree tags and page permissions.

Once a suspicious process has been detected, the system's memory, assessed with an antivirus scanner and, if necessary, reverse engineered.

Note: memory forensics is a highly specialized process that if not conducted correctly has ability to disrupt rather than aid an organization's response to cyber-attacks. Rather than risk losing vital evidence and facilitating the spread of an infection, organizations are advised to consult a threat detection and incident response specialist.

Simulation: -

Software: -

https://accessdata.com/products-services/forensic-toolkit-ftk: - AccessData Forensic Toolkit :- capture memory dumps. Dumps means virtual image.

https://www.magnetforensics.com/resources/magnet-ram-capture :- Magnet Ram Capture :- capture memory dumps. Dumps means virtual image.

https://www.hhdsoftware.com/free-hex-editor :- Hex Editor :- Watch content of dumps.

Tools: -

https://cisofy.com/lynis: - Lynis :- Tool to scan memory malware.

https://searchnetworking.techtarget.com/feature/Most-popular-viruses-and-hacking-tools :- Virus Making Tools

https://docs.oracle.com/cd/E19120-02/open.solaris/819-3194/dnsref-9/index.html :- Binding File Tools

https://gisgeography.com/open-source-remote-sensing-software-packages :- Remote Access Tools

Possible Solutions: -

Use a firewall to block all incoming connections from the internet to services that should not be publicly available. By default, you should not be denying all incoming connections and only allow services you explicitly want to offer to the outside world.

Enforce a password policy. Complex passwords make it difficult to crack password files on compromised computers. This helps to prevent or limit damage when a computer is compromised.

Ensure that programs and users of the computer use the lowest level of privileges necessary to complete a task. When prompted for a root or UAC password, ensure that the program asking for administration-level access is a legitimate application.

Disable AutoPlay to prevent the automatic launching of executable files on network and removable drivers when not required. If write access is not required, enable read-only mode is the option is available.

Turn off file sharing if not needed. If file sharing is required, use ACLs and password protection to limit access. Disable anonymous access to shared folders. Grant access only to user accounts with strong passwords to folders that must be shared.

Turn off and remove unnecessary services. By default, many operating systems install auxiliary services that are not critical. These services are avenues of attack. If they are removed, threats have less avenues of attack.

If a threat exploits one or more network services, disable, or block access to, those services until a patch is applied.

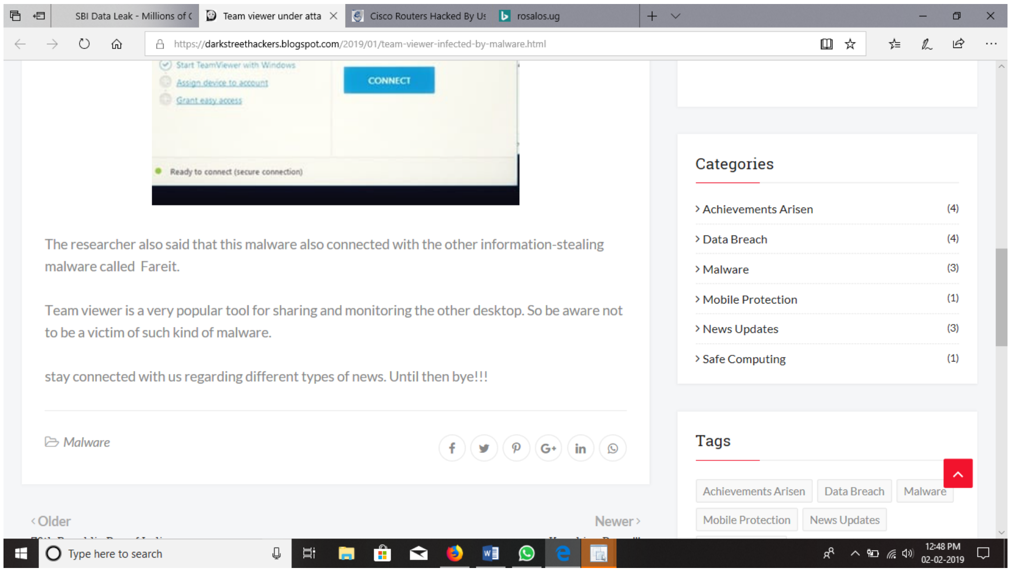
Always keep your patch levels up-to-date, especially on computers that host public services and are accessible through the firewall, such as HTTP, FTP, mail, and DNS services.

