

METHOD AND SYSTEM FOR DETERMINING NETWORK VULNERABILITIES

TECHNICAL FIELD

[1]The present technology broadly relates to the area of information security; and in particular, to remote scanning network architecture elements.

BACKGROUND

[2]Scanners are hardware or software tools used for diagnostics and monitoring a network and structural nodes thereof (also referred to herein as “network architecture elements”). These tools can be configured to scan networks, computers and applications run thereon for possible security issues, and evaluate and report identified information in order to prevent future occurrences of the vulnerabilities.

[3]Modern scanners may be applied to various segments of the network enabling to obtain comprehensive information about a current security status thereof. Due to distributed architecture, all data about identified vulnerabilities and flaws may be consolidated in a single location. Therefore, it may be possible to track changes in the network by automatically comparing the scanned data at different moments in time, and by constantly monitoring the changes.

[4]Certain prior art approaches are directed to specific implementations of such scanners.

[5]**Chinese Patent No.: CN 105,429,955-B** issued on December 11, 2018 and entitled “*A Kind of Detection Method of Long-Range Loophole*” discloses The invention discloses a kind of detection methods of long-range loophole, include: first step creation scan node: clicking addition task in scanner home page first, python code is replicated in one column of node, is run in python environment on the server as node, can be created node; Second step adds scan address: the network address scanned will be needed to be added in scan box in one column of addition task, and selects Scanning Options, addition task can be completed; Third step opens scanning: the option that selection needs to scan on one column of option after the addition was complete, click start to be scanned.4th step checks scanning result: can obtain the loophole list of targeted website after the completion of scanning, contain the detailed vulnerability information of targeted website.

[6]**United States Patent Application Publication No.: 2004/0193918-A1**published on September 30, 2004, assigned to Trustwave Holdings Inc., and entitled “*Apparatus and Method for Network*

Vulnerability Detection and Compliance Assessment” discloses an apparatus and method for detecting vulnerabilities in networks. In particular, the present invention may relate to an apparatus and method for detecting network security flaws in a computer network. The types of computer networks which the present invention may aid in protecting include both local area and other private networks, and networks connected to the internet or a similar wide area public network.

[7]**PCT Patent Application Publication No.: WO 2019/153384-A1** published on August 15, 2019 and entitled “*Vulnerability Scanning Method and System, and Server*” discloses a vulnerability scanning method and system, and a server. The method comprises: recognizing a host service running in a target host and establishing a scanning task adapting to the recognized host service; distributing the established scanning task to a task scheduling center so that a proxy node obtains at least one scanning task from the task scheduling center, the scanning result being obtained after executing, by the proxy node, the at least one scanning task for the target host; and receiving the scanning result fed back by the proxy node and determining whether a designated host service exists in the recognized host service, the designated host service being used for indicating whether a website resource runs in the target host; if yes, re-distributing the scanning sub-task corresponding to the designated host service to the task scheduling center. The technical solution provided by the present application can improve the vulnerability scanning precision.

SUMMARY

[8]It is an object of the present technology to ameliorate at least some of the shortcomings present in the prior art.

[9]Developers of the present technology have realized that the prior art approaches lack flexibility as most of them require predetermined tasks for scanning the network for detection a specific vulnerability (or a specific set thereof) therein. Further, some of the known approaches require manual selection of the tasks.

[10] Thus, the developers have devised methods and systems for determining vulnerabilities associated with network architecture elements of the network based on respective task templates having been automatically determined therefor. More specifically, non-limiting embodiments of the present technology are directed to iteratively determining network architecture elements and vulnerabilities therein, based on previously identified vulnerabilities.

[11] For example, for identifying vulnerabilities associated with a given network architecture element, a respective task template may be used, which has automatically been pre-configured for

detecting vulnerabilities associated specifically with this given network architecture element. The detected vulnerabilities may further be indicative of links between the given network architecture element and some other ones, which can thus be verified for further potential vulnerabilities using a different task template. By doing so, the determining further network architecture elements and examining thereof for potential vulnerabilities continue until no further vulnerability can be identified.

