Time	Event
2025-09-01T22:21:29+0100	"209654","","","None","192.168.1.244","tcp","0","OS Fingerprints Detected","Multiple OS fingerprints were detected.","Using a combination of remote probes (TCP/IP, SMB, HTTP, NTP, SNMP, etc), it was possible to gather one or more fingerprints from the remote system. While the highest-confidence result was reported in plugin 11936, “ OS Identification ” , the complete set of fingerprints detected are reported here.","n/a",""," Following OS Fingerprints were found Remote operating system : Ubuntu 18.04 Linux Kernel 4.15 Confidence level : 56 Method : MLSinFP Type : unknown Fingerprint : unknown Remote operating system : Linux Kernel 2.6 Confidence level : 65 Method : SinFP Type : general-purpose Fingerprint : SinFP: P1:B10113:F0x12:W64240:O0204ffff:M1460: P2:B10113:F0x12:W65160:O0204ffff0402080affffffff4445414401030307:M1460: P3:B00000:F0x00:W0:O0:M0 P4:191301_7_p=22 Following fingerprints could not be used to determine OS : SSH:!:SSH-2.0-OpenSSH_9.6p1 Ubuntu-3ubuntu13.13 HTTP:!:Server: Apache/2.4.58 (Ubuntu) "
2025-09-01T22:21:29+0100	"181418","","","None","192.168.1.244","tcp","22","OpenSSH Detection","An OpenSSH-based SSH server was detected on the remote host.","An OpenSSH-based SSH server was detected on the remote host.","n /a","https://www.openssh.com/"," Service : ssh Version : 9.6p1 Banner : SSH-2.0-OpenSSH_9.6p1 Ubuntu-3ubuntu13.13 "
2025-09-01T22:21:29+0100	"153588","","","None","192.168.1.244","tcp","22","SSH SHA-1 HMAC Algorithms Enabled","The remote SSH server is configured to enable SHA-1 HMAC algorithms.","The remote SSH server is configured to enable SHA-1 HMAC algorithms. Although NIST has formally deprecated use of SHA-1 for digital signatures, SHA-1 is still considered secure for HMAC as the security of HMAC does not rely on the underlying hash function being resistant to collisions. Note that this plugin only checks for the options of the remote SSH server.","n/a",""," The following client-to-server SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are supported : hmac-sha1 hmac-sha1-etm@openssh.com The following server-to-client SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are supported : hmac-sha1 hmac-sha1-etm@openssh.com "
2025-09-01T22:21:29+0100	"149334","","","None","192.168.1.244","tcp","22","SSH Password Authentication Accepted","The SSH server on the remote host accepts password authentication.","The SSH server on the remote host accepts password authentication.","n/a","https://tools.ietf.org/html/rfc4252#section-8",""

Time	Event
2025-09-01T22:21:29+0100	"117886","","","None","192.168.1.244","tcp","0","OS Security Patch Assessment Not Available","OS Security Patch Assessment is not available.","OS Security Patch Assessment is not available on the remote host. This does not necessarily indicate a problem with the scan. Credentials may not have been provided, OS security patch assessment may not be supported for the target, the target may not have been identified, or another issue may have occurred that prevented OS security patch assessment from being available. See plugin output for details. This plugin reports non-failure information impacting the availability of OS Security Patch Assessment. Failure information is reported by plugin 21745 : 'OS Security Patch Assessment failed'. If a target host is not supported for OS Security Patch Assessment, plugin 110695 : 'OS Security Patch Assessment Checks Not Supported' will report concurrently with this plugin.","n/a",""," The following issues were reported : - Plugin : no_local_checks_credentials.nasl Plugin ID : 110723 Plugin Name : Target Credential Status by Authentication Protocol - No Credentials Provided Message : Credentials were not provided for detected SSH service. "
2025-09-01T22:21:29+0100	"110723","","","None","192.168.1.244","tcp","0","Target Credential Status by Authentication Protocol - No Credentials Provided","Nessus was able to find common ports used for local checks, however, no credentials were provided in the scan policy.","Nessus was not able to successfully authenticate directly to the remote target on an available authentication protocol. Nessus was able to connect to the remote port and identify that the service running on the port supports an authentication protocol, but Nessus failed to authenticate to the remote service using the provided credentials. There may have been a protocol failure that prevented authentication from being attempted or all of the provided credentials for the authentication protocol may be invalid. See plugin output for error details. Please note the following : - This plugin reports per protocol, so it is possible for valid credentials to be provided for one protocol and not another. For example, authentication may succeed via SSH but fail via SMB, while no credentials were provided for an available SNMP service. - Providing valid credentials for all available authentication protocols may improve scan coverage, but the value of successful authentication for a given protocol may vary from target to target depending upon what data (if any) is gathered from the target via that protocol. For example, successful authentication via SSH is more valuable for Linux targets than for Windows targets, and likewise successful authentication via SMB is more valuable for Windows targets than for Linux targets.","n/a","","SSH was detected on port 22 but no credentials were provided. SSH local checks were not enabled. "
2025-09-01T22:21:29+0100	"86420","","","None","192.168.1.244","tcp","0","Ethernet MAC Addresses","This plugin gathers MAC addresses from various sources and consolidates them into a list.","This plugin gathers MAC addresses discovered from both remote probing of the host (e.g. SNMP and Netbios) and from running local checks (e.g. ifconfig). It then consolidates the MAC addresses into a single, unique, and uniform list.","n/a","","The following is a consolidated list of detected MAC addresses: - 00:0C:29:ED:57:15 "

```
Time                      Event
2025-09-01T22:21:29+0100  "70657","","","None","192.168.1.244","tcp","22","SSH Algorithms and Languages Supported","An
                          SSH server is listening on this port.","This script detects which algorithms and languages are supported by
                          the remote service for encrypting communications.","n/a","","
                          Nessus negotiated the following encryption algorithm(s) with the server :

                            Client to Server: aes256-ctr
                            Server to Client: aes256-ctr

                          The server supports the following options for compression_algorithms_server_to_client :

                            none
                            zlib@openssh.com

                          The server supports the following options for mac_algorithms_client_to_server :

                            hmac-sha1
                            hmac-sha1-etm@openssh.com
                            hmac-sha2-256
                            hmac-sha2-256-etm@openssh.com
                            hmac-sha2-512
                            hmac-sha2-512-etm@openssh.com
                            umac-128-etm@openssh.com
                            umac-128@openssh.com
                            umac-64-etm@openssh.com
                            umac-64@openssh.com

                          The server supports the following options for server_host_key_algorithms :

                            ecdsa-sha2-nistp256
                            rsa-sha2-256
                            rsa-sha2-512
                            ssh-ed25519

                          The server supports the following options for encryption_algorithms_client_to_server :

                            aes128-ctr
                            aes128-gcm@openssh.com
                            aes192-ctr
                            aes256-ctr
                            aes256-gcm@openssh.com
                            chacha20-poly1305@openssh.com

                          The server supports the following options for mac_algorithms_server_to_client :

                            hmac-sha1
                            hmac-sha1-etm@openssh.com
                            hmac-sha2-256
                            hmac-sha2-256-etm@openssh.com
                            hmac-sha2-512
                            hmac-sha2-512-etm@openssh.com
                            umac-128-etm@openssh.com
                            umac-128@openssh.com
                            umac-64-etm@openssh.com
                            umac-64@openssh.com

                          The server supports the following options for kex_algorithms :

                            curve25519-sha256
                            curve25519-sha256@libssh.org
                            diffie-hellman-group-exchange-sha256
                            diffie-hellman-group14-sha256
                            diffie-hellman-group16-sha512
                            diffie-hellman-group18-sha512
                            ecdh-sha2-nistp256
                            ecdh-sha2-nistp384
                            ecdh-sha2-nistp521
                            ext-info-s
                            kex-strict-s-v00@openssh.com
                            sntrup761x25519-sha512@openssh.com

                          The server supports the following options for compression_algorithms_client_to_server :

                            none
                          ... Truncated. 85.5421686746988% shown.
```