Configure your email server to block or remove email that contains file attachments that are commonly used to spread threats, such as .vbs, .bat, .exe, .pif and .scr files.

Isolate compromised computers quickly to prevent threats from spreading further. Perform a forensic analysis and restore the computers using trusted media.

Train employees not to open attachments unless they are expecting them. Also, do not execute software that is downloaded from Internet unless it has been scanned for compromised Website can cause infection if certain browser vulnerabilities are not patched.

If Bluetooth is not required for mobile devices, it should be turned off. If you require its use, ensure that the device’s visibility is set to “Hidden” so that it cannot be scanned by other Bluetooth devices. If device pairing must be used, ensure that all devices are set to “Unauthorized”, requiring authorization for each connection request. Do not accept applications that are unsigned or sent from unknown sources.


SBI Data Leak - Millions of (
Team viewer under atta
Cisco Routers Hacked By Us
rosalos.ug
https://darkstreethackers.blogspot.com/2019/01/team-viewer-infected-by-malware.html
Start TeamViewer with Windows
Assign device to account
Grant easy access
CONNECT
Ready to connect (secure connection)

The researcher also said that this malware also connected with the other information-stealing malware called Fareit.

Team viewer is a very popular tool for sharing and monitoring the other desktop. So be aware not to be a victim of such kind of malware.

stay connected with us regarding different types of news. Until then bye!!!

Malware

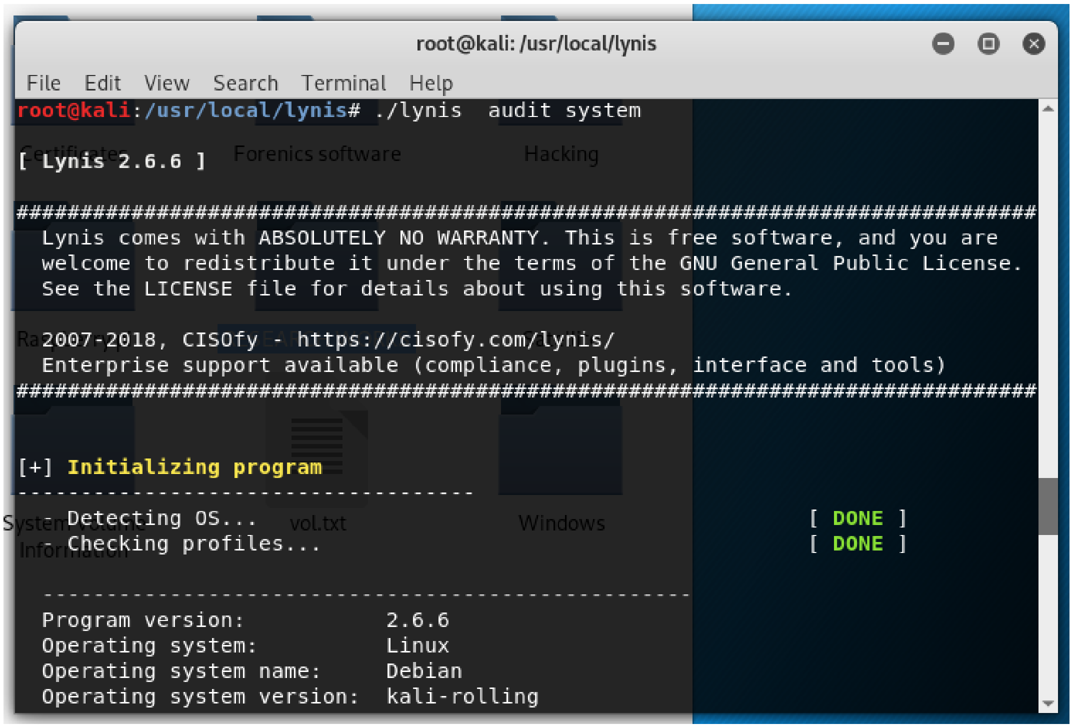
Categories

› Achievements Arisen	(4)
› Data Breach	(4)
› Malware	(3)
› Mobile Protection	(1)
› News Updates	(3)
› Safe Computing	(1)

