PROJECT WORK ON CYBER SECURITY & ETHICAL HACKING

TRAINING PROGRAM OFFERED BY INMOVIDU TECHNOLOGIES LTD.

(IN COLLABORATION WITH **IIT-BOMBAY**)

PROJECT DETAILS

- NAME : GUDENA ASHISH
- E-mail ID : ashishgudena@gmail.com
- Mobile Number : +91 9390414807
- Training Program(Domain) : Cyber Security & Ethical Hacking
- Instructor :Varun Pathak

TASKS

- VULNERABILITY ASSESSMENTS
  - Perform a VA on testphp.vulnweb.com
  - Perform a VA on host machine/virtual machine
  - Prepare a Customized Report of both VA
- PASSWORD CRACKING
  - Find password of username hidden in following directory www.varunpathak.in/m1ss10n.zip
- STEGANOGRAPHY
  - Find a way to hide a video behind an image and run it

TASK-1

VULNERABILITY ASSESSMENTS

SECURITY TESTING (OVERVIEW)

- Motto :-

  To identify security issues that can be exploited to escalated privileges.

- Procedure :-

  Perform an external vulnerability assessment, using an automatic scanner.

- Report :-

  During assessment, we found that there are manifold threats and vulnerabilities in the given website(testphp.vulnweb.com) & host machine(Windows-10).

APPROACH

i. Performed expansive scan to assess systems/applications

ii. Performed target scan and manual investigation

iii. Ranked the vulnerabilities based on the threat level

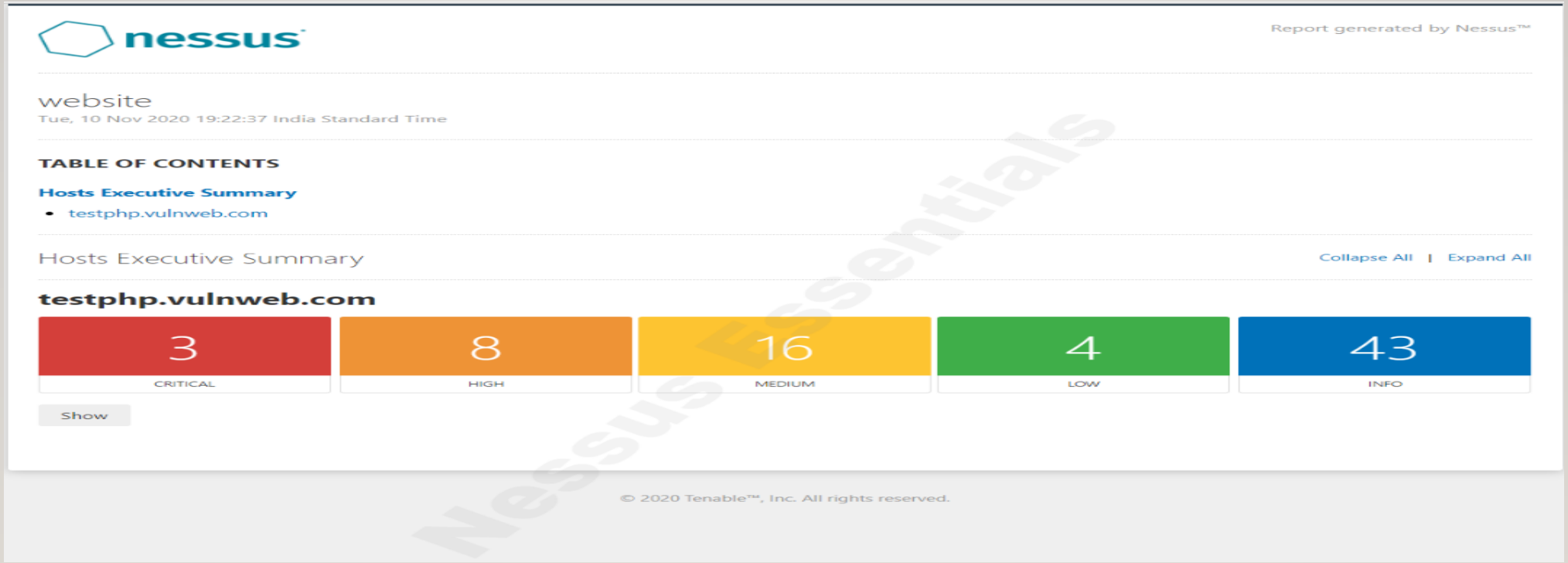
iv. The recommended remedies for the issues are identified

v. Communicated the whole scenario through this report

RISK (DEFINITION)