Time	Event
2025-09-01T22:21:29+0100	"66717","","","None","192.168.1.244","udp","5353","mDNS Detection (Local Network)","It is possible to obtain information about the remote host.","The remote service understands the Bonjour (also known as ZeroConf or mDNS) protocol, which allows anyone to uncover information from the remote host such as its operating system type and exact version, its hostname, and the list of services it is running. This plugin attempts to discover mDNS used by hosts residing on the same network segment as Nessus.","Filter incoming traffic to UDP port 5353, if desired.","","Nessus was able to extract the following information : - mDNS hostname : olaniyi-UbuntuVM.local. "
2025-09-01T22:21:29+0100	"54615","","","None","192.168.1.244","tcp","0","Device Type","It is possible to guess the remote device type.","Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).","n/a","","Remote device type : general-purpose Confidence level : 65 "
2025-09-01T22:21:29+0100	"52703","","","None","192.168.1.244","tcp","21","vsftpd Detection","An FTP server is listening on the remote port.","The remote host is running vsftpd, an FTP server for UNIX-like systems written in C.","n/a","http://vsftpd.beasts.org/"," Source : 220 (vsFTPd 3.0.5) Version : 3.0.5 "

2025-09-01T22:21:29+0100	"48204","","","None","192.168.1.244","tcp","80","Apache HTTP Server Version","It is possible to
	obtain the version number of the remote Apache HTTP
	server.","The remote host is running the Apache HTTP Server, an open source web
	server. It was possible to read the version number from the banner.","n/a","https://httpd.apache.org/","
	  URL : http://olaniyi-UbuntuVM.lan/
	  Version : 2.4.99
	  Source : Server: Apache/2.4.58 (Ubuntu)
	  backported : 1
	  os : ConvertedUbuntu
	"

2025-09-01T22:21:29+0100	"45590","","","None","192.168.1.244","tcp","0","Common Platform Enumeration (CPE)","It was possible to enumerate CPE names that matched on the remote system.","By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host. Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.","n/a","http://cpe.mitre.org/ https://nvd.nist.gov/products/cpe"," The remote operating system matched the following CPE : cpe:/o:linux:linux_kernel -> Linux Kernel Following application CPE's matched on the remote system : cpe:/a:apache:http_server:2.4.58 -> Apache Software Foundation Apache HTTP Server cpe:/a:apache:http_server:2.4.99 -> Apache Software Foundation Apache HTTP Server cpe:/a:openbsd:openssh:9.6 -> OpenBSD OpenSSH cpe:/a:openbsd:openssh:9.6p1 -> OpenBSD OpenSSH "