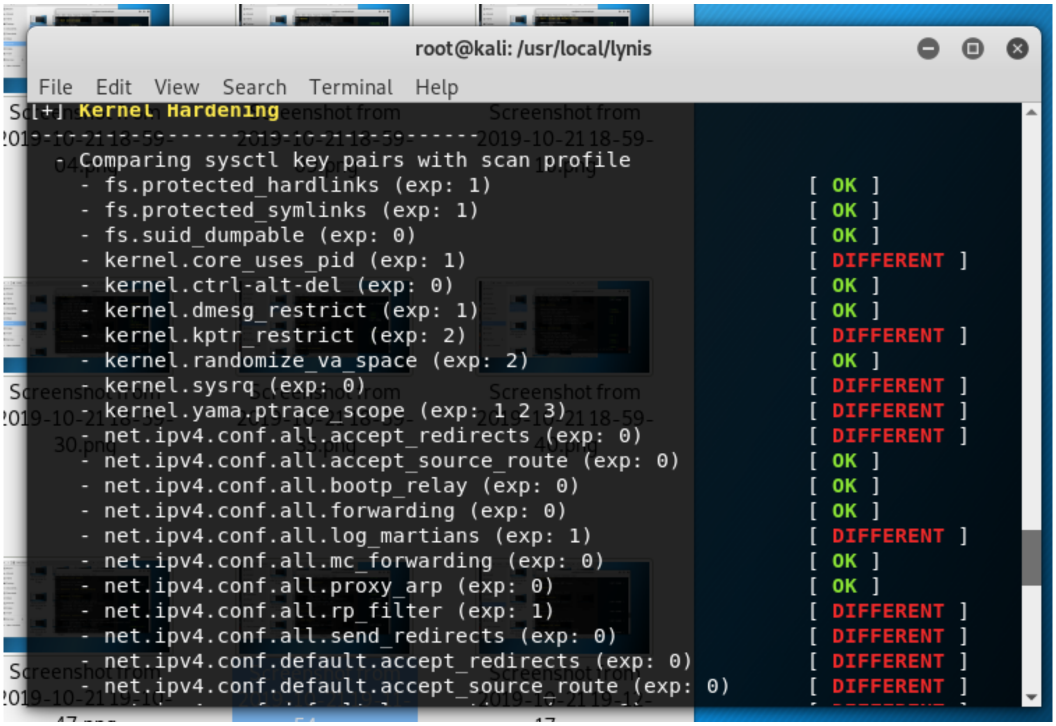
Tags

Achievements Arisen Data Breach Malware Mobile Protection News Updates

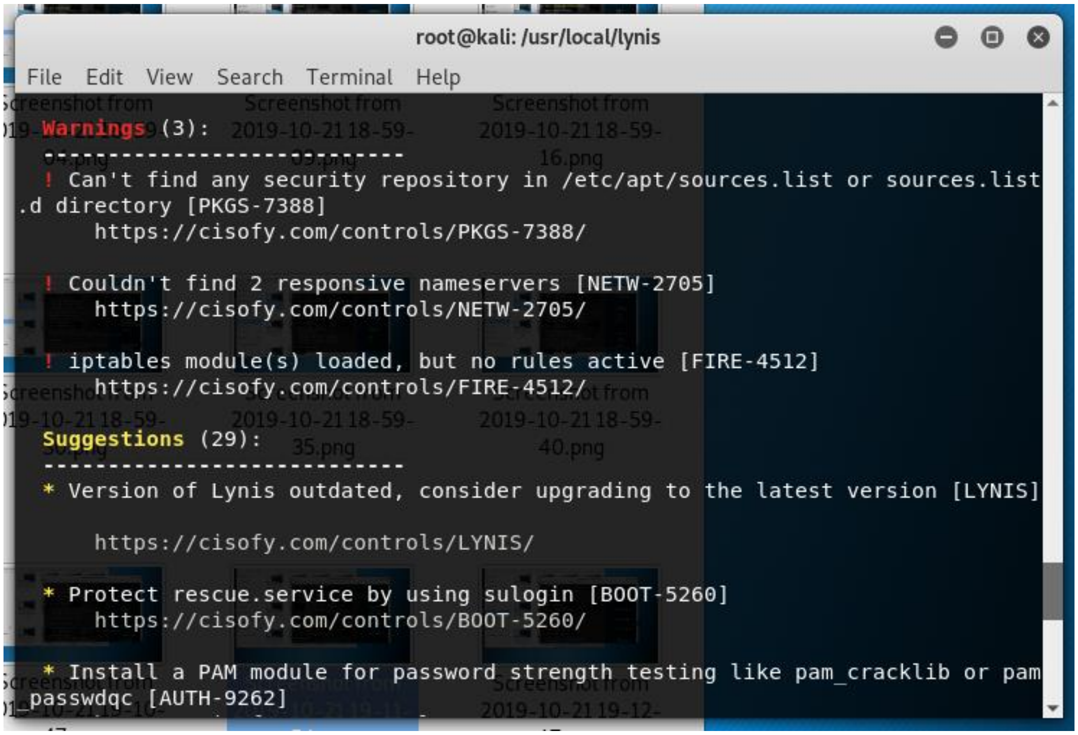
Proof of Content Fareit found in Team viewer :- https://darkstreethackers.blogspot.com/2019/01/team-viewer-infected-by-malware.html



