b'\r\n'
b'(The Multi-Tool Web Vulnerability Scanner)\r\n'
b'\r\n'
b'[Checking Available Security Scanning Tools Phase... Initiated.]\r\n'
b'\twapiti...available.\r\n'
b'\twhatweb...available.\r\n'
b'\tnmap...available.\r\n'
b'\tgolismero...available.\r\n'
b'\thost...available.\r\n'
b'\twget...available.\r\n'
b'\tuniscan...available.\r\n'
b'\twafw00f...available.\r\n'
b'\tdirb...available.\r\n'
b'\tdavtest...available.\r\n'
b'\ttheharvester...available.\r\n'
b'\txsser...available.\r\n'
b'\tdnsrecon...available.\r\n'
b'\tfierce...available.\r\n'
b'\tdnswalk...available.\r\n'
b'\twhois...available.\r\n'
b'\tsslyze...available.\r\n'
b'\tlbd...available.\r\n'
b'\tgolismero...available.\r\n'
b'\tdnsenum...available.\r\n'
b'\tdmitry...available.\r\n'
b'\tdavtest...available.\r\n'
b'\tnikto...available.\r\n'
b'\tdnsmap...available.\r\n'
b'\tAll Scanning Tools are available. All vulnerability checks will be performed by RapidScan.\r\n'
b'[Checking Available Security Scanning Tools Phase... Completed.]\r\n'
b'\r\n'
b'\r\n'
b'[Preliminary Scan Phase Initiated... Loaded 80.0 vulnerability checks.]\r\n'
b'[\xe2\x97\x8f < 20s] Deploying 1/80.0 | Nmap [XSS Filter Check] - Checks if XSS Protection Header is present. | \x08\x08...Completed in 1s\r\n'
b'\r\n'
b'[\xe2\x97\x8f < 35s] Deploying 2/80.0 | Nmap [LOGJAM] - Checks for LOGJAM Vulnerability. / \x08\x08...Completed in 1s\r\n'
b'\r\n'
b'[\xe2\x97\x8f < 20s] Deploying 3/80.0 | Checks for SMB Service over UDP \\ \x08| \x08\x08...Completed in 1s\r\n'
b'\r\n'
b'[\xe2\x97\x8f < 30s] Deploying 4/80.0 | Nmap [FREAK] - Checks only for FREAK Vulnerability. / \x08\x08...Completed in 1s\r\n'
b'\r\n'
b"[\xe2\x97\x8f < 3m] Deploying 5/80.0 | The Harvester - Scans for emails using Google's passive search. \\ \x08\x08...Completed in 1s\r\n"
b'\r\n'
b'Vulnerability Threat Level\r\n'

b'\t low Email Addresses Found.\r\n'
b'Vulnerability Definition\r\n'
b'\tChances are very less to compromise a target with email addresses. However, attackers use this as a supporting data to gather information around the target. An attacker may make use of the username on the email address and perform brute-force attacks on not just email servers, but also on other legitimate panels like SSH, CMS, etc with a password list as they have a legitimate name. This is however a shoot in the dark scenario, the attacker may or may not be successful depending on the level of interest\r\n'
b'Vulnerability Remediation\r\n'
b'\tSince the chances of exploitation is feeble there is no need to take action. Perfect remediation would be choosing different usernames for different services will be more thoughtful.\r\n'
b'[\xe2\x97\x8f < 35s] Deploying 6/80.0 | Nikto - Checks for MS10-070 Vulnerability. |
\x08\x08...Completed in 1s\r\n'
b'\r\n'
b'Vulnerability Threat Level\r\n'
b'\t high Webserver vulnerable to MS10-070.\r\n'
b'Vulnerability Definition\r\n'
b'\tAn attacker who successfully exploited this vulnerability could read data, such as the view state, which was encrypted by the server. This vulnerability can also be used for data tampering, which, if successfully exploited, could be used to decrypt and tamper with the data encrypted by the server.\r\n'
b'Vulnerability Remediation\r\n'
b'\tMicrosoft has released a set of patches on their website to mitigate this issue. The information required to fix this vulnerability can be inferred from this resource.