Time	Event
2025-09-01T22:21:29+0100	"43111","","","None","192.168.1.244","tcp","80","HTTP Methods Allowed (per directory)","This plugin determines which HTTP methods are allowed on various CGI directories.","By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory. The following HTTP methods are considered insecure: PUT, DELETE, CONNECT, TRACE, HEAD Many frameworks and languages treat 'HEAD' as a 'GET' request, albeit one without any body in the response. If a security constraint was set on 'GET' requests such that only 'authenticatedUsers' could access GET requests for a particular servlet or resource, it would be bypassed for the 'HEAD' version. This allowed unauthorized blind submission of any privileged GET request. As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes' in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501. Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.","n/a","http://www.nessus.org/u?d9c03a9a http://www.nessus.org/u?b019cbdb https://www.owasp.org/index.php/Test_HTTP_Methods_(OTG-CONFIG-006)","Based on the response to an OPTIONS request : - HTTP methods GET HEAD OPTIONS POST are allowed on : / "
2025-09-01T22:21:29+0100	"39521","","","None","192.168.1.244","tcp","80","Backported Security Patch Detection (WWW)"," Security patches are backported.","Security patches may have been 'backported' to the remote HTTP server without changing its version number. Banner-based checks have been disabled to avoid false positives. Note that this test is informational only and does not denote any security problem.","n/a","https://access.redhat.com/security/updates/backporting/?sc_cid=3093"," Give Nessus credentials to perform local checks. "
2025-09-01T22:21:29+0100	"39520","","","None","192.168.1.244","tcp","22","Backported Security Patch Detection (SSH)"," Security patches are backported.","Security patches may have been 'backported' to the remote SSH server without changing its version number. Banner-based checks have been disabled to avoid false positives. Note that this test is informational only and does not denote any security problem.","n/a","https://access.redhat.com/security/updates/backporting/?sc_cid=3093"," Give Nessus credentials to perform local checks. "
2025-09-01T22:21:29+0100	"35716","","","None","192.168.1.244","tcp","0","Ethernet Card Manufacturer Detection","The manufacturer can be identified from the Ethernet OUI.","Each ethernet MAC address starts with a 24-bit Organizationally Unique Identifier (OUI). These OUIs are registered by IEEE.","n/a","https://standards.ieee.org/faqs/regauth.html http://www.nessus.org/u?794673b4"," The following card manufacturers were identified : 00:0C:29:ED:57:15 : VMware, Inc. "
2025-09-01T22:21:29+0100	"25220","","","None","192.168.1.244","tcp","0","TCP/IP Timestamps Supported","The remote service implements TCP timestamps.","The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.","n/a","http://www.ietf.org/rfc/rfc1323.txt",""

```
Time                      Event
2025-09-01T22:21:29+0100  "24260","","","None","192.168.1.244","tcp","80","HyperText Transfer Protocol (HTTP) Information","
                          Some information about the remote HTTP configuration can be extracted.","This test gives some information about the
                           remote HTTP protocol - the
                          version used, whether HTTP Keep-Alive is enabled, etc...
                          This test is informational only and does not denote any security
                          problem.","n/a","","
                          Response Code : HTTP/1.1 200 OK
                          Protocol version : HTTP/1.1
                          HTTP/2 TLS Support: No
                          HTTP/2 Cleartext Support: No
                          SSL : no
                          Keep-Alive : yes
                          Options allowed : (Not implemented)
                          Headers :
                            Date: Mon, 01 Sep 2025 20:24:39 GMT
                            Server: Apache/2.4.58 (Ubuntu)
                            Last-Modified: Mon, 01 Sep 2025 19:59:36 GMT
                            ETag: ""29af-63dc2cf995dc1""
                            Accept-Ranges: bytes
                            Content-Length: 10671
                            Vary: Accept-Encoding
                            Keep-Alive: timeout=5, max=100
                            Connection: Keep-Alive
                            Content-Type: text/html

                          Response Body :
                          <!DOCTYPE html PUBLIC ""-//W3C//DTD XHTML 1.0 Transitional//EN"" ""http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd"">
                          <html xmlns=""http://www.w3.org/1999/xhtml"">
                            <!--
                              Modified from the Debian original for Ubuntu
                              Last updated: 2022-03-22
                              See: https://launchpad.net/bugs/1966004
                            -->
                            <head>
                              <meta http-equiv=""Content-Type"" content=""text/html; charset=UTF-8"" />
                              <title>Apache2 Ubuntu Default Page: It works</title>
                              <style type=""text/css"" media=""screen"">
                            * {
                              margin: 0px 0px 0px 0px;
                              padding: 0px 0px 0px 0px;
                            }
                            body, html {
                              padding: 3px 3px 3px 3px;
                              background-color: #D8DBE2;
                              font-family: Ubuntu, Verdana, sans-serif;
                              font-size: 11pt;
                              text-align: center;
                            }
                            div.main_page {
                              position: relative;
                              display: table;
                              width: 800px;
                              margin-bottom: 3px;
                              margin-left: auto;
                              margin-right: auto;
                              padding: 0px 0px 0px 0px;
                              border-width: 2px;
                              border-color: #212738;
                              border-style: solid;
                              background-color: #FFFFFF;
                              text-align: center;
                            }
                            div.page_header {
                              height: 180px;
                              width: 100%;
                              background-color: #F5F6F7;
                            }
                            div.page_header span {
                              margin: 15px 0px 0px 50px;
                              font-size: 180%;
                              font-weight: bold;
                            }
                            div.page_header img {
                          ... Truncated. 70.0% shown.
2025-09-01T22:21:29+0100  "22964","","","None","192.168.1.244","tcp","80","Service Detection","The remote service could be
                          identified.","Nessus was able to identify the remote service by its banner or by
                          looking at the error message it sends when it receives an HTTP
                          request.","n/a","","A web server is running on this port."
```