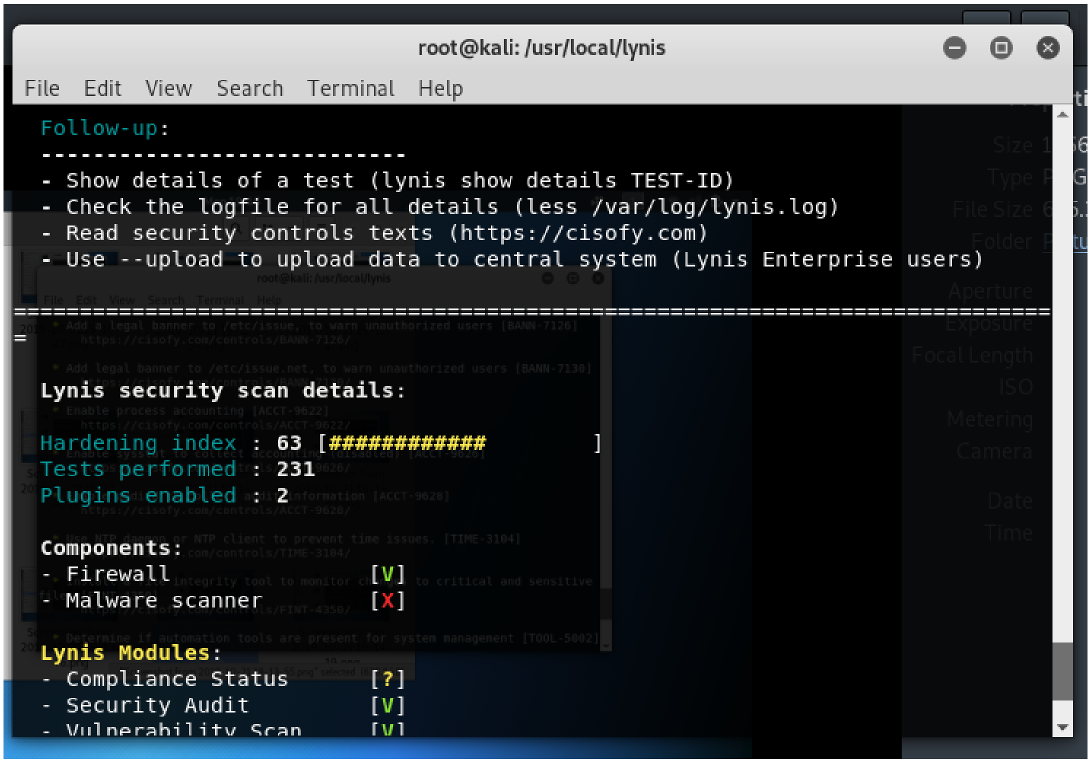
```
root@kali:/usr/local/lynis# ./lynis  audit system

[ Lynis 2.6.6 ]

################################################################################
  Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
  welcome to redistribute it under the terms of the GNU General Public License.
  See the LICENSE file for details about using this software.

  2007-2018, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)
################################################################################


[+] Initializing program
------------------------------------
  - Detecting OS...                                           [ DONE ]
  - Checking profiles...                                      [ DONE ]

  ---------------------------------------------------
  Program version:           2.6.6
  Operating system:          Linux
  Operating system name:     Debian
  Operating system version:  kali-rolling
```