https://docs.microsoft.com/en-us/security-updates/securitybulletins/2010/ms10-070\r\n'
b'[\xe2\x97\x8f < 5m] Deploying 7/80.0 | Uniscan - Brutes Directories on the Domain. /
\x08\x08...Completed in 1s\r\n'
b'\r\n'
b'[\xe2\x97\x8f < 35s] Deploying 8/80.0 | Nikto - Checks for Apache Expect XSS Header. \\
\x08\x08...Completed in 1s\r\n'
b'\r\n'
b'Vulnerability Threat Level\r\n'
b'\t medium Apache Expect XSS Header not present.\r\n'
b'Vulnerability Definition\r\n'
b'\tAs the target is lacking this header, older browsers will be prone to Reflected XSS attacks.\r\n'
b'Vulnerability Remediation\r\n'
b'\tModern browsers does not face any issues with this vulnerability (missing headers). However, older browsers are strongly recommended to be upgraded.\r\n'
b'[\xe2\x97\x8f < 30s] Deploying 9/80.0 | DMitry - Passively Harvests Emails from the Domain. |
\x08\x08...Completed in 1s\r\n'
b'\r\n'
b'Vulnerability Threat Level\r\n'
b'\t low Email Addresses discovered with DMitry.\r\n'
b'Vulnerability Definition\r\n'
b'\tChances are very less to compromise a target with email addresses. However, attackers use this as a supporting data to gather information around the target. An attacker may make use of the username on the email address and perform brute-force attacks on not just email servers, but also on other legitimate panels like SSH, CMS, etc with a password list as they have a legitimate name. This is however a shoot in the dark scenario, the attacker may or may not be successful depending on the level of interest\r\n'

b'Vulnerability Remediation\r\n'
b'\tSince the chances of exploitation is feeble there is no need to take action. Perfect remediation would be choosing different usernames for different services will be more thoughtful.\r\n'
b'[\xe2\x97\x8f < 30m] Deploying 10/80.0 | DNSMap - Brutes Subdomains. / \x08\\ \x08\x08...Completed in 1s\r\n'
b'\r\n'
b'[\xe2\x97\x8f < 75m] Deploying 11/80.0 | Fierce Subdomains Bruter - Brute Forces Subdomain Discovery. | \x08/ \x08\\ \x08| \x08/ \x08\\ \x08| \x08/ \x08\\ \x08\x08...Completed in 1s\r\n'
b'\r\n'
b'Vulnerability Threat Level\r\n'
b'\t medium Found Subdomains with Fierce.\r\n'
b'Vulnerability Definition\r\n'
b'\tAttackers may gather more information from subdomains relating to the parent domain. Attackers may even find other services from the subdomains and try to learn the architecture of the target. There are even chances for the attacker to find vulnerabilities as the attack surface gets larger with more subdomains discovered.\r\n'
b'Vulnerability Remediation\r\n'
b'\tIt is sometimes wise to block sub domains like development, staging to the outside world, as it gives more information to the attacker about the tech stack. Complex naming practices also help in reducing the attack surface as attackers find hard to perform subdomain bruteforcing through dictionaries and wordlists.\r\n'
b'[\xe2\x97\x8f < 20s] Deploying 12/80.0 | Nmap [STUXNET] - Checks if the host is affected by STUXNET Worm. | \x08\x08...Completed in 1s\r\n'
b'\r\n'
b'[\xe2\x97\x8f < 30m] Deploying 13/80.0 | Golismero Subdomains Bruter - Brute Forces Subdomain Discovery. / \x08\x08...Completed in 1s\r\n'
b'\r\n'
b'[\xe2\x97\x8f < 35s] Deploying 14/80.0 | Nikto - Checks for Injectable Paths. \\ \x08\x08...Completed in 1s\r\n'
b'\r\n'
b'[\xe2\x97\x8f < 35s] Deploying 15/80.0 | Nikto - Checks if Server is Outdated. | \x08\x08...Completed in 1s\r\n'
b'\r\n'
b'Vulnerability Threat Level\r\n'
b'\t high Webserver is Outdated.\r\n'