Time	Event
2025-09-01T22:21:29+0100	"22964","","","None","192.168.1.244","tcp","22","Service Detection","The remote service could be identified.","Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.","n/a","","An SSH server is running on this port."
2025-09-01T22:21:29+0100	"22964","","","None","192.168.1.244","tcp","21","Service Detection","The remote service could be identified.","Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.","n/a","","An FTP server is running on this port."
2025-09-01T22:21:29+0100	"20094","","","None","192.168.1.244","tcp","0","VMware Virtual Machine Detection","The remote host is a VMware virtual machine.","According to the MAC address of its network adapter, the remote host is a VMware virtual machine.","Since it is physically accessible through the network, ensure that its configuration matches your organization's security policy.",""," The remote host is a VMware virtual machine. "
2025-09-01T22:21:29+0100	"19506","","","None","192.168.1.244","tcp","0","Nessus Scan Information","This plugin displays information about the Nessus scan.","This plugin displays, for each tested host, information about the scan itself : - The version of the plugin set. - The type of scanner (Nessus or Nessus Home). - The version of the Nessus Engine. - The port scanner(s) used. - The port range scanned. - The ping round trip time - Whether credentialed or third-party patch management checks are possible. - Whether the display of superseded patches is enabled - The date of the scan. - The duration of the scan. - The number of hosts scanned in parallel. - The number of checks done in parallel.","n/a","","Information about this scan : Nessus version : 10.9.1 Nessus build : 20006 Plugin feed version : 202508220729 Scanner edition used : Nessus Home Scanner OS : LINUX Scanner distribution : ubuntu1604-x86-64 Scan type : Normal Scan name : UbuntuVM scan Scan policy used : Basic Network Scan Scanner IP : 192.168.1.113 Port scanner(s) : nessus_syn_scanner Port range : default Ping RTT : 107.353 ms Thorough tests : no Experimental tests : no Scan for Unpatched Vulnerabilities : no Plugin debugging enabled : no Paranoia level : 1 Report verbosity : 1 Safe checks : yes Optimize the test : yes Credentialed checks : no Patch management checks : None Display superseded patches : yes (supersedence plugin did not launch) CGI scanning : disabled Web application tests : disabled Max hosts : 30 Max checks : 4 Recv timeout : 5 Backports : Detected Allow post-scan editing : Yes Nessus Plugin Signature Checking : Enabled Audit File Signature Checking : Disabled Scan Start Date : 2025/9/1 21:23 BST (UTC +01:00) Scan duration : 399 sec Scan for malware : no "
2025-09-01T22:21:29+0100	"12053","","","None","192.168.1.244","tcp","0","Host Fully Qualified Domain Name (FQDN) Resolution ","It was possible to resolve the name of the remote host.","Nessus was able to resolve the fully qualified domain name (FQDN) of the remote host.","n/a",""," 192.168.1.244 resolves as olaniyi-UbuntuVM.lan. "

Time	Event
2025-09-01T22:21:29+0100	"11936","","","None","192.168.1.244","tcp","0","OS Identification","It is possible to guess the remote operating system.","Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.","n/a",""," Remote operating system : Linux Kernel 2.6 Confidence level : 65 Method : SinFP The remote host is running Linux Kernel 2.6"
2025-09-01T22:21:29+0100	"11219","","","None","192.168.1.244","tcp","80","Nessus SYN scanner","It is possible to determine which TCP ports are open.","This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target. Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.","Protect your target with an IP filter.","","Port 80/tcp was found to be open"
2025-09-01T22:21:29+0100	"11219","","","None","192.168.1.244","tcp","22","Nessus SYN scanner","It is possible to determine which TCP ports are open.","This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target. Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.","Protect your target with an IP filter.","","Port 22/tcp was found to be open"
2025-09-01T22:21:29+0100	"11219","","","None","192.168.1.244","tcp","21","Nessus SYN scanner","It is possible to determine which TCP ports are open.","This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target. Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.","Protect your target with an IP filter.","","Port 21/tcp was found to be open"
2025-09-01T22:21:29+0100	"10881","","","None","192.168.1.244","tcp","22","SSH Protocol Versions Supported","A SSH server is running on the remote host.","This plugin determines the versions of the SSH protocol supported by the remote SSH daemon.","n/a","","The remote SSH daemon supports the following versions of the SSH protocol : - 1.99 - 2.0 "
2025-09-01T22:21:29+0100	"10287","","","None","192.168.1.244","udp","0","Traceroute Information","It was possible to obtain traceroute information.","Makes a traceroute to the remote host.","n/a","","For your information, here is the traceroute from 192.168.1.113 to 192.168.1.244 : 192.168.1.113 192.168.1.244 Hop Count: 1 "
2025-09-01T22:21:29+0100	"10267","","","None","192.168.1.244","tcp","22","SSH Server Type and Version Information","An SSH server is listening on this port.","It is possible to obtain information about the remote SSH server by sending an empty authentication request.","n/a",""," SSH version : SSH-2.0-OpenSSH_9.6p1 Ubuntu-3ubuntu13.13 SSH supported authentication : publickey,password "
2025-09-01T22:21:29+0100	"10114","CVE-1999-0524","2.1","Low","192.168.1.244","icmp","0","ICMP Timestamp Request Remote Date Disclosure","It is possible to determine the exact time set on the remote host.","The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols. Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.","Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).","","The remote clock is synchronized with the local clock. "
2025-09-01T22:21:29+0100	"10107","","","None","192.168.1.244","tcp","80","HTTP Server Type and Version","A web server is running on the remote host.","This plugin attempts to determine the type and the version of the remote web server.","n/a","","The remote web server type is : Apache/2.4.58 (Ubuntu)"