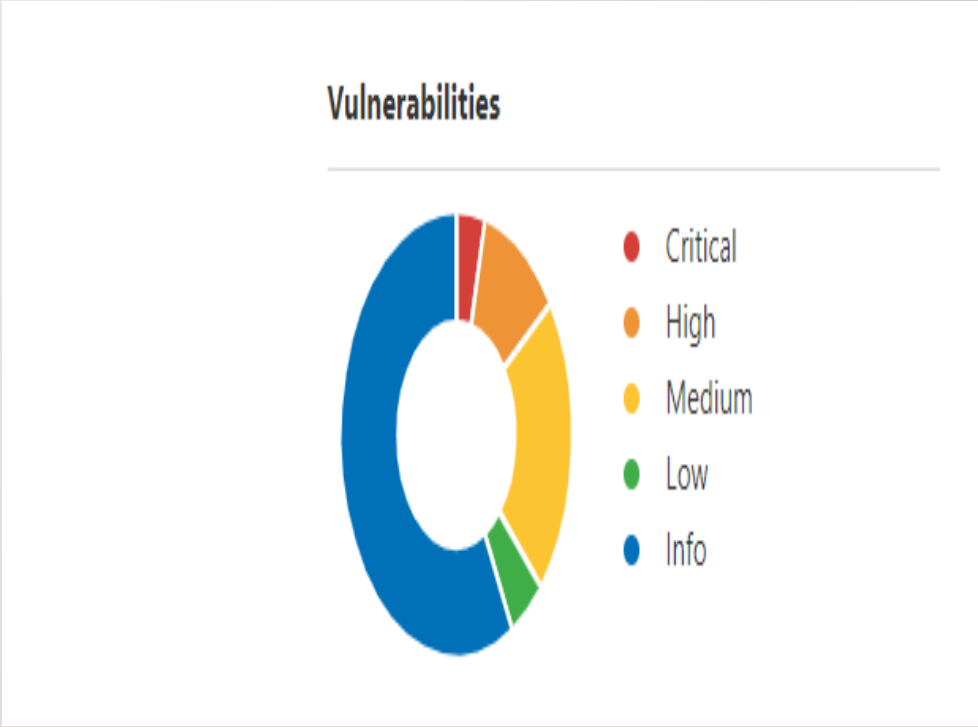
High Risk	Weakness in controls that represent exposure to the organization or risks that could seriously compromise the control framework, data integrity and / or operational efficiency. These risks need to be addressed with utmost priority.
Medium Risk	Potential weakness in controls, which could develop into an exposure. Or Issues that represent areas of concern and may impact controls. They should be addressed reasonably promptly.
Low Risk	Potential weaknesses in controls, which in combination with other weaknesses can develop into exposure. Suggested improvements not immediately/directly affecting controls.

VULNERABILITY ASSESSMENT (WEBSITE)



RISK
(IN %)

1) Critical = 1.75
2) High = 5.85
3) Medium = 30.99
4) Low = 2.34
5) Info =59.06



UNIX OPERATING SYSTEM (UNSUPPORTED VERSION DETECTION)

- **Risk Factor :-** Critical
- **Description :-** According to its self-reported version number, the Unix operating system running on the remote host is no longer supported.
- **Impact :-** Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.
- **Solution :-**Upgrade to a version of the Unix operating system that is currently supported.

PHP (UNSUPPORTED VERSION DETECTION)

- **Risk Factor :-** Critical
- **Description :-** According to its version, the installation of PHP on the remote host is no longer supported.
- **Impact :-** Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.
- **Solution :-** Upgrade to a version of PHP that is currently supported.

PHP 5.3.X < 5.3.15 (MULTIPLE VULNERABILITIES)

- **Risk Factor :-** Critical
- **Description :-** According to its banner, the version of PHP installed on the remote host is 5.3.x earlier than 5.3.15.
- **Impact :-** Potentially affected by the following vulnerabilities;

- An unspecified overflow vulnerability exists in the function '_php_stream_scandir' in the file 'main/streams/streams.c'. (CVE-2012-2688)

- An unspecified error exists that can allow the 'open_basedir' constraint to be bypassed. (CVE-2012-3365)

- **Solution :-** Upgrade to PHP version 5.3.15 or later.

PHP < 5.3.12 / 5.4.2 (CGI QUERY STRING CODE EXECUTION)

- **Risk Factor :-** High
- **Description :-**According to its banner, the version of PHP installed on the remote host is earlier than 5.3.12 / 5.4.2, and as such is potentially affected by a remote code execution and information disclosure vulnerability.
- **Impact :-** An error in the file 'sapi/cgi/cgi_main.c' can allow a remote attacker to obtain PHP source code from the web server or to potentially execute arbitrary code. In vulnerable configurations, PHP treats certain query string parameters as command line arguments including switches such as '-s', '-d', and '-c'.

  (NOTE : This vulnerability is exploitable only when PHP is used in CGI-based configurations. Apache with 'mod_php' is not an exploitable configuration.)
- **Solution :-** Upgrade to PHP version 5.3.12 / 5.4.2 or later. A 'mod_rewrite' workaround is available as well.

PHP 5.3.X < 5.3.13 (CGI QUERY STRING CODE EXECUTION)

- **Risk Factor :-** High
- **Description :-** According to its banner, the version of PHP installed on the remote host is 5.3.x earlier than 5.3.13 and, as such, is potentially affected by a remote code execution and information disclosure vulnerability.
- **Impact :-** The fix for CVE-2012-1823 does not completely correct the CGI query vulnerability. Disclosure of PHP source code and code execution via query parameters are still possible.

  (NOTE : This vulnerability is exploitable only when PHP is used in CGI-based configurations. Apache with 'mod_php' is not an exploitable configuration.)
- **Solution :-**Upgrade to PHP version 5.3.13 or later. A 'mod_rewrite' workaround is available as well.

PHP 5.3.X < 5.3.14 (MULTIPLE VULNERABILITIES)

- **Risk factor :-** High
- **Description :-** According to its banner, the version of PHP installed on the remote host is 5.3.x earlier than 5.3.14.
- **Impact :-** Potentially affected by the following vulnerabilities;

  - An integer overflow error exists in the function 'phar_parse_tarfile' in the file 'ext/phar/tar.c'. This error can lead to a heap-based buffer overflow when handling a maliciously crafted TAR file. Arbitrary code execution is possible due to this error. (CVE-2012-2386)

  - A weakness exists in the 'crypt' function related to the DES implementation that can allow brute-force attacks. (CVE-2012-2143)

  - Several design errors involving the incorrect parsing of PHP PDO prepared statements could lead to disclosure of sensitive information or denial of service.
  (CVE-2012-3450)

  - A variable initialization error exists in the file 'ext/openssl/openssl.c' that can allow process memory contents to be disclosed when input data is of length zero. (CVE-2012-6113)

- **Solution :-** Upgrade to PHP version 5.3.14 or later.