[12] Therefore, according to a first broad aspect of the present technology, there is provided a method for determining vulnerabilities on a network. The method being executable by a processor. The method comprising: receiving, by the processor, data indicative of a first network architecture element; determining, by the processor, based on the data indicative of the first network architecture element, a respective one of a plurality of predetermined task templates, the respective one of the plurality of predetermined task templates including one or more tasks executable for identifying respective vulnerabilities associated with the first network architecture element; in response to identifying, based on the respective one of the plurality of predetermined task templates, at least one vulnerability associated with the first network architecture element, the at least one vulnerability providing access to a second network architecture element associated with the first network architecture element: determining, by the processor, data indicative of the second network architecture element; storing, by the processor, the data indicative of the second network architecture element in a database; and using, by the processor, the data indicative of the second network architecture element for identifying further vulnerabilities on the network.

[13] In some implementations of the method, the first network architecture element is associated with a first network architecture element type comprising at least one of: an IP address, a website, a Uniform Resource Locator (URL), a domain name, and a network port.

[14] In some implementations of the method, if the first network architecture element type is the domain name, the method further comprises verifying, by the processor, availability of the domain name using a WHOIS web service.

[15] In some implementations of the method, the method further comprises determining, by the processor, using the WHOIS web service, registration data associated with an owner of the domain name.

[16] In some implementations of the method, the verifying the availability of the domain name further comprises analyzing, by the processor, data responsive to requests for random subdomain names associated with the domain name.

[17] In some implementations of the method, if the first network architecture element type is the website, the method further comprises verifying, by the processor, availability of the website, the verifying comprising establishing a connection with the website, the connection being one of a direct connection and a connection via a proxy server.

[18] In some implementations of the method, if the first network architecture element type is the URL, the method further comprises verifying availability of the URL, the verifying comprising transmitting, by the processor, at least one request to a webserver associated with the URL, and the verifying further comprising at least one of: analyzing a response code of a response received from the webserver associated with the URL; a content associated with the response; a header of the response; and a type of the URL, wherein the type of the URL is associated with one of a file, a directory, and underdetermined.

[19] In some implementations of the method, the verifying the availability of the URL further comprises determining at least one of: if the URL is responsive to requests for non-existing files; if the URL is associated with a predetermined exclusion template; if the webserver associated with the URL is configured to redirect the at least one request to at least one another URL, and determining the at least one another URL.

[20] In some implementations of the method, the data indicative of the first network architecture element is received from one of: a user input and the database.

[21] In some implementations of the method, the the respective one of the plurality of predetermined task templates is associated with a plurality of network architecture element types, to which the respective one of the plurality of predetermined task templates is applicable.

[22] In some implementations of the method, the one or more tasks comprise at least one of: tasks for identifying subdomain names; tasks for identifying URLs; tasks for identifying open network ports; tasks for retrieving information of at least one web service associated with the open network ports; tasks for password mining for accessing the at least one web service associated with the open network ports; and tasks for identifying vulnerabilities associated with the at least one web service.

[23] In some implementations of the method, the method further comprises: receiving, by the processor, the data indicative of the second network architecture element; determining, by the processor, based on the data indicative of the second network architecture element, another one of the plurality of predetermined task templates, the other one of the plurality of predetermined task templates including one or more tasks executable for identifying respective vulnerabilities

associated with the second network architecture element; in response to identifying, based on the other one of the plurality of predetermined task templates, at least one vulnerability associated with the second network architecture element, the at least one vulnerability providing access to a third network architecture element associated with the second network architecture element: determining, by the processor, data indicative of the third network architecture element; storing, by the processor, the data indicative of the third network architecture element in the database; and using, by the processor, the data indicative of the third network architecture element for identifying further vulnerabilities on the network.

[24] In some implementations of the method, the method further comprises iteratively repeating at least the steps of the receiving data and the determining a predetermined task template until no further vulnerability is identified.