Time	Event
2025-09-01T22:21:29+0100	"10092","","","None","192.168.1.244","tcp","21","FTP Server Detection","An FTP server is listening on a remote port.","It is possible to obtain the banner of the remote FTP server by connecting to a remote port.","n/a","","" The remote FTP banner is : 220 (vsFTPd 3.0.5) "
2025-09-01T22:14:09+0100	"209654","","","None","192.168.1.244","tcp","0","OS Fingerprints Detected","Multiple OS fingerprints were detected.","Using a combination of remote probes (TCP/IP, SMB, HTTP, NTP, SNMP, etc), it was possible to gather one or more fingerprints from the remote system. While the highest-confidence result was reported in plugin 11936, “ OS Identification ” , the complete set of fingerprints detected are reported here.","n/a","","" Following OS Fingerprints were found Remote operating system : Ubuntu 18.04 Linux Kernel 4.15 Confidence level : 56 Method : MLSinFP Type : unknown Fingerprint : unknown Remote operating system : Linux Kernel 2.6 Confidence level : 65 Method : SinFP Type : general-purpose Fingerprint : SinFP: P1:B10113:F0x12:W64240:O0204ffff:M1460: P2:B10113:F0x12:W65160:O0204ffff0402080affffffff4445414401030307:M1460: P3:B00000:F0x00:W0:O0:M0 P4:191301_7_p=22 Following fingerprints could not be used to determine OS : SSH:!:SSH-2.0-OpenSSH_9.6p1 Ubuntu-3ubuntu13.13 HTTP:!:Server: Apache/2.4.58 (Ubuntu) "

2025-09-01T22:14:09+0100	"181418","","","None","192.168.1.244","tcp","22","OpenSSH Detection","An OpenSSH-based SSH
	server was detected on the remote host.","An OpenSSH-based SSH server was detected on the remote host.","n/a","https://www.openssh.com/",""
	  Service : ssh
	  Version : 9.6p1
	  Banner : SSH-2.0-OpenSSH_9.6p1 Ubuntu-3ubuntu13.13
	"

2025-09-01T22:14:09+0100	"153588","","","None","192.168.1.244","tcp","22","SSH SHA-1 HMAC Algorithms Enabled","The remote SSH server is configured to enable SHA-1 HMAC algorithms.","The remote SSH server is configured to enable SHA-1 HMAC algorithms. Although NIST has formally deprecated use of SHA-1 for digital signatures, SHA-1 is still considered secure for HMAC as the security of HMAC does not rely on the underlying hash function being resistant to collisions. Note that this plugin only checks for the options of the remote SSH server.","n/a","","" The following client-to-server SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are supported : hmac-sha1 hmac-sha1-etm@openssh.com The following server-to-client SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are supported : hmac-sha1 hmac-sha1-etm@openssh.com "
2025-09-01T22:14:09+0100	"149334","","","None","192.168.1.244","tcp","22","SSH Password Authentication Accepted","The SSH server on the remote host accepts password authentication.","The SSH server on the remote host accepts password authentication.","n/a","https://tools.ietf.org/html/rfc4252#section-8",""

Time	Event
2025-09-01T22:14:09+0100	"117886","","","None","192.168.1.244","tcp","0","OS Security Patch Assessment Not Available","OS Security Patch Assessment is not available.","OS Security Patch Assessment is not available on the remote host. This does not necessarily indicate a problem with the scan. Credentials may not have been provided, OS security patch assessment may not be supported for the target, the target may not have been identified, or another issue may have occurred that prevented OS security patch assessment from being available. See plugin output for details. This plugin reports non-failure information impacting the availability of OS Security Patch Assessment. Failure information is reported by plugin 21745 : 'OS Security Patch Assessment failed'. If a target host is not supported for OS Security Patch Assessment, plugin 110695 : 'OS Security Patch Assessment Checks Not Supported' will report concurrently with this plugin.","n/a","","" The following issues were reported : - Plugin : no_local_checks_credentials.nasl Plugin ID : 110723 Plugin Name : Target Credential Status by Authentication Protocol - No Credentials Provided Message : Credentials were not provided for detected SSH service. "
2025-09-01T22:14:09+0100	"110723","","","None","192.168.1.244","tcp","0","Target Credential Status by Authentication Protocol - No Credentials Provided","Nessus was able to find common ports used for local checks, however, no credentials were provided in the scan policy.","Nessus was not able to successfully authenticate directly to the remote target on an available authentication protocol. Nessus was able to connect to the remote port and identify that the service running on the port supports an authentication protocol, but Nessus failed to authenticate to the remote service using the provided credentials. There may have been a protocol failure that prevented authentication from being attempted or all of the provided credentials for the authentication protocol may be invalid. See plugin output for error details. Please note the following : - This plugin reports per protocol, so it is possible for valid credentials to be provided for one protocol and not another. For example, authentication may succeed via SSH but fail via SMB, while no credentials were provided for an available SNMP service. - Providing valid credentials for all available authentication protocols may improve scan coverage, but the value of successful authentication for a given protocol may vary from target to target depending upon what data (if any) is gathered from the target via that protocol. For example, successful authentication via SSH is more valuable for Linux targets than for Windows targets, and likewise successful authentication via SMB is more valuable for Windows targets than for Linux targets.","n/a","","SSH was detected on port 22 but no credentials were provided. SSH local checks were not enabled. "
2025-09-01T22:14:09+0100	"86420","","","None","192.168.1.244","tcp","0","Ethernet MAC Addresses","This plugin gathers MAC addresses from various sources and consolidates them into a list.","This plugin gathers MAC addresses discovered from both remote probing of the host (e.g. SNMP and Netbios) and from running local checks (e.g. ifconfig). It then consolidates the MAC addresses into a single, unique, and uniform list.","n/a","","The following is a consolidated list of detected MAC addresses: - 00:0C:29:ED:57:15 "