PHP 5.3.X < 5.3.22 (MULTIPLE VULNERABILITIES)

- **Risk Factor :-** High
- **Description :-**According to its banner, the version of PHP 5.3.x installed on the remote host is prior to 5.3.22.
- **Impact :-** Potentially affected by the following vulnerabilities;
  -An error exists in the file 'ext/soap/soap.c' related to the 'soap.wsdl_cache_dir' configuration directive and writing cache files that could allow remote 'wsdl' files to be written to arbitrary locations. (CVE-2013-1635)

  - An error exists in the file 'ext/soap/php_xml.c' related to parsing SOAP 'wsdl' files and external entities that could cause PHP to parse remote XML documents defined by an attacker. This could allow access to arbitrary files. (CVE-2013-1643)

  (NOTE : This plugin does not attempt to exploit the vulnerabilities but, instead relies only on PHP's self-reported version number.)
- **Solution :-** Upgrade to PHP version 5.3.22 or later.

PHP 5.3.X < 5.3.23 (MULTIPLE VULNERABILITIES)

- **Risk Factor :-** High
- **Description :-** According to its banner, the version of PHP 5.3.x installed on the remote host is prior to 5.3.23.
- **Impact :-** Potentially affected by the following vulnerabilities;
  - An error exists in the file 'ext/soap/soap.c' related to the 'soap.wsdl_cache_dir' configuration directive and writing cache files that could allow remote 'wsdl' files to be written to arbitrary locations. (CVE-2013-1635)

  - An error exists in the file 'ext/soap/php_xml.c' related to parsing SOAP 'wsdl' files and external entities that could cause PHP to parse remote XML documents defined by an attacker. This could allow access to arbitrary files. (CVE-2013-1643)

  - An information disclosure in the file 'ext/soap/php_xml.c' related to parsing SOAP 'wsdl' files and external entities that could cause PHP to parse remote XML documents defined by an attacker. This could allow access to arbitrary files. (CVE-2013-1824)

  (NOTE : This plugin does not attempt to exploit the vulnerability, but instead relies only on PHP's self-reported version number.)
- **Solution :-** Upgrade to PHP version 5.3.23 or later.

PHP 5.3.X < 5.3.28 (MULTIPLE OPENSSL VULNERABILITIES)

- **Risk Factor :-** High
- **Description :-** According to its banner, the version of PHP installed on the remote host is 5.3.x prior to 5.3.28.
- **Impact :-** Potentially affected by the following vulnerabilities;
  - A flaw exists in the PHP OpenSSL extension's hostname identity check when handling certificates that contain hostnames with NULL bytes. An attacker could potentially exploit this flaw to conduct man-in-the-middle attacks to spoof SSL servers. Note that to exploit this issue, an attacker would need to obtain a carefully-crafted certificate signed by an authority that the client trusts. (CVE-2013-4073, CVE-2013-4248)

  - A memory corruption flaw exists in the way the openssl_x509_parse() function of the PHP OpenSSL extension parsed X.509 certificates. A remote attacker could use this flaw to provide a malicious, self-signed certificate or a certificate signed by a trusted authority to a PHP application using the aforementioned function. This could cause the application to crash or possibly allow the attacker to execute arbitrary code with the privileges of the user running the PHP interpreter. (CVE-2013-6420)

  (NOTE : This plugin does not attempt to exploit these vulnerabilities, but instead relies only on PHP's self-reported version number.)
- **Solution :-** Upgrade to PHP version 5.3.28 or later.

PHP 5.3.X < 5.3.29 (MULTIPLE VULNERABILITIES)

- **Risk Factor :-** High
- **Description :-** According to its banner, the version of PHP installed on the remote host is 5.3.x prior to 5.3.29.
- **Impact :-** Potentially affected by the following vulnerabilities;
  - A heap-based buffer overflow error exists in the file 'ext/date/lib/parse_iso_intervals.c' related to handling DateInterval objects that allows denial of service attacks. (CVE-2013-6712)

  - A boundary checking error exists related to the Fileinfo extension, Composite Document Format (CDF) handling, and the function 'cdf_read_short_sector'. (CVE-2014-0207)

  - A flaw exists with the 'cdf_unpack_summary_info()' function within 'src/cdf.c' where multiple file_printf calls occur when handling specially crafted CDF files.
  This could allow a context dependent attacker to crash the web application using PHP. (CVE-2014-0237)

  - A flaw exists with the 'cdf_read_property_info()' function within 'src/cdf.c' where an infinite loop occurs when handling specially crafted CDF files. This could allow a context dependent attacker to crash the web application using PHP. (CVE-2014-0238)

  - A type-confusion error exists related to the Standard PHP Library (SPL) extension and the function 'unserialize'. (CVE-2014-3515)

  - An error exists related to configuration scripts and temporary file handling that could allow insecure file usage. (CVE-2014-3981)

  - A heap-based buffer overflow error exists related to the function 'dns_get_record' that could allow execution of arbitrary code. (CVE-2014-4049)

  - An out-of-bounds read exists in printf. (Bug #67249)

  Note that Nessus has not attempted to exploit these issues, but has instead relied only on the application's self-reported version number.