[25] In some implementations of the method, the method further comprises generating, at each iteration, an intermediate report including data of vulnerabilities having been identified on the network.

[26] In some implementations of the method, the other one of the plurality of predetermined task templates is a same as the respective one of the plurality of predetermined task templates.

[27] In some implementations of the method, the other one of the plurality of predetermined task templates is at least partially different from the respective one of a plurality of predetermined task templates.

[28] According to a second broad aspect of the present technology, there is provided a system for determining vulnerabilities on a network. The system comprises a computing device. The computing device further comprises: a processor; a non-transitory computer-readable medium comprising instructions. The processor, upon executing the instructions, is configured to: receive data indicative of a first network architecture element; determine based on the data indicative of the first network architecture element, a respective one of a plurality of predetermined task templates, the respective one of the plurality of predetermined task templates including one or more tasks executable for identifying respective vulnerabilities associated with the first network architecture element; in response to identifying, based on the respective one of the plurality of predetermined task templates, at least one vulnerability associated with the first network architecture element, the at least one vulnerability providing access to a second network architecture element associated with the first network architecture element: determine data indicative of the second network architecture element; store the data indicative of the second network architecture element in a database; and use

the data indicative of the second network architecture element for identifying further vulnerabilities on the network.

[29] In some implementations of the system, the processor is further configured to: receive the data indicative of the second network architecture element; determine, based on the data indicative of the second network architecture element, another one of the plurality of predetermined task templates, the other one of the plurality of predetermined task templates including one or more tasks executable for identifying respective vulnerabilities associated with the second network architecture element; in response to identifying, based on the other one of the plurality of predetermined task templates, at least one vulnerability associated with the second network architecture element, the at least one vulnerability providing access to a third network architecture element associated with the second network architecture element: determine data indicative of the third network architecture element; store the data indicative of the third network architecture element in the database; and use the data indicative of the third network architecture element for identifying further vulnerabilities on the network.

[30] In some implementations of the system, the processor is further configured to iteratively repeat at least the steps of the receiving data and the determining a predetermined task template until no further vulnerability is identified.

[31] In some implementations of the system, the processor is further configured to generate, at each iteration, an intermediate report including data of vulnerabilities having been identified on the network.

[32] In the context of the present specification, unless expressly provided otherwise, a computer system may refer, but is not limited to, an “electronic device”, an “operation system”, a “system”, a “computer-based system”, a “controller unit”, a “control device” and/or any combination thereof appropriate to the relevant task at hand.

[33] In the context of the present specification, unless expressly provided otherwise, the expression “computer-readable medium” and “memory” are intended to include media of any nature and kind whatsoever, non-limiting examples of which include RAM, ROM, disks (CD-ROMs, DVDs, floppy disks, hard disk drives, etc.), USB keys, flash memory cards, solid state-drives, and tape drives.

[34] In the context of the present specification, a “database” is any structured collection of data, irrespective of its particular structure, the database management software, or the computer hardware

on which the data is stored, implemented or otherwise rendered available for use. A database may reside on the same hardware as the process that stores or makes use of the information stored in the database or it may reside on separate hardware, such as a dedicated server or plurality of servers.

[35] In the context of the present specification, unless expressly provided otherwise, the words “first”, “second”, “third”, etc. have been used as adjectives only for the purpose of allowing for distinction between the nouns that they modify from one another, and not for the purpose of describing any particular relationship between those nouns.

[36] Embodiments of the present technology each have at least one of the above-mentioned object and/or aspects, but do not necessarily have all of them. It should be understood that some aspects of the present technology that have resulted from attempting to attain the above-mentioned object may not satisfy this object and/or may satisfy other objects not specifically recited herein.

[37] Additional and/or alternative features, aspects and advantages of embodiments of the present technology will become apparent from the following description, the accompanying drawings and the appended claims.