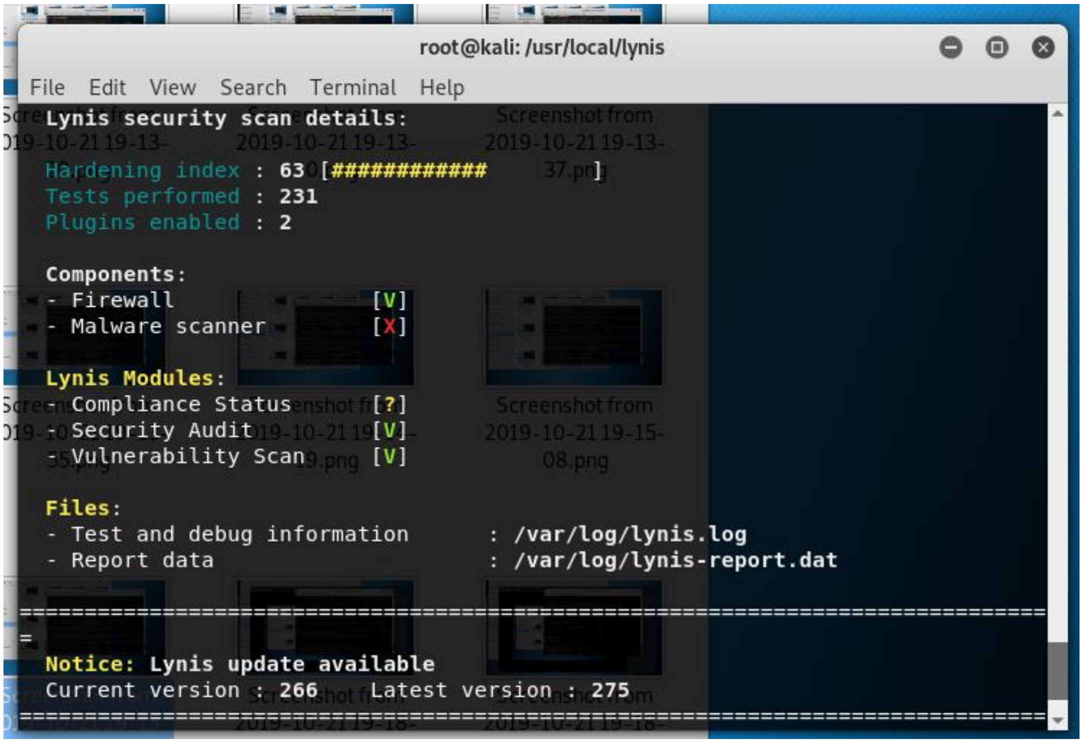
```
[+] Kernel Hardening
------------------------------------
  - Comparing sysctl key pairs with scan profile
    - fs.protected_hardlinks (exp: 1)                         [ OK ]
    - fs.protected_symlinks (exp: 1)                          [ OK ]
    - fs.suid_dumpable (exp: 0)                               [ OK ]
    - kernel.core_uses_pid (exp: 1)                           [ DIFFERENT ]
    - kernel.ctrl-alt-del (exp: 0)                            [ OK ]
    - kernel.dmesg_restrict (exp: 1)                          [ OK ]
    - kernel.kptr_restrict (exp: 2)                           [ DIFFERENT ]
    - kernel.randomize_va_space (exp: 2)                      [ OK ]
    - kernel.sysrq (exp: 0)                                   [ DIFFERENT ]
    - kernel.yama.ptrace_scope (exp: 1 2 3)                   [ DIFFERENT ]
    - net.ipv4.conf.all.accept_redirects (exp: 0)             [ DIFFERENT ]
    - net.ipv4.conf.all.accept_source_route (exp: 0)          [ OK ]
    - net.ipv4.conf.all.bootp_relay (exp: 0)                  [ OK ]
    - net.ipv4.conf.all.forwarding (exp: 0)                   [ OK ]
    - net.ipv4.conf.all.log_martians (exp: 1)                 [ DIFFERENT ]
    - net.ipv4.conf.all.mc_forwarding (exp: 0)                [ OK ]
    - net.ipv4.conf.all.proxy_arp (exp: 0)                    [ OK ]
    - net.ipv4.conf.all.rp_filter (exp: 1)                    [ DIFFERENT ]
    - net.ipv4.conf.all.send_redirects (exp: 0)               [ DIFFERENT ]
    - net.ipv4.conf.default.accept_redirects (exp: 0)         [ DIFFERENT ]
    - net.ipv4.conf.default.accept_source_route (exp: 0)      [ DIFFERENT ]
```