  Additionally, note that version 5.3.29 marks the end of support for the PHP 5.3.x branch.
- **Solution :-** Upgrade to PHP version 5.3.29 or later.

SSL (VERSION 2 AND 3 PROTOCOL DETECTION)

- **Risk Factor :-** High
- **Description :-** The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0.
- **Impact :-** These versions of SSL are affected by several cryptographic flaws, including;

  - An insecure padding scheme with CBC ciphers.

  - Insecure session renegotiation and resumption schemes.

  An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

  Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.

  NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

- **Solution :-** Consult the application's documentation to disable SSL 2.0 and 3.0.

  Use TLS 1.2 (with approved cipher suites) or higher instead.

PHP < 5.3.11 (MULTIPLE VULNERABILITIES)

- **Risk Factor :-** Medium
- **Description :-** According to its banner, the version of PHP installed on the remote host is earlier than 5.3.11.
- **Impact :-** Potentially affected by the following vulnerabilities :

  - During the import of environment variables, temporary changes to the 'magic_quotes_gpc' directive are not handled properly. This can lower the difficulty for SQL injection attacks. (CVE-2012-0831)

  - The '$_FILES' variable can be corrupted because the names of uploaded files are not properly validated. (CVE-2012-1172)

  - The 'open_basedir' directive is not properly handled by the functions 'readline_write_history' and 'readline_read_history'.

  - The 'header()' function does not detect multi-line headers with a CR. (Bug #60227 / CVE-2011-1398)

- **Solution :-** Upgrade to PHP version 5.3.11 or later.

PHP 5.3.X < 5.3.26 (MULTIPLE VULNERABILITIES)

- **Risk Factor :-** Medium
- **Description :-** According to its banner, the version of PHP 5.3.x installed on the remote host is prior to 5.3.26.
- **Impact :-** Potentially affected by the following vulnerabilities:

  - An error exists in the function 'php_quot_print_encode' in the file 'ext/standard/quot_print.c' that could allow a heap-based buffer overflow when attempting to parse certain strings (Bug #64879)

  - An integer overflow error exists related to the value of 'JEWISH_SDN_MAX' in the file 'ext/calendar/jewish.c' that could allow denial of service attacks. (Bug #64895)

  (NOTE : This plugin does not attempt to exploit these vulnerabilities, but instead relies only on PHP's self-reported version number.)
- **Solution :-** Apply the vendor patch or upgrade to PHP version 5.3.26 or later.

PHP 5.3.X < 5.3.27 (MULTIPLE VULNERABILITIES)

- **Risk Factor :-** Medium
- **Description :-** According to its banner, the version of PHP 5.3.x installed on the remote host is prior to 5.3.27.
- **Impact :-** Potentially affected by the following vulnerabilities:

  - A buffer overflow error exists in the function '_pdo_pgsql_error'. (Bug #64949)

  - A heap corruption error exists in numerous functions in the file 'ext/xml/xml.c'. (CVE-2013-4113 / Bug #65236)

  (NOTE : This plugin does not attempt to exploit these vulnerabilities, but instead relies only on PHP's self-reported version number.)
- **Solution :-** Apply the vendor patch or upgrade to PHP version 5.3.27 or later.

PHP PHP_RSHUTDOWN_FUNCTION (SECURITY BYPASS)

- **Risk Factor :-** Medium
- **Description :-** According to its banner, the version of PHP 5.x installed on the remote host is 5.x prior to 5.3.11 or 5.4.x prior to 5.4.1.
- **Impact :-** Potentially affected by a security bypass vulnerability.

  An error exists related to the function 'PHP_RSHUTDOWN_FUNCTION' in the libxml extension and the 'stream_close' method that could allow a remote attacker to bypass 'open_basedir' protections and obtain sensitive information.

  (NOTE : This plugin has not attempted to exploit this issue, but has instead relied only on PHP's self-reported version number.)
- **Solution :-** Upgrade to PHP version 5.3.11 / 5.4.1 or later.

SSL (CERTIFICATE CANNOT BE TRUSTED)

- **Risk Factor :-** Medium
- **Description :-** The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

  - First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

  - Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

  - Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.
- **Impact :-** If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.
- **Solution :-** Purchase or generate a proper SSL certificate for this service.

SSL (CERTIFICATE EXPIRY)

- **Risk Factor :-** Medium
- **Description :-** This plugin checks expiry dates of certificates associated with SSL-enabled services on the target and reports whether any have already expired.
- **Impact :-** Possibility for Man-in-the-middle attacks.
- **Solution :-** Purchase or generate a new SSL certificate to replace the existing one.

SSL (CERTIFICATE WITH WRONG HOSTNAME)

- **Risk Factor :-** Medium
- **Description :-** The 'commonName' (CN) attribute of the SSL certificate presented for this service is for a different machine.
- **Impact :-** Possibility for improper authentication.
- **Solution :-** Purchase or generate a proper SSL certificate for this service.

SSL
(MEDIUM STRENGTH CIPHER SUITES SUPPORTED (SWEET32))

- **Risk Factor :-** Medium
- **Description :-** The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.
- **Impact :-** It is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.
- **Solution :-** Reconfigure the affected application if possible to avoid use of medium strength ciphers.