Time	Event

2025-09-01T22:14:09+0100	"70657","","","None","192.168.1.244","tcp","22","SSH Algorithms and Languages Supported","An
	SSH server is listening on this port.","This script detects which algorithms and languages are supported by
	the remote service for encrypting communications.","n/a","",""
	Nessus negotiated the following encryption algorithm(s) with the server :
	
	  Client to Server: aes256-ctr
	  Server to Client: aes256-ctr
	
	The server supports the following options for compression_algorithms_server_to_client :
	
	  none
	  zlib@openssh.com
	
	The server supports the following options for mac_algorithms_client_to_server :
	
	  hmac-sha1
	  hmac-sha1-etm@openssh.com
	  hmac-sha2-256
	  hmac-sha2-256-etm@openssh.com
	  hmac-sha2-512
	  hmac-sha2-512-etm@openssh.com
	  umac-128-etm@openssh.com
	  umac-128@openssh.com
	  umac-64-etm@openssh.com
	  umac-64@openssh.com
	
	The server supports the following options for server_host_key_algorithms :
	
	  ecdsa-sha2-nistp256
	  rsa-sha2-256
	  rsa-sha2-512
	  ssh-ed25519
	
	The server supports the following options for encryption_algorithms_client_to_server :
	
	  aes128-ctr
	  aes128-gcm@openssh.com
	  aes192-ctr
	  aes256-ctr
	  aes256-gcm@openssh.com
	  chacha20-poly1305@openssh.com
	
	The server supports the following options for mac_algorithms_server_to_client :
	
	  hmac-sha1
	  hmac-sha1-etm@openssh.com
	  hmac-sha2-256
	  hmac-sha2-256-etm@openssh.com
	  hmac-sha2-512
	  hmac-sha2-512-etm@openssh.com
	  umac-128-etm@openssh.com
	  umac-128@openssh.com
	  umac-64-etm@openssh.com
	  umac-64@openssh.com
	
	The server supports the following options for kex_algorithms :
	
	  curve25519-sha256
	  curve25519-sha256@libssh.org
	  diffie-hellman-group-exchange-sha256
	  diffie-hellman-group14-sha256
	  diffie-hellman-group16-sha512
	  diffie-hellman-group18-sha512
	  ecdh-sha2-nistp256
	  ecdh-sha2-nistp384
	  ecdh-sha2-nistp521
	  ext-info-s
	  kex-strict-s-v00@openssh.com
	  sntrup761x25519-sha512@openssh.com
	
	The server supports the following options for compression_algorithms_client_to_server :
	
	  none
	... Truncated. 85.5421686746988% shown.

Time	Event
2025-09-01T22:14:09+0100	"66717","","","None","192.168.1.244","udp","5353","mDNS Detection (Local Network)","It is possible to obtain information about the remote host.","The remote service understands the Bonjour (also known as ZeroConf or mDNS) protocol, which allows anyone to uncover information from the remote host such as its operating system type and exact version, its hostname, and the list of services it is running. This plugin attempts to discover mDNS used by hosts residing on the same network segment as Nessus.","Filter incoming traffic to UDP port 5353, if desired.","","Nessus was able to extract the following information : - mDNS hostname : olaniyi-UbuntuVM.local. "
2025-09-01T22:14:09+0100	"54615","","","None","192.168.1.244","tcp","0","Device Type","It is possible to guess the remote device type.","Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).","n/a","","Remote device type : general-purpose Confidence level : 65 "
2025-09-01T22:14:09+0100	"52703","","","None","192.168.1.244","tcp","21","vsftpd Detection","An FTP server is listening on the remote port.","The remote host is running vsftpd, an FTP server for UNIX-like systems written in C.","n/a","http://vsftpd.beasts.org/"," Source : 220 (vsFTPd 3.0.5) Version : 3.0.5 "

2025-09-01T22:14:09+0100	"48204","","","None","192.168.1.244","tcp","80","Apache HTTP Server Version","It is possible to
	obtain the version number of the remote Apache HTTP
	server.","The remote host is running the Apache HTTP Server, an open source web
	server. It was possible to read the version number from the banner.","n/a","https://httpd.apache.org/","
	  URL : http://olaniyi-UbuntuVM.lan/
	  Version : 2.4.99
	  Source : Server: Apache/2.4.58 (Ubuntu)
	  backported : 1
	  os : ConvertedUbuntu
	"

2025-09-01T22:14:09+0100	"45590","","","None","192.168.1.244","tcp","0","Common Platform Enumeration (CPE)","It was possible to enumerate CPE names that matched on the remote system.","By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host. Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.","n/a","http://cpe.mitre.org/ https://nvd.nist.gov/products/cpe"," The remote operating system matched the following CPE : cpe:/o:linux:linux_kernel -> Linux Kernel Following application CPE's matched on the remote system : cpe:/a:apache:http_server:2.4.58 -> Apache Software Foundation Apache HTTP Server cpe:/a:apache:http_server:2.4.99 -> Apache Software Foundation Apache HTTP Server cpe:/a:openbsd:openssh:9.6 -> OpenBSD OpenSSH cpe:/a:openbsd:openssh:9.6p1 -> OpenBSD OpenSSH "