b'Vulnerability Definition\r\n'
b"\tAny outdated web server may contain multiple vulnerabilities as their support would've been ended. An attacker may make use of such an opportunity to leverage attacks.\r\n"
b'Vulnerability Remediation\r\n'
b'\tIt is highly recommended to upgrade the web server to the available latest version.\r\n'
b'[\xe2\x97\x8f < 30s] Deploying 16/80.0 | WebDAV - Checks if WEBDAV enabled on Home directory. / \x08\x08...Completed in 1s\r\n'
b'\r\n'
b'[\xe2\x97\x8f < 9m] Deploying 17/80.0 | Uniscan - Stress Tests the Domain. \\ \x08\x08...Completed in 1s\r\n'
b'\r\n'
b'[\xe2\x97\x8f < 40s] Deploying 18/80.0 | Uniscan - Checks for robots.txt & sitemap.xml | \x08\x08...Completed in 1s\r\n'
b'\r\n'

b'[\xe2\x97\x8f < 35s] Deploying 19/80.0 | Nmap [POODLE] - Checks only for Poodle Vulnerability. / \x08\x08...Completed in 1s\r\n'
b'\r\n'
b'[\xe2\x97\x8f < 45m] Deploying 20/80.0 | Nmap [Slowloris DoS] - Checks for Slowloris Denial of Service Vulnerability. \\ \x08\x08...Completed in 1s\r\n'
b'\r\n'
b'[\xe2\x97\x8f < 35s] Deploying 21/80.0 | Nikto - Checks for any interesting files on the Domain. | \x08\x08...Completed in 1s\r\n'
b'\r\n'
b'Vulnerability Threat Level\r\n'
b'\t medium Interesting Files Detected.\r\n'
b'Vulnerability Definition\r\n'
b'\tAttackers may find considerable amount of information from these files. There are even chances attackers may get access to critical information from these files.\r\n'
b'Vulnerability Remediation\r\n'
b'\tIt is recommended to block or restrict access to these files unless necessary.\r\n'
b'[\xe2\x97\x8f < 8m] Deploying 22/80.0 | Uniscan - Checks for LFI, RFI and RCE. / \x08\x08...Completed in 1s\r\n'
b'\r\n'
b'[\xe2\x97\x8f < 30s] Deploying 23/80.0 | Checks for ASP.net Elmah Logger \\ \x08\x08...Completed in 1s\r\n'
b'\r\n'
b'[\xe2\x97\x8f < 35s] Deploying 24/80.0 | Nmap [OpenSSL CCS Injection] - Checks only for CCS Injection. | \x08\x08...Completed in 1s\r\n'
b'\r\n'
b'[\xe2\x97\x8f < 40s] Deploying 25/80.0 | Nmap - Checks for IIS WebDAV / \x08\x08...Completed in 1s\r\n'
b'\r\n'
b'[\xe2\x97\x8f < 35s] Deploying 26/80.0 | Nikto - Checks for Server Issues. \\ \x08\x08...Completed in 1s\r\n'
b'\r\n'
b'Vulnerability Threat Level\r\n'
b'\t medium Some issues found on the Webserver.\r\n'
b'Vulnerability Definition\r\n'
b'\tParticular Scanner found multiple vulnerabilities that an attacker may try to exploit the target.\r\n'
b'Vulnerability Remediation\r\n'
b'\tRefer to RS-Vulnerability-Report to view the complete information of the vulnerability, once the scan gets completed.\r\n'
b'[\xe2\x97\x8f < 30s] Deploying 27/80.0 | WordPress Checker - Checks for WordPress Installation. | \x08\x08...Completed in 1s\r\n'
b'\r\n'
b'[\xe2\x97\x8f < 45s] Deploying 28/80.0 | Golismero - Checks if the domain is spoofed or hijacked. / \x08\x08...Completed in 1s\r\n'
b'\r\n'
b'Vulnerability Threat Level\r\n'
b'\t high Domain is spoofed/hijacked.\r\n'
b'Vulnerability Definition\r\n'
b"\tAn attacker can forwarded requests that comes to the legitimate URL or web application to a third party address or to the attacker's location that can serve malware and affect the end user's

machine.\r\n"
b'Vulnerability Remediation\r\n'
b'\tIt is highly recommended to deploy DNSSec on the host target. Full deployment of DNSSEC will ensure the end user is connecting to the actual web site or other service corresponding to a particular domain name. For more information, check this resource.