SSL
(RC4 CIPHER SUITES SUPPORTED (BAR MITZVAH))

- **Risk Factor :-** Medium
- **Description :-** The remote host supports the use of RC4 in one or more cipher suites. The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.
- **Impact :-** If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.
- **Solution :-** Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

SSL (SELF-SIGNED CERTIFICATE)

- **Risk Factor :-** Medium
- **Description :-** The X.509 certificate chain for this service is not signed by a recognized certificate authority.
- **Impact :-** If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.
  (NOTE : This plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.)
- **Solution :-** Purchase or generate a proper SSL certificate for this service.

SSL
(WEAK CIPHER SUITES SUPPORTED)

- **Risk Factor :-** Medium
- **Description :-** The remote host supports the use of SSL ciphers that offer weak encryption.
- **Impact :-** This is considerably easier to exploit if the attacker is on the same physical network.
- **Solution :-** Reconfigure the affected application, if possible to avoid the use of weak ciphers.

SSLV3 (POODLE VULNERABILITY)

- **Risk Factor :-** Medium
- **Description :-** The remote host is affected by a man-in-the-middle (MitM) information disclosure vulnerability known as POODLE. The vulnerability is due to the way SSL 3.0 handles padding bytes when decrypting messages encrypted using block ciphers in cipher block chaining (CBC) mode.
  MitM attackers can decrypt a selected byte of a cipher text in as few as 256 tries if they are able to force a victim application to repeatedly send the same data over newly created SSL 3.0 connections.

  As long as a client and service both support SSLv3, a connection can be 'rolled back' to SSLv3, even if TLSv1 or newer is supported by the client and service.

  The TLS Fallback SCSV mechanism prevents 'version rollback' attacks without impacting legacy clients; however, it can only protect connections when the client and service support the mechanism. Sites that cannot disable SSLv3 immediately should enable this mechanism.

  This is a vulnerability in the SSLv3 specification, not in any particular SSL implementation. Disabling SSLv3 is the only way to completely mitigate the vulnerability.
- **Impact :-** Padding Oracle On Downgraded Legacy Encryption(POODLE) vulnerability can led to man-in-the-middle attacks.
- **Solution :-** Disable SSLv3.

  Services that must support SSLv3 should enable the TLS Fallback SCSV mechanism until SSLv3 can be disabled.

TLS (VERSION 1.0 PROTOCOL DETECTION)

- **Risk Factor :-** Medium
- **Description :-** The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.

  As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

  PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.
- **Impact :-** Possibility of external threats & attacks.
- **Solution :-** Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

SSL/TLS EXPORT_RSA <= 512-BIT (CIPHER SUITES SUPPORTED (FREAK))

- **Risk Factor :-** Medium
- **Description :-** The remote host supports EXPORT_RSA cipher suites with keys less than or equal to 512 bits. An attacker can factor a 512-bit RSA modulus in a short amount of time.
- **Impact :-** A man-in-the middle attacker may be able to downgrade the session to use EXPORT_RSA cipher suites (e.g. CVE-2015-0204). Thus, it is recommended to remove support for weak cipher suites.
- **Solution :-** Reconfigure the service to remove support for EXPORT_RSA cipher suites.

SSH
(WEAK ALGORITHMS SUPPORTED)

- **Risk Factor :-** Medium
- **Description :-** It has detected that the remote SSH server is configured to use the Arcfour stream cipher or no cipher at all. RFC 4253 advises against using Arcfour due to an issue with weak keys.
- **Impact :-** Possibility of threats and attacks.
- **Solution :-** Contact the vendor or consult product documentation to remove the weak ciphers.

SSL (DROWN ATTACK VULNERABILITY)

- **Risk Factor :-** Medium
- **Description :-** The remote host supports SSLv2 and therefore may be affected by a vulnerability that allows a cross-protocol Bleichenbacher padding oracle attack known as DROWN (Decrypting RSA with Obsolete and Weakened eNcryption). This vulnerability exists due to a flaw in the Secure Sockets Layer Version 2 (SSLv2) implementation, and it allows captured TLS traffic to be decrypted.
- **Impact :-** A man-in-the-middle attacker can exploit this to decrypt the TLS connection by utilizing previously captured traffic and weak cryptography along with a series of specially crafted connections to an SSLv2 server that uses the same private key.
- **Solution :-** Disable SSLv2 and export grade cryptography cipher suites. Ensure that private keys are not used anywhere with server software that supports SSLv2 connections

SSL
(ANONYMOUS CIPHER SUITES SUPPORTED)

- **Risk Factor :-** Low
- **Description :-** The remote host supports the use of anonymous SSL ciphers.
- **Impact :-** While this enables an administrator to set up a service that encrypts traffic without having to generate and configure SSL certificates, it offers no way to verify the remote host's identity and renders the service vulnerable to a man-in-the-middle attack.

  (Note: This is considerably easier to exploit if the attacker is on the same physical network.)
- **Solution :-** Reconfigure the affected application if possible to avoid use of weak ciphers.

SSH
(SERVER CBC MODE CIPHERS ENABLED)

- **Risk Factor :-** Low
- **Description :-** The SSH server is configured to support Cipher Block Chaining (CBC) encryption.
- **Impact :-** This may allow an attacker to recover the plaintext message from the ciphertext.

  (NOTE : his plugin only checks for the options of the SSH server and does not check for vulnerable software versions.)
- **Solution :-** Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption.