root@kali: /usr/local/lynis
File Edit View Search Terminal Help

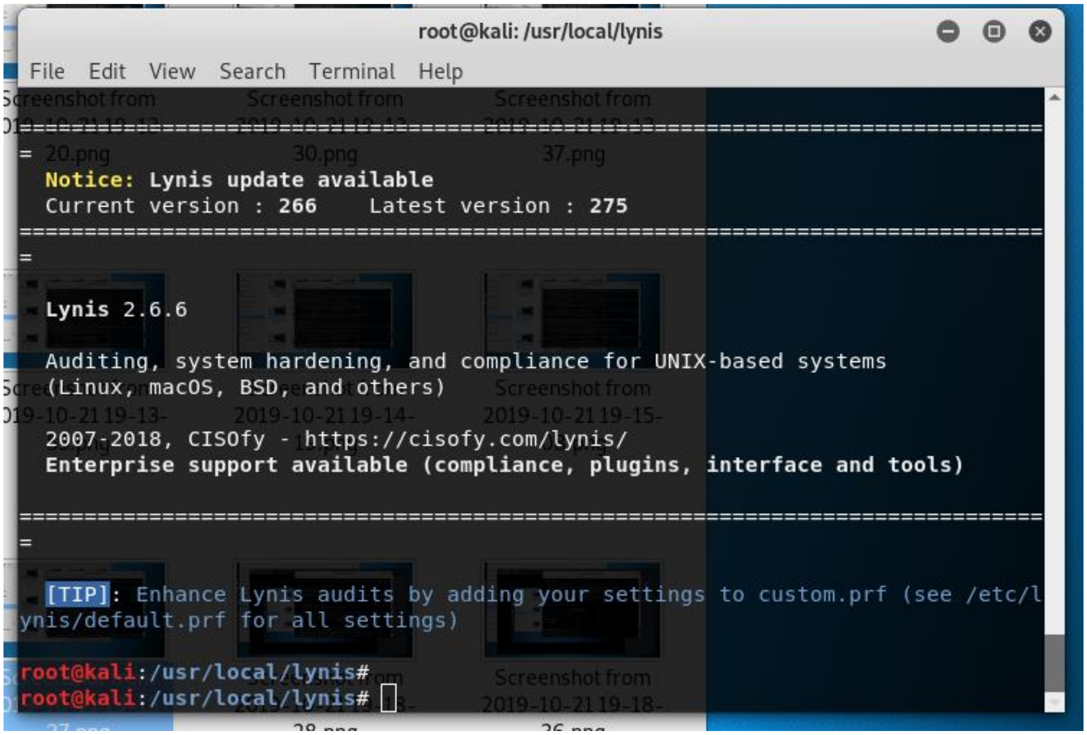
```
  Warnings (3):
  ----------------------------
  ! Can't find any security repository in /etc/apt/sources.list or sources.list
.d directory [PKGS-7388]
      https://cisofy.com/controls/PKGS-7388/

  ! Couldn't find 2 responsive nameservers [NETW-2705]
      https://cisofy.com/controls/NETW-2705/

  ! iptables module(s) loaded, but no rules active [FIRE-4512]
      https://cisofy.com/controls/FIRE-4512/

  Suggestions (29):
  ----------------------------
  * Version of Lynis outdated, consider upgrading to the latest version [LYNIS]

      https://cisofy.com/controls/LYNIS/

  * Protect rescue.service by using sulogin [BOOT-5260]
      https://cisofy.com/controls/BOOT-5260/

  * Install a PAM module for password strength testing like pam_cracklib or pam
_passwdqc [AUTH-9262]
```