https://www.cloudflare.com/dns/dnssec/how-dnssec-works/\r\n'
b'[\xe2\x97\x8f > 75m] Deploying 29/80.0 | Nmap - Performs a Full UDP Port Scan \\ \x08\x08...Completed in 1s\r\n'
b'\r\n'
b'[\xe2\x97\x8f < 45s] Deploying 30/80.0 | Golismero SSL Scans - Performs SSL related Scans. | \x08\x08...Completed in 1s\r\n'
b'\r\n'
b'[\xe2\x97\x8f < 20s] Deploying 31/80.0 | Checks for SMB Service over TCP / \x08\x08...Completed in 1s\r\n'
b'\r\n'
b'[\xe2\x97\x8f < 35s] Deploying 32/80.0 | Nikto - Brutes Subdomains. \\ \x08\x08...Completed in 1s\r\n'
b'\r\n'
b'Vulnerability Threat Level\r\n'
b'\t medium Found Subdomains with Nikto.\r\n'
b'Vulnerability Definition\r\n'
b'\tAttackers may gather more information from subdomains relating to the parent domain. Attackers may even find other services from the subdomains and try to learn the architecture of the target. There are even chances for the attacker to find vulnerabilities as the attack surface gets larger with more subdomains discovered.\r\n'
b'Vulnerability Remediation\r\n'
b'\tIt is sometimes wise to block sub domains like development, staging to the outside world, as it gives more information to the attacker about the tech stack. Complex naming practices also help in reducing the attack surface as attackers find hard to perform subdomain bruteforcing through dictionaries and wordlists.\r\n'
b'[\xe2\x97\x8f < 45s] Deploying 33/80.0 | Golismero - BruteForces for certain files on the Domain. | \x08\x08...Completed in 1s\r\n'
b'\r\n'
b'Vulnerability Threat Level\r\n'
b'\t medium Open Files Found with Golismero BruteForce.\r\n'
b'Vulnerability Definition\r\n'
b'\tAttackers may find considerable amount of information from these files. There are even chances attackers may get access to critical information from these files.\r\n'
b'Vulnerability Remediation\r\n'
b'\tIt is recommended to block or restrict access to these files unless necessary.\r\n'
b'[\xe2\x97\x8f < 15s] Deploying 34/80.0 | Nmap [TELNET] - Checks if TELNET service is running. / \x08\x08...Completed in 1s\r\n'
b'\r\n'
b'[\xe2\x97\x8f < 35s] Deploying 35/80.0 | Nikto - Checks for HTTP Options on the Domain. \\ \x08\x08...Completed in 1s\r\n'
b'\r\n'
b'Vulnerability Threat Level\r\n'
b'\t low Some issues found with HTTP Options.\r\n'
b'Vulnerability Definition\r\n'
b'\tThere are chances for an attacker to manipulate files on the webserver.\r\n'

b'Vulnerability Remediation\r\n'
b"\tIt is recommended to disable the HTTP PUT and DEL methods incase if you don't use any REST API Services. Following resources helps you how to disable these methods.
http://www.techstacks.com/howto/disable-http-methods-in-tomcat.html
https://docs.oracle.com/cd/E19857-01/820-5627/gghwc/index.html
https://developer.ibm.com/answers/questions/321629/how-to-disable-http-methods-head-put-delete-option/\r\n"
b'[\xe2\x97\x8f < 30s] Deploying 36/80.0 | Drupal Checker - Checks for Drupal Installation. | \x08\x08...Completed in 1s\r\n'
b'\r\n'
b'[\xe2\x97\x8f < 15s] Deploying 37/80.0 | Nmap - Checks for Remote Desktop Service over UDP / \x08\x08...Completed in 1s\r\n'
b'\r\n'
b'[\xe2\x97\x8f < 5m] Deploying 38/80.0 | Wapiti - Checks for SQLi, RCE, XSS and Other Vulnerabilities \\ \x08\x08...Completed in 1s\r\n'
b'\r\n'
b'[\xe2\x97\x8f < 30s] Deploying 39/80.0 | Nmap [Heartbleed] - Checks only for Heartbleed Vulnerability. | \x08\x08...Completed in 1s\r\n'
b'\r\n'
b'[\xe2\x97\x8f < 35s] Deploying 40/80.0 | Nikto - Checks for HTTP PUT DEL. / \x08\x08...Completed in 1s\r\n'
b'\r\n'
b'Vulnerability Threat Level\r\n'
b'\t medium HTTP PUT DEL Methods Enabled.\r\n'
b'Vulnerability Definition\r\n'
b'\tThere are chances for an attacker to manipulate files on the webserver.\r\n'
b'Vulnerability Remediation\r\n'
b"\tIt is recommended to disable the HTTP PUT and DEL methods incase if you don't use any REST API Services. Following resources helps you how to disable these methods.