SSH
(WEAK MAC ALGORITHMS ENABLED)

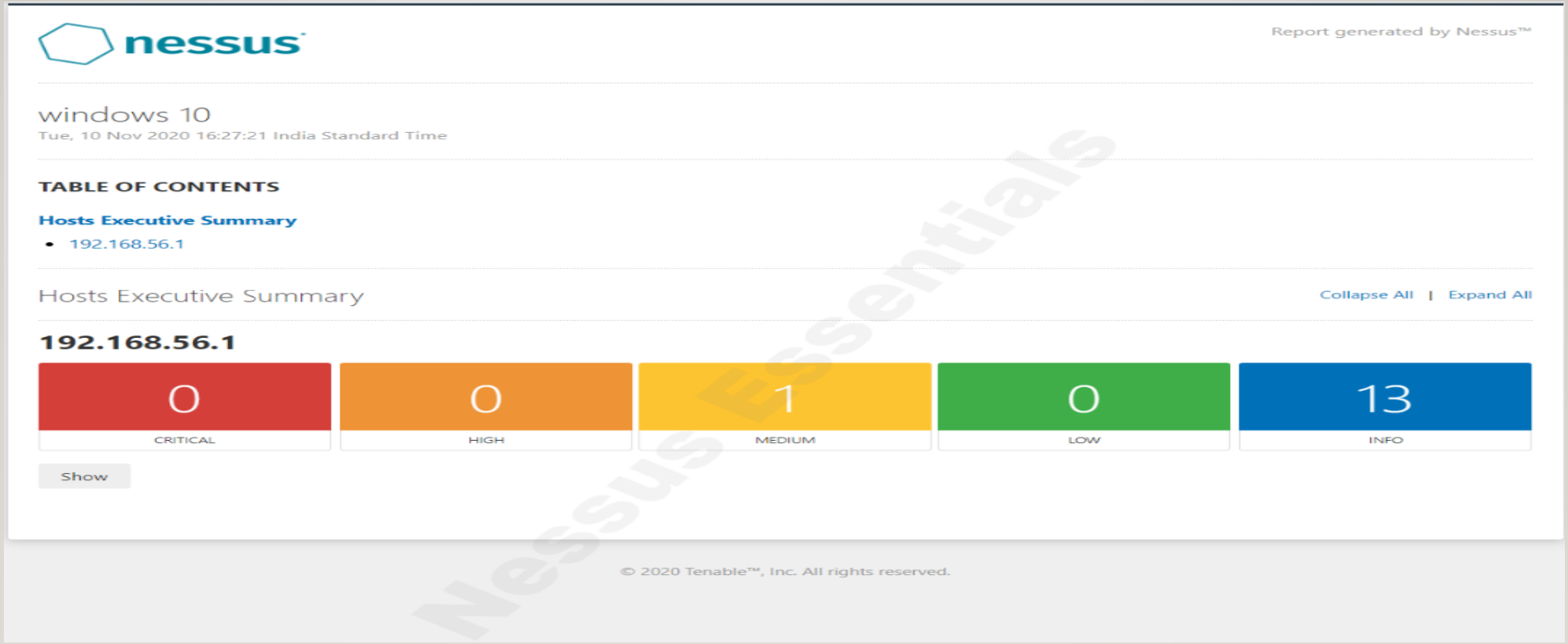
- **Risk Factor :-** Low
- **Description :-** The remote SSH server is configured to allow either MD5 or 96-bit MAC algorithms.
- **Impact :-** Both of these are considered weak.

  (NOTE : This plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions.)
- **Solution :-** Contact the vendor or consult product documentation to disable MD5 and 96-bit MAC algorithms.

POP3 (CLEARTEXT LOGINS PERMITTED)

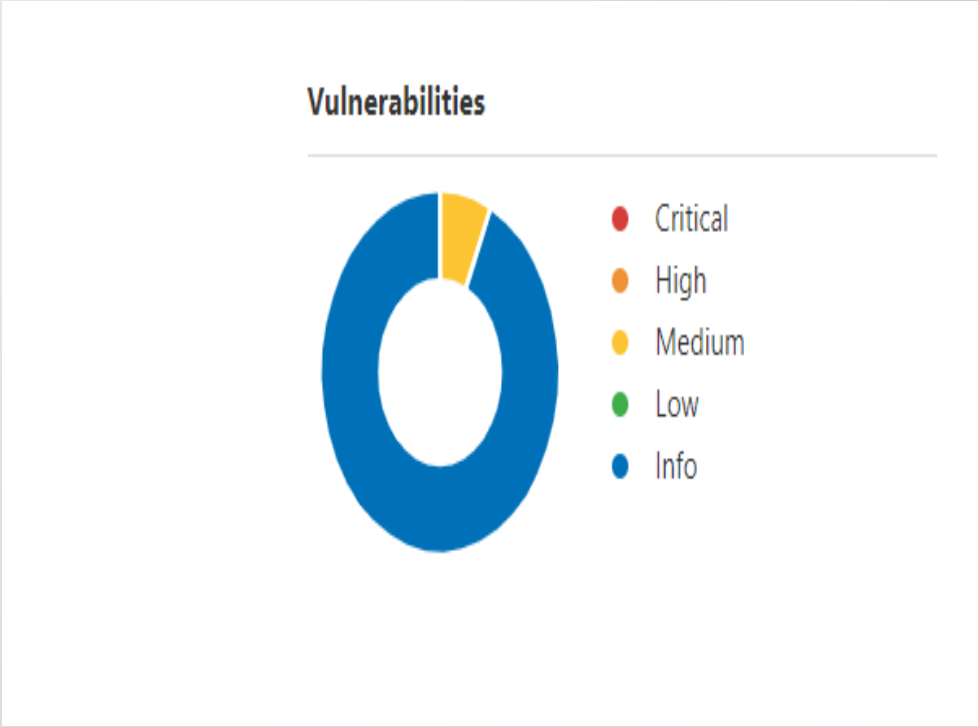
- **Risk factor :-** Low
- **Description :-** The remote host is running a POP3 daemon that allows cleartext logins over unencrypted connections.
- **Impact :-** An attacker can uncover user names and passwords by sniffing traffic to the POP3 daemon if a less secure authentication mechanism (eg, USER command, AUTH PLAIN, AUTH LOGIN) is used.
- **Solution :-** Contact your vendor for a fix or encrypt traffic with SSL / TLS using stunnel.