BRIEF DESCRIPTION OF DRAWINGS

[38] Non-limiting embodiments of the present technology are described herein with reference to the accompanying drawings; these drawings are only presented to explain the essence of the technology and are not limiting the scope of the present technology in any way, where:

[39] Figure 1 depicts a flowchart diagram of an example sequence of steps executed for scanning a network for determining vulnerabilities associated with a given network architecture element, in accordance with certain non-limiting embodiments of the present technology;

[40] Figure 2 depicts a schematic diagram of a predetermined task template used for determining vulnerabilities associated with the given network architecture element, in accordance with certain non-limiting embodiments of the present technology;

[41] Figure 3 depicts a schematic diagram of a process of using the predetermined task template of Figure 2 by a task manager module for scanning the network, in accordance with certain non-limiting embodiments of the present technology;

[1]Figure 4 depicts a schematic diagram of an example computing environment configurable for execution of the method of Figure 1, in accordance with certain non-limiting embodiments of the present technology.

DETAILED DESCRIPTION

[42] The following detailed description is provided to enable any one skilled in the art to implement and use the non-limiting embodiments of the present technology. Specific details are provided merely for descriptive purposes and to give insights into the present technology, and no way as a limitation. However, it would be apparent for a person skilled in the art that some of these specific details may not be necessary to implement certain non-limiting embodiments of the present technology. The descriptions of specific implementations are only provided as representative examples. Various modifications of these embodiments may become apparent to the person skilled in the art; the general principles defined in this document may be applied to other non-limiting embodiments and implementations without departing from the scope of the present technology.

[43] Certain non-limiting embodiments of the present technology are directed to systems and methods for identifying vulnerabilities associated with network architecture elements of a network.

[44] According to certain non-limiting embodiments of the present technology, a process for identifying vulnerabilities associated with a given network architecture element may be broken down into four stages: (1) data collection, (2) binding, (3) evaluation, and (4) penetration.

[45] According to certain non-limiting embodiments of the present technology, at the data collection stage, via scanning the network, a plurality of network architecture elements, such as network devices, may be identified. Further, at the binding and evaluation stages a given network architecture element, for example, running a certain service or application may be identified. Further, the given network architecture element may be examined for possible vulnerabilities. Finally, at the penetration stage, the so identified vulnerabilities may further be used to determine other network architecture elements, associated with the given one, within which further vulnerabilities may be identified.

[46] With reference to Figure 1, there is depicted a flowchart diagram of a method 100 of scanning a network for determining vulnerabilities associated with a given network architecture element, in

accordance with certain non-limiting embodiments of the present technology. The method 100 may be executed by a processor of a computing device (such as a computing device 400 of Figure 4), description of which is provided below.

STEP 102: RECEIVING DATA INDICATIVE OF A GIVEN NETWORK ARCHITECTURE ELEMENT

[47] At step 102, according to certain non-limiting embodiments of the present technology, the processor may be configured to receive data indicative of the given network architecture element, thereby identifying it within the network.

[48] In some non-limiting embodiments of the present technology, the given network architecture element may be associated with at least one of the following network architecture element types: an IP address, a website, a Universal Resource Locator (URL), a domain name, a network port.

[49] In some non-limiting embodiments of the present technology, the processor may be configured to receive the data indicative of the given network architecture element via a user input, for example, from an operator of the network. In other non-limiting embodiments of the present technology, the processor may be configured to receive the data indicative of the given network architecture element from a database of network architecture elements communicatively coupled therewith. In some non-limiting of the present technology, the database of the network architecture elements is used for storing all newly identified network architecture elements on the network by the processor executing the method 100, as will become apparent from the description herein below.

[50] The method 100 thus proceeds to step 104.

STEP 104: VERIFYING AVAILABILITY OF THE GIVEN NETWORK ARCHITECTURE ELEMENT

[51] At step 104, the processor may further be configured to verify availability of the given network architecture elements, which may differ, according to certain non-limiting embodiments of the present technology, depending on an associated network architecture element type thereof.

[52] In some non-limiting embodiments of the present technology, if the associated network architecture element type is the IP address, it is only checked for availability.