http://www.techstacks.com/howto/disable-http-methods-in-tomcat.html
https://docs.oracle.com/cd/E19857-01/820-5627/gghwc/index.html
https://developer.ibm.com/answers/questions/321629/how-to-disable-http-methods-head-put-delete-option/\r\n"
b'[\xe2\x97\x8f < 15s] Deploying 41/80.0 | Host - Checks for existence of IPV6 address. \\ \x08\x08...Completed in 1s\r\n'
b'\r\n'
b'Vulnerability Threat Level\r\n'
b'\t info Does not have an IPv6 Address. It is good to have one.\r\n'
b'Vulnerability Definition\r\n'
b'\tNot a vulnerability, just an informational alert. The host does not have IPv6 support. IPv6 provides more security as IPSec (responsible for CIA - Confidentiality, Integrity and Availablity) is incorporated into this model. So it is good to have IPv6 Support.\r\n'
b'Vulnerability Remediation\r\n'
b'\tIt is recommended to implement IPv6. More information on how to implement IPv6 can be found from this resource.
https://www.cisco.com/c/en/us/solutions/collateral/enterprise/cisco-on-cisco/IPv6-Implementation_CS.html\r\n'
b'[\xe2\x97\x8f < 35s] Deploying 42/80.0 | DNSWalk - Attempts Zone Transfer. | \x08/ \x08\x08...Completed in 1s\r\n'

b'\r\n'
b'[\xe2\x97\x8f < 30s] Deploying 43/80.0 | Nmap - Checks for SNMP Service \\ \x08\x08...Completed in 1s\r\n'
b'\r\n'
b'[\xe2\x97\x8f > 50m] Deploying 44/80.0 | Nmap - Performs a Full TCP Port Scan | \x08\x08...Completed in 1s\r\n'
b'\r\n'
b'[\xe2\x97\x8f < 15s] Deploying 45/80.0 | Nmap - Checks for ORACLE DB / \x08\x08...Completed in 1s\r\n'
b'\r\n'
b'[\xe2\x97\x8f < 4m] Deploying 46/80.0 | LBD - Checks for DNS/HTTP Load Balancers. \\ \x08\x08...Completed in 1s\r\n'
b'\r\n'
b'[\xe2\x97\x8f < 15s] Deploying 47/80.0 | Nmap - Checks for MySQL DB | \x08\x08...Completed in 1s\r\n'
b'\r\n'
b'[\xe2\x97\x8f < 15s] Deploying 48/80.0 | Golismero - Does a fingerprint on the Domain. / \x08\x08...Completed in 1s\r\n'
b'\r\n'
b'Vulnerability Threat Level\r\n'
b'\t low Found some information through Fingerprinting.\r\n'
b'Vulnerability Definition\r\n'
b'\tAttackers always do a fingerprint of any server before they launch an attack. Fingerprinting gives them information about the server type, content- they are serving, last modification times etc, this gives an attacker to learn more information about the target\r\n'
b'Vulnerability Remediation\r\n'
b"\tA good practice is to obfuscate the information to outside world. Doing so, the attackers will have tough time understanding the server's tech stack and therefore leverage an attack.\r\n"
b'[\xe2\x97\x8f < 30s] Deploying 49/80.0 | Joomla Checker - Checks for Joomla Installation. \\ \x08\x08...Completed in 1s\r\n'
b'\r\n'
b'[\xe2\x97\x8f < 2m] Deploying 50/80.0 | Nmap - Fast Scan [Only Few Port Checks] | \x08\x08...Completed in 1s\r\n'
b'\r\n'
b'[\xe2\x97\x8f < 4m] Deploying 51/80.0 | XSSer - Checks for Cross-Site Scripting [XSS] Attacks. / \x08\x08...Completed in 1s\r\n'
b'\r\n'
b'Vulnerability Threat Level\r\n'
b'\t critical XSSer found XSS vulnerabilities.\r\n'
b'Vulnerability Definition\r\n'
b'\tAn attacker will be able to steal cookies, deface web application or redirect to any third party address that can serve malware.\r\n'
b'Vulnerability Remediation\r\n'
b'\tInput validation and Output Sanitization can completely prevent Cross Site Scripting (XSS) attacks. XSS attacks can be mitigated in future by properly following a secure coding methodology. The following comprehensive resource provides detailed information on fixing this vulnerability. https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet\r\n'
b'[\xe2\x97\x8f < 45s] Deploying 52/80.0 | DNSEnum - Attempts Zone Transfer. \\ \x08\x08...Completed in 1s\r\n'

b'\r\n'
b'Vulnerability Threat Level\r\n'
b'\t high Zone Transfer Successful using DNSEnum. Reconfigure DNS immediately.\r\n'
b'Vulnerability Definition\r\n'
b'\tZone Transfer reveals critical topological information about the target. The attacker will be able to query all records and will have more or less complete knowledge about your host.\r\n'
b'Vulnerability Remediation\r\n'
b'\tGood practice is to restrict the Zone Transfer by telling the Master which are the IPs of the slaves that can be given access for the query. This SANS resource provides more information. https://www.sans.org/reading-room/whitepapers/dns/securing-dns-zone-transfer-868\r\n'