Time	Event
2025-09-01T22:14:09+0100	"43111","","","None","192.168.1.244","tcp","80","HTTP Methods Allowed (per directory)","This plugin determines which HTTP methods are allowed on various CGI directories.","By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory. The following HTTP methods are considered insecure: PUT, DELETE, CONNECT, TRACE, HEAD Many frameworks and languages treat 'HEAD' as a 'GET' request, albeit one without any body in the response. If a security constraint was set on 'GET' requests such that only 'authenticatedUsers' could access GET requests for a particular servlet or resource, it would be bypassed for the 'HEAD' version. This allowed unauthorized blind submission of any privileged GET request. As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes' in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501. Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.","n/a","http://www.nessus.org/u?d9c03a9a http://www.nessus.org/u?b019cbdb https://www.owasp.org/index.php/Test_HTTP_Methods_(OTG-CONFIG-006)","Based on the response to an OPTIONS request : - HTTP methods GET HEAD OPTIONS POST are allowed on : / "
2025-09-01T22:14:09+0100	"39521","","","None","192.168.1.244","tcp","80","Backported Security Patch Detection (WWW)"," Security patches are backported.","Security patches may have been 'backported' to the remote HTTP server without changing its version number. Banner-based checks have been disabled to avoid false positives. Note that this test is informational only and does not denote any security problem.","n/a","https://access.redhat.com/security/updates/backporting/?sc_cid=3093"," Give Nessus credentials to perform local checks. "
2025-09-01T22:14:09+0100	"39520","","","None","192.168.1.244","tcp","22","Backported Security Patch Detection (SSH)"," Security patches are backported.","Security patches may have been 'backported' to the remote SSH server without changing its version number. Banner-based checks have been disabled to avoid false positives. Note that this test is informational only and does not denote any security problem.","n/a","https://access.redhat.com/security/updates/backporting/?sc_cid=3093"," Give Nessus credentials to perform local checks. "
2025-09-01T22:14:09+0100	"35716","","","None","192.168.1.244","tcp","0","Ethernet Card Manufacturer Detection","The manufacturer can be identified from the Ethernet OUI.","Each ethernet MAC address starts with a 24-bit Organizationally Unique Identifier (OUI). These OUIs are registered by IEEE.","n/a","https://standards.ieee.org/faqs/regauth.html http://www.nessus.org/u?794673b4"," The following card manufacturers were identified : 00:0C:29:ED:57:15 : VMware, Inc. "
2025-09-01T22:14:09+0100	"25220","","","None","192.168.1.244","tcp","0","TCP/IP Timestamps Supported","The remote service implements TCP timestamps.","The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.","n/a","http://www.ietf.org/rfc/rfc1323.txt",""

```
Time                      Event
2025-09-01T22:14:09+0100  "24260","","","None","192.168.1.244","tcp","80","HyperText Transfer Protocol (HTTP) Information","
                          Some information about the remote HTTP configuration can be extracted.","This test gives some information about the
                           remote HTTP protocol - the
                          version used, whether HTTP Keep-Alive is enabled, etc...
                          This test is informational only and does not denote any security
                          problem.","n/a","","
                          Response Code : HTTP/1.1 200 OK
                          Protocol version : HTTP/1.1
                          HTTP/2 TLS Support: No
                          HTTP/2 Cleartext Support: No
                          SSL : no
                          Keep-Alive : yes
                          Options allowed : (Not implemented)
                          Headers :
                            Date: Mon, 01 Sep 2025 20:24:39 GMT
                            Server: Apache/2.4.58 (Ubuntu)
                            Last-Modified: Mon, 01 Sep 2025 19:59:36 GMT
                            ETag: ""29af-63dc2cf995dc1""
                            Accept-Ranges: bytes
                            Content-Length: 10671
                            Vary: Accept-Encoding
                            Keep-Alive: timeout=5, max=100
                            Connection: Keep-Alive
                            Content-Type: text/html

                          Response Body :
                          <!DOCTYPE html PUBLIC ""-//W3C//DTD XHTML 1.0 Transitional//EN"" ""http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd"">
                          <html xmlns=""http://www.w3.org/1999/xhtml"">
                            <!--
                              Modified from the Debian original for Ubuntu
                              Last updated: 2022-03-22
                              See: https://launchpad.net/bugs/1966004
                            -->
                            <head>
                              <meta http-equiv=""Content-Type"" content=""text/html; charset=UTF-8"" />
                              <title>Apache2 Ubuntu Default Page: It works</title>
                              <style type=""text/css"" media=""screen"">
                            * {
                              margin: 0px 0px 0px 0px;
                              padding: 0px 0px 0px 0px;
                            }
                            body, html {
                              padding: 3px 3px 3px 3px;
                              background-color: #D8DBE2;
                              font-family: Ubuntu, Verdana, sans-serif;
                              font-size: 11pt;
                              text-align: center;
                            }
                            div.main_page {
                              position: relative;
                              display: table;
                              width: 800px;
                              margin-bottom: 3px;
                              margin-left: auto;
                              margin-right: auto;
                              padding: 0px 0px 0px 0px;
                              border-width: 2px;
                              border-color: #212738;
                              border-style: solid;
                              background-color: #FFFFFF;
                              text-align: center;
                            }
                            div.page_header {
                              height: 180px;
                              width: 100%;
                              background-color: #F5F6F7;
                            }
                            div.page_header span {
                              margin: 15px 0px 0px 50px;
                              font-size: 180%;
                              font-weight: bold;
                            }
                            div.page_header img {
                          ... Truncated. 70.0% shown.
2025-09-01T22:14:09+0100  "22964","","","None","192.168.1.244","tcp","80","Service Detection","The remote service could be
                          identified.","Nessus was able to identify the remote service by its banner or by
                          looking at the error message it sends when it receives an HTTP
                          request.","n/a","","A web server is running on this port."
```