VULNERABILITY ASSESSMENT (HOST MACHINE)



RISK
(IN %)

1) Critical = 0
2) High = 0
3) Medium = 4.55
4) Low = 0
5) Info =95.45



SMB SIGNING NOT REQUIRED

- **Risk Factor :-** Medium
- **Description :-** Signing is not required on the remote SMB server.
- **Impact :-** An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.
- **Solution :-** Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'.

TASK-2

PASSWORD CRACKING

APPROACH

1.Open the terminal in Kali Linux.

2.Follow the commands as mentioned in the screenshot-1.(refer next slide)

3.You'll obtain the password for pass.txt file.

4.Now,copy all the contents form pass.txt file and paste it in the terminal.(refer next slide)

5.Follow the commands as mentioned in the screenshot-2.

6.Now,you'll obtain 3 cracked hashes of passwords mapped with their usernames.

7.That's all! Your task is completed successfully.

RESULT:-

1.Password of pass.txt = !!!123blahblah!!

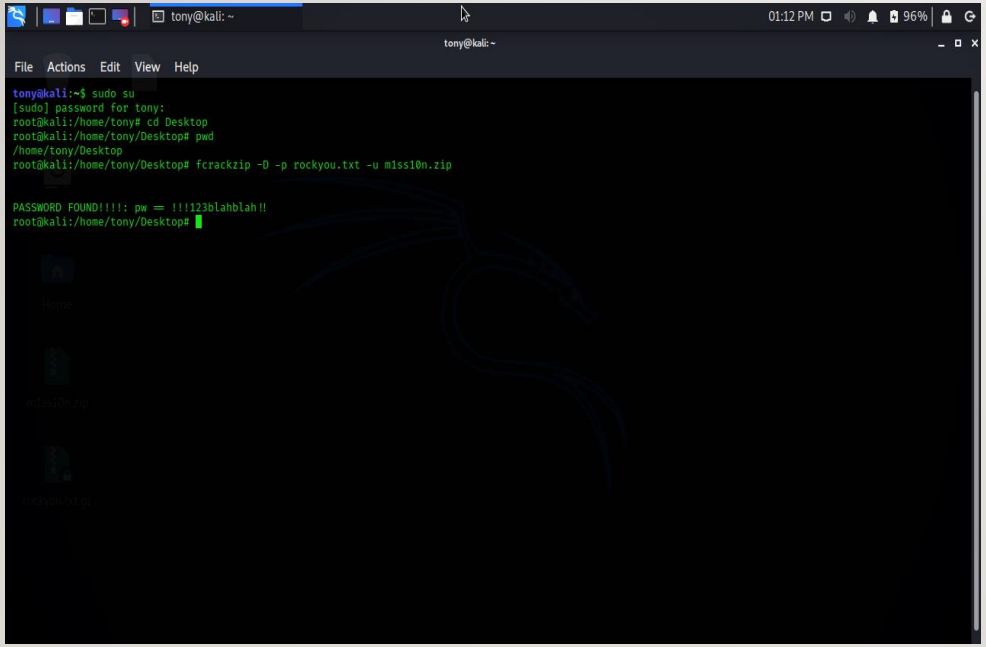
2.Password of Usernames(root)=kali

(kali)=kali

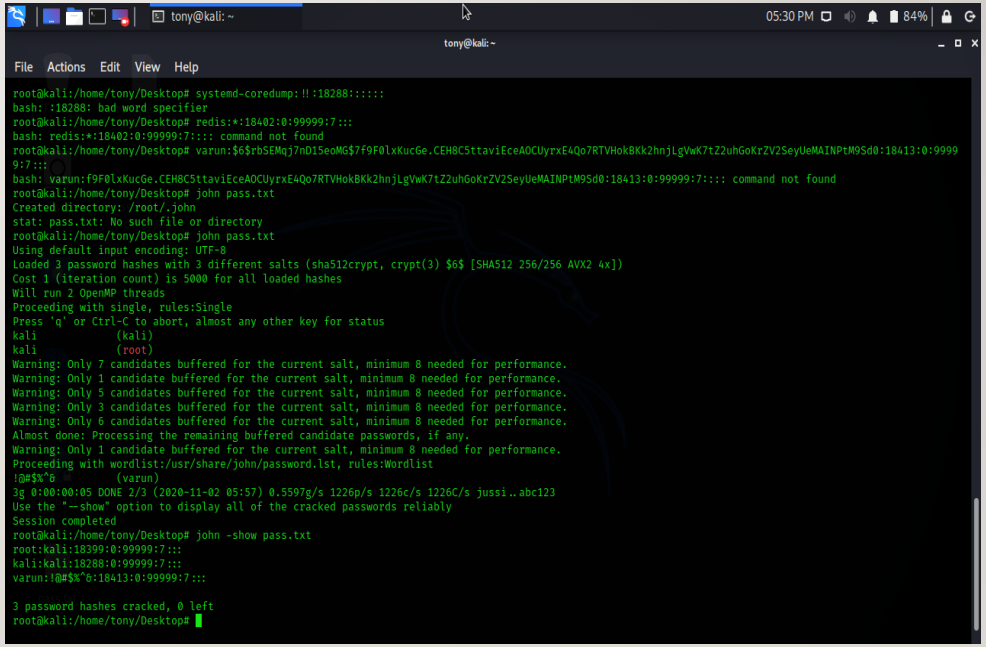
(varun)=!@#$%^&

SCREENSHOTS (KALI LINUX-TERMINAL)

SCREENSHOT-1



SCREENSHOT-2



TASK-3

STEGANOGRAPHY

APPROACH

Steps to approach:-

1.Consider an image on the desktop.