b'[\xe2\x97\x8f < 35s] Deploying 53/80.0 | Nikto - Checks the Domain Headers. | \x08\x08...Completed in 1s\r\n'
b'\r\n'
b'Vulnerability Threat Level\r\n'
b'\t medium Some vulnerable headers exposed.\r\n'
b'Vulnerability Definition\r\n'
b'\tAttackers try to learn more about the target from the amount of information exposed in the headers. An attacker may know what type of tech stack a web application is emphasizing and many other information.\r\n'
b'Vulnerability Remediation\r\n'
b'\tBanner Grabbing should be restricted and access to the services from outside would should be made minimum.\r\n'
b'[\xe2\x97\x8f < 35m] Deploying 54/80.0 | DirB - Brutes the target for Open Directories. / \x08\x08...Completed in 1s\r\n'
b'\r\n'
b'Vulnerability Threat Level\r\n'
b'\t medium Open Directories Found with DirB.\r\n'
b'Vulnerability Definition\r\n'
b'\tAttackers may find considerable amount of information from these directories. There are even chances attackers may get access to critical information from these directories.\r\n'
b'Vulnerability Remediation\r\n'
b'\tIt is recommended to block or restrict access to these directories unless necessary.\r\n'
b'[\xe2\x97\x8f < 30s] Deploying 55/80.0 | ASP.Net Misconfiguration - Checks for ASP.Net Misconfiguration. \\ \x08\x08...Completed in 1s\r\n'
b'\r\n'
b'[\xe2\x97\x8f < 15s] Deploying 56/80.0 | Nmap - Checks for MS-SQL Server DB | \x08\x08...Completed in 1s\r\n'
b'\r\n'
b'[\xe2\x97\x8f < 35s] Deploying 57/80.0 | Nikto - Enumerates CGI Directories. / \x08\x08...Completed in 1s\r\n'
b'\r\n'
b'Vulnerability Threat Level\r\n'
b'\t low CGI Directories Enumerated.\r\n'
b'Vulnerability Definition\r\n'
b'\tAttackers may find considerable amount of information from these directories. There are even chances attackers may get access to critical information from these directories.\r\n'
b'Vulnerability Remediation\r\n'
b'\tIt is recommended to block or restrict access to these directories unless necessary.\r\n'
b'[\xe2\x97\x8f < 30s] Deploying 58/80.0 | SSLyze - Checks for Session Resumption Support with

[Session IDs/TLS Tickets]. \\ \x08\x08...Completed in 1s\r\n'
b'\r\n'
b'[\xe2\x97\x8f < 20s] Deploying 59/80.0 | DNSRecon - Attempts Multiple Zone Transfers on Nameservers. | \x08\x08...Completed in 1s\r\n'
b'\r\n'
b'[\xe2\x97\x8f < 15s] Deploying 60/80.0 | Nmap - Checks for Remote Desktop Service over TCP / \x08\x08...Completed in 1s\r\n'
b'\r\n'
b'[\xe2\x97\x8f < 4m] Deploying 61/80.0 | Golismero Nikto Scans - Uses Nikto Plugin to detect vulnerabilities. \\ \x08\x08...Completed in 1s\r\n'
b'\r\n'
b'Vulnerability Threat Level\r\n'
b'\t medium Golismero Nikto Plugin found vulnerabilities.\r\n'
b'Vulnerability Definition\r\n'
b'\tParticular Scanner found multiple vulnerabilities that an attacker may try to exploit the target.\r\n'
b'Vulnerability Remediation\r\n'
b'\tRefer to RS-Vulnerability-Report to view the complete information of the vulnerability, once the scan gets completed.\r\n'
b'[\xe2\x97\x8f < 3m] Deploying 62/80.0 | WhatWeb - Checks for X-XSS Protection Header | \x08\x08...Completed in 1s\r\n'
b'\r\n'
b'Vulnerability Threat Level\r\n'
b'\t medium X-XSS Protection is not Present\r\n'
b'Vulnerability Definition\r\n'
b'\tAs the target is lacking this header, older browsers will be prone to Reflected XSS attacks.\r\n'
b'Vulnerability Remediation\r\n'
b'\tModern browsers does not face any issues with this vulnerability (missing headers). However, older browsers are strongly recommended to be upgraded.\r\n'
b'[\xe2\x97\x8f < 35s] Deploying 63/80.0 | Nikto - Checks for Internal IP Leak. / \x08\x08...Completed in 1s\r\n'
b'\r\n'
b'Vulnerability Threat Level\r\n'
b'\t low Webserver leaks Internal IP.\r\n'
b'Vulnerability Definition\r\n'
b"\tGives attacker an idea on how the address scheming is done internally on the organizational network. Discovering the private addresses used within an organization can help attackers in carrying out network-layer attacks aiming to penetrate the organization's internal infrastructure.\r\n"
b'Vulnerability Remediation\r\n'
b'\tRestrict the banner information to the outside world from the disclosing service. More information on mitigating this vulnerability can be found here.