Time	Event
2025-09-01T22:14:09+0100	"22964","","","None","192.168.1.244","tcp","22","Service Detection","The remote service could be identified.","Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.","n/a","","An SSH server is running on this port."
2025-09-01T22:14:09+0100	"22964","","","None","192.168.1.244","tcp","21","Service Detection","The remote service could be identified.","Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.","n/a","","An FTP server is running on this port."
2025-09-01T22:14:09+0100	"20094","","","None","192.168.1.244","tcp","0","VMware Virtual Machine Detection","The remote host is a VMware virtual machine.","According to the MAC address of its network adapter, the remote host is a VMware virtual machine.","Since it is physically accessible through the network, ensure that its configuration matches your organization's security policy.","","" The remote host is a VMware virtual machine. "
2025-09-01T22:14:09+0100	"19506","","","None","192.168.1.244","tcp","0","Nessus Scan Information","This plugin displays information about the Nessus scan.","This plugin displays, for each tested host, information about the scan itself : - The version of the plugin set. - The type of scanner (Nessus or Nessus Home). - The version of the Nessus Engine. - The port scanner(s) used. - The port range scanned. - The ping round trip time - Whether credentialed or third-party patch management checks are possible. - Whether the display of superseded patches is enabled - The date of the scan. - The duration of the scan. - The number of hosts scanned in parallel. - The number of checks done in parallel.","n/a","","Information about this scan : Nessus version : 10.9.1 Nessus build : 20006 Plugin feed version : 202508220729 Scanner edition used : Nessus Home Scanner OS : LINUX Scanner distribution : ubuntu1604-x86-64 Scan type : Normal Scan name : UbuntuVM scan Scan policy used : Basic Network Scan Scanner IP : 192.168.1.113 Port scanner(s) : nessus_syn_scanner Port range : default Ping RTT : 107.353 ms Thorough tests : no Experimental tests : no Scan for Unpatched Vulnerabilities : no Plugin debugging enabled : no Paranoia level : 1 Report verbosity : 1 Safe checks : yes Optimize the test : yes Credentialed checks : no Patch management checks : None Display superseded patches : yes (supersedence plugin did not launch) CGI scanning : disabled Web application tests : disabled Max hosts : 30 Max checks : 4 Recv timeout : 5 Backports : Detected Allow post-scan editing : Yes Nessus Plugin Signature Checking : Enabled Audit File Signature Checking : Disabled Scan Start Date : 2025/9/1 21:23 BST (UTC +01:00) Scan duration : 399 sec Scan for malware : no "
2025-09-01T22:14:09+0100	"12053","","","None","192.168.1.244","tcp","0","Host Fully Qualified Domain Name (FQDN) Resolution ","It was possible to resolve the name of the remote host.","Nessus was able to resolve the fully qualified domain name (FQDN) of the remote host.","n/a","","" 192.168.1.244 resolves as olaniyi-UbuntuVM.lan. "

Time	Event
2025-09-01T22:14:09+0100	"11936","","","None","192.168.1.244","tcp","0","OS Identification","It is possible to guess the remote operating system.","Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.","n/a",""," Remote operating system : Linux Kernel 2.6 Confidence level : 65 Method : SinFP The remote host is running Linux Kernel 2.6"
2025-09-01T22:14:09+0100	"11219","","","None","192.168.1.244","tcp","80","Nessus SYN scanner","It is possible to determine which TCP ports are open.","This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target. Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.","Protect your target with an IP filter.","","Port 80/tcp was found to be open"
2025-09-01T22:14:09+0100	"11219","","","None","192.168.1.244","tcp","22","Nessus SYN scanner","It is possible to determine which TCP ports are open.","This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target. Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.","Protect your target with an IP filter.","","Port 22/tcp was found to be open"
2025-09-01T22:14:09+0100	"11219","","","None","192.168.1.244","tcp","21","Nessus SYN scanner","It is possible to determine which TCP ports are open.","This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target. Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.","Protect your target with an IP filter.","","Port 21/tcp was found to be open"
2025-09-01T22:14:09+0100	"10881","","","None","192.168.1.244","tcp","22","SSH Protocol Versions Supported","A SSH server is running on the remote host.","This plugin determines the versions of the SSH protocol supported by the remote SSH daemon.","n/a","","The remote SSH daemon supports the following versions of the SSH protocol : - 1.99 - 2.0 "
2025-09-01T22:14:09+0100	"10287","","","None","192.168.1.244","udp","0","Traceroute Information","It was possible to obtain traceroute information.","Makes a traceroute to the remote host.","n/a","","For your information, here is the traceroute from 192.168.1.113 to 192.168.1.244 : 192.168.1.113 192.168.1.244 Hop Count: 1 "
2025-09-01T22:14:09+0100	"10267","","","None","192.168.1.244","tcp","22","SSH Server Type and Version Information","An SSH server is listening on this port.","It is possible to obtain information about the remote SSH server by sending an empty authentication request.","n/a",""," SSH version : SSH-2.0-OpenSSH_9.6p1 Ubuntu-3ubuntu13.13 SSH supported authentication : publickey,password "
2025-09-01T22:14:09+0100	"10114","CVE-1999-0524","2.1","Low","192.168.1.244","icmp","0","ICMP Timestamp Request Remote Date Disclosure","It is possible to determine the exact time set on the remote host.","The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols. Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.","Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).","","The remote clock is synchronized with the local clock. "
2025-09-01T22:14:09+0100	"10107","","","None","192.168.1.244","tcp","80","HTTP Server Type and Version","A web server is running on the remote host.","This plugin attempts to determine the type and the version of the remote web server.","n/a","","The remote web server type is : Apache/2.4.58 (Ubuntu)"

Time	Event
2025-09-01T22:14:09+0100	"10092","","","None","192.168.1.244","tcp","21","FTP Server Detection","An FTP server is listening on a remote port.","It is possible to obtain the banner of the remote FTP server by connecting to a remote port.","n/a",""," The remote FTP banner is : 220 (vsFTPd 3.0.5) "