root@kali: /usr/local/lynis
File Edit View Search Terminal Help

```
  Follow-up:
  ----------------------------
  - Show details of a test (lynis show details TEST-ID)
  - Check the logfile for all details (less /var/log/lynis.log)
  - Read security controls texts (https://cisofy.com)
  - Use --upload to upload data to central system (Lynis Enterprise users)

================================================================================
=

  Lynis security scan details:

  Hardening index : 63 [############         ]
  Tests performed : 231
  Plugins enabled : 2

  Components:
  - Firewall               [V]
  - Malware scanner        [X]

  Lynis Modules:
  - Compliance Status      [?]
  - Security Audit         [V]
  - Vulnerability Scan     [V]
```


root@kali: /usr/local/lynis
File Edit View Search Terminal Help

```
  Lynis security scan details:

  Hardening index : 63 [############        ]
  Tests performed : 231
  Plugins enabled : 2

  Components:
  - Firewall               [V]
  - Malware scanner        [X]

  Lynis Modules:
  - Compliance Status      [?]
  - Security Audit         [V]
  - Vulnerability Scan     [V]

  Files:
  - Test and debug information      : /var/log/lynis.log
  - Report data                     : /var/log/lynis-report.dat

================================================================================
=

  Notice: Lynis update available
  Current version : 266    Latest version : 275

================================================================================
```


root@kali: /usr/local/lynis
File Edit View Search Terminal Help

```
================================================================================
=
  Notice: Lynis update available
  Current version : 266    Latest version : 275
================================================================================
=


  Lynis 2.6.6

  Auditing, system hardening, and compliance for UNIX-based systems
  (Linux, macOS, BSD, and others)

  2007-2018, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)

================================================================================
=

  [TIP]: Enhance Lynis audits by adding your settings to custom.prf (see /etc/l
ynis/default.prf for all settings)

root@kali:/usr/local/lynis#
root@kali:/usr/local/lynis# 
```

Tool Lynis usage photo.

Conclusion: -

The experimental process concludes that in order to detect the malware in memory is so difficult and a long process which take much time. Virus making tools and binding tools are used if we want to make it on own. Remote Access Tools are used to send it remotely to someone's PC without using USB.

First process starts with AccessData Forensic Toolkit or Magnet Ram Capture after antivirus detect malware which is found in internet content downloaded or by external decive. This software make dumps of memory. Hex Editor or Forensic Toolkit is used to view content of it.

Second process started with Lynis (routine-software) which scans hole system. To generate a result of malware detected in volatile memory.

Third stage to protect PC from this kind of malware which steals user's data are solved by possible solution shown.

Reference: -

Practical Cloud Security a Guide for Secure Design and Deployment by: - Chris Doston

Linux Basics for Hackers: Getting Started with Networking, Scripting, and Security in Kali By :- OccupyThe Web

Cyber Forensics By :- Dejey, Murugan

Computer Forensics and Cyber Crime: An Introduction, 2e By :- Britz

https://cisofy.com/lynis : - Lynis

https://accessdata.com/products-services/forensic-toolkit-ftk :- AccessData Forensic Toolkit

https://www.magnetforensics.com/resources/magnet-ram-capture :- Magnet Ram Capture

https://www.hhdsoftware.com/free-hex-editor :- Hex Editor

https://searchnetworking.techtarget.com/feature/Most-popular-viruses-and-hacking-tools :- Virus Making Tools

https://docs.oracle.com/cd/E19120-02/open.solaris/819-3194/dnsref-9/index.html :- Binding File Tools

https://gisgeography.com/open-source-remote-sensing-software-packages :- Remote Access Tools

https://darkstreethackers.blogspot.com/2019/01/team-viewer-infected-by-malware.html :- Proof of Content Fareit found in Team viewer.