https://portswigger.net/kb/issues/00600300_private-ip-addresses-disclosed\r\n'
b'[\xe2\x97\x8f < 40s] Deploying 64/80.0 | Golismero - BruteForces for certain directories on the Domain. \\ \x08\x08...Completed in 1s\r\n'
b'\r\n'
b'Vulnerability Threat Level\r\n'
b'\t medium Open Directories Found with Golismero BruteForce.\r\n'
b'Vulnerability Definition\r\n'
b'\tAttackers may find considerable amount of information from these directories. There are even chances attackers may get access to critical information from these directories.\r\n'

b'Vulnerability Remediation\r\n'
b'\tIt is recommended to block or restrict access to these directories unless necessary.\r\n'
b'[\xe2\x97\x8f < 45s] Deploying 65/80.0 | Golismero - SQLMap [Retrieves only the DB Banner] | \x08\x08...Completed in 1s\r\n'
b'\r\n'
b'Vulnerability Threat Level\r\n'
b'\t low DB Banner retrieved with SQLMap.\r\n'
b'Vulnerability Definition\r\n'
b'\tMay not be SQLi vulnerable. An attacker will be able to know that the host is using a backend for operation.\r\n'
b'Vulnerability Remediation\r\n'
b'\tBanner Grabbing should be restricted and access to the services from outside would should be made minimum.\r\n'
b"[\xe2\x97\x8f < 25s] Deploying 66/80.0 | WHOis - Checks for Administrator's Contact Information. / \x08\\ \x08\x08...Completed in 1s\r\n"
b'\r\n'
b'[\xe2\x97\x8f < 30s] Deploying 67/80.0 | Fierce - Attempts Zone Transfer [No Brute Forcing] | \x08/ \x08\\ \x08| \x08/ \x08\\ \x08| \x08/ \x08\\ \x08| \x08\x08...Completed in 1s\r\n'
b'\r\n'
b'[\xe2\x97\x8f < 30s] Deploying 68/80.0 | SSLyze - Checks for ZLib Deflate Compression. / \x08\x08...Completed in 1s\r\n'
b'\r\n'
b'[\xe2\x97\x8f < 2m] Deploying 69/80.0 | Uniscan - Brutes for Filenames on the Domain. \\ \x08\x08...Completed in 1s\r\n'
b'\r\n'
b'[\xe2\x97\x8f < 35s] Deploying 70/80.0 | DMitry - Passively Harvests Subdomains from the Domain. | \x08\x08...Completed in 1s\r\n'
b'\r\n'
b'Vulnerability Threat Level\r\n'
b'\t medium Subdomains discovered with DMitry.\r\n'
b'Vulnerability Definition\r\n'
b'\tAttackers may gather more information from subdomains relating to the parent domain. Attackers may even find other services from the subdomains and try to learn the architecture of the target. There are even chances for the attacker to find vulnerabilities as the attack surface gets larger with more subdomains discovered.\r\n'
b'Vulnerability Remediation\r\n'
b'\tIt is sometimes wise to block sub domains like development, staging to the outside world, as it gives more information to the attacker about the tech stack. Complex naming practices also help in reducing the attack surface as attackers find hard to perform subdomain bruteforcing through dictionaries and wordlists.\r\n'
b'[\xe2\x97\x8f < 9m] Deploying 71/80.0 | Uniscan - Checks for XSS, SQLi, BSQLi & Other Checks. / \x08\x08...Completed in 1s\r\n'
b'\r\n'
b'[\xe2\x97\x8f < 45s] Deploying 72/80.0 | Wafw00f - Checks for Application Firewalls. \\ \x08| \x08/ \x08\\ \x08\x08...Completed in 1s\r\n'
b'\r\n'
b'[\xe2\x97\x8f < 40s] Deploying 73/80.0 | SSLyze - Checks only for Heartbleed Vulnerability. | \x08\x08...Completed in 1s\r\n'
b'\r\n'