2.Consider a video on the desktop.

3.Now,open "COMMAND PROMPT".

4.Enter the command :cd desktop

5.Now you're able to access the files/folders on the destop.

6.Enter the command : copy /b image.ext + file.ext New_File.ext

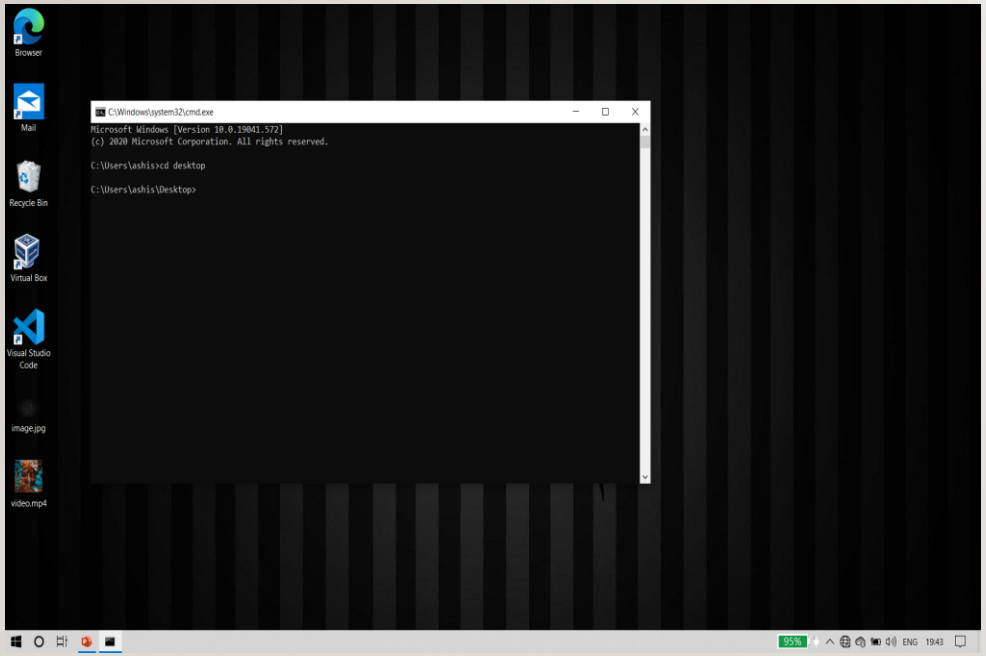
(Here,".ext" refers to the extension of the file type)

7.That's all! Your task is completed successfully.

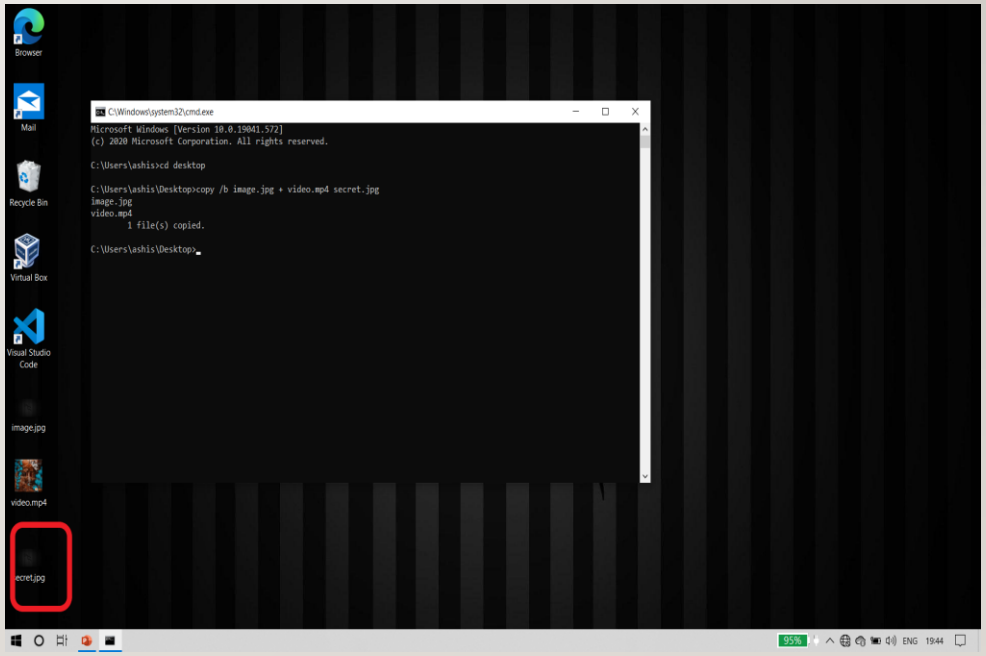
(NOTE : Please refer next slide for clarification)

SCREENSHOTS (EXECUTION OF STEGANOGRAPHY)

BEFORE



AFTER



THANK YOU!

BY;

-GUDENA ASHISH