b'[\xe2\x97\x8f < 25s] Deploying 74/80.0 | SSLyze - Checks for Secure Renegotiation Support and Client Renegotiation. / \x08\x08...Completed in 1s\r\n'
b'\r\n'
b'[\xe2\x97\x8f < 35s] Deploying 75/80.0 | Nikto - Performs SSL Checks. \\ \x08\x08...Completed in 1s\r\n'
b'\r\n'
b'Vulnerability Threat Level\r\n'
b'\t medium Vulnerabilities reported in SSL Scans.\r\n'
b'Vulnerability Definition\r\n'
b'\tSSL related vulnerabilities breaks the confidentiality factor. An attacker may perform a MiTM attack, intrepret and eavesdrop the communication.\r\n'
b'Vulnerability Remediation\r\n'
b'\tProper implementation and upgraded version of SSL and TLS libraries are very critical when it comes to blocking SSL related vulnerabilities.\r\n'
b'[\xe2\x97\x8f < 30s] Deploying 76/80.0 | Golismero Zone Transfer - Attempts Zone Transfer. | \x08\x08...Completed in 1s\r\n'
b'\r\n'
b'[\xe2\x97\x8f < 35s] Deploying 77/80.0 | Nikto - Checks for Shellshock Bug. / \x08\x08...Completed in 1s\r\n'
b'\r\n'
b'Vulnerability Threat Level\r\n'
b'\t critical Webserver vulnerable to Shellshock Bug.\r\n'
b'Vulnerability Definition\r\n'
b'\tAttackers exploit the vulnerability in BASH to perform remote code execution on the target. An experienced attacker can easily take over the target system and access the internal sources of the machine\r\n'
b'Vulnerability Remediation\r\n'
b'\tThis vulnerability can be mitigated by patching the version of BASH. The following resource gives an indepth analysis of the vulnerability and how to mitigate it.
https://www.symantec.com/connect/blogs/shellshock-all-you-need-know-about-bash-bug-vulnerability
https://www.digitalocean.com/community/tutorials/how-to-protect-your-server-against-the-shellshock-bash-vulnerability\r\n'
b'[\xe2\x97\x8f < 15s] Deploying 78/80.0 | Nmap [FTP] - Checks if FTP service is running. \\ \x08\x08...Completed in 1s\r\n'
b'\r\n'
b'[\xe2\x97\x8f < 25s] Deploying 79/80.0 | SSLyze - Checks for OCSP Stapling. | \x08\x08...Completed in 1s\r\n'
b'\r\n'
b'[\xe2\x97\x8f < 40s] Deploying 80/80.0 | Golismero - Checks only for Heartbleed Vulnerability. / \x08\x08...Completed in 1s\r\n'
b'\r\n'
b'Vulnerability Threat Level\r\n'
b'\t high HEARTBLEED Vulnerability Found with Golismero.\r\n'
b'Vulnerability Definition\r\n'
b'\tThis vulnerability seriously leaks private information of your host. An attacker can keep the TLS connection alive and can retrieve a maximum of 64K of data per heartbeat.\r\n'
b'Vulnerability Remediation\r\n'
b'\tPFS (Perfect Forward Secrecy) can be implemented to make decryption difficult. Complete remediation and resource information is available here. http://heartbleed.com/\r\n'

b'[Preliminary Scan Phase Completed.]\r\n'
b'\r\n'
b'\r\n'
b'[Report Generation Phase Initiated.]\r\n'
b'\tComplete Vulnerability Report for iclan.cm named `RS-Vulnerability-Report` is available under the same directory RapidScan resides.\r\n'
b'\tTotal Number of Vulnerability Checks : 80\r\n'
b'\tTotal Number of Vulnerability Checks Skipped: 0\r\n'
b'\tTotal Number of Vulnerabilities Detected : 29\r\n'
b'\tTotal Time Elapsed for the Scan : 7s\r\n'
b'\r\n'
b'\r\n'
b'\tFor Debugging Purposes, You can view the complete output generated by all the tools named `RS-Debug-ScanLog` under the same directory.\r\n'
b'[Report Generation Phase Completed.]\r\n'