[53] Further, in other non-limiting embodiments of the present technology, if the associated network architecture element type is the domain name, the processor may be configured to verify availability thereof via a WHOIS web service. By doing so, the processor may further be configured

to retrieve, via the WHOIS web service, registration data associated with the domain name, such as information of an owner of the domain name. In additional non-limiting embodiments of the present technology, the processor may further be configured to verify the availability of the domain name by submitting requests for random subdomain names associated with the domain name and analyzing respective responses.

[54] In yet other non-limiting embodiments of the present technology, where the associated network architecture element type is the website, the processor may be configured to verify availability thereof by establishing a connection therewith. In these embodiments, the connection may be established directly or via a proxy server, as an example.

[55] Finally, in those non-limiting embodiments of the present technology, where associated network architecture element type is the URL, the processor may be configured to verify availability thereof by submitting a request to a webserver associated with the URL. Further, upon receiving a response from the webserver associated with the URL, the processor may be configured to analyze at least some of the following information associated with the response in order to verify the availability of the URL: a response code of the response; a content of the response; and a header of the response. Finally, the processor may be configured to determine a type of the URL, which, according to certain non-limiting embodiments of the present technology, may be at least one of: a file, a directory, and undetermined. Additionally, the processor may be configured to determine whether or not the URL responds to requests for non-existing files; whether the URL is associated with an predetermined exclusion task template; and whether or not the webserver associated with the URL is configured to redirect requests submitted by the processor, and if this is the case – the processor may further be configured to determine a URL associated with the redirection.

[56] The method 100 thus proceeds to step 106.

STEP 106: DETERMINING A RESPECTIVE PREDETERMINED TASK TEMPLATE ASSOCIATED WITH THE GIVEN NETWORK ARCHITECTURE ELEMENT

[57] According to certain non-limiting embodiments of the present technology, at step 106, the processor may be configured to determine tasks for scanning the given network architecture element for determining potential vulnerabilities associated therewith.

[58] To that end, in some non-limiting embodiments of the present technology, the processor may be configured to apply a respective predetermined task template including tasks configured for scanning the given network architecture element for detecting vulnerabilities associated therewith.

[59] With reference to Figure 2, according to certain non-limiting embodiments of the present technology, a predetermined task template 200 may be associated with at least one of: an ID of a scanning module (such as a given scanning module 306 of Figure 3), at which the predetermined task template 200 is to be executed; settings associated with launching the scanning module; and types of network architecture elements, to which the predetermined task template may be applied. The types of network architecture elements, to which the predetermined task template 200 may be applied, can typically be defined by tasks associated therewith as the associated tasks can typically be configured to target specific vulnerabilities associated with respective types of network architecture elements as will become apparent from the description below.

[60] According to certain non-limiting embodiments of the present technology, the predetermined task template 200 may be updated. For example, a user may modify predetermined task template 200 and create new templates based thereon, as needed. In additional non-limiting embodiments of the present technology, multiple users may modify predetermined task template 200 simultaneously, for example, by adding additional tasks therein, such as those associated with different types of network architecture elements to be scanned or extending a range of tasks for scanning the given network architecture element, modify the settings of the scanning, etc., without causing conflicts among actions thereof.

[61] According to some non-limiting embodiments of the present technology, the processor may be configured to have access to a plurality of such predetermined task templates for further selecting at least respective one therefrom for determining vulnerabilities associated with various network architecture elements on the network.

[62] The method 100 thus advances to step 108.

STEP 108: USING THE RESPECTIVE PREDETERMINED TASK TEMPLATE FOR SCANNING THE NETWORK, THEREBY IDENTIFYING AT LEAST ONE VULNERABILITY ASSOCIATED WITH THE GIVEN NETWORK ARCHITECTURE ELEMENT

[63] With reference to Figure 3, there is depicted an example configuration of a scanning system 300, in accordance with certain non-limiting embodiments of the present technology. At step 108, once the predetermined task template 200 is ready to be used for scanning, the processor may be configured to transmit it to a task manager module 302, with which the processor is communicatively coupled. Further, after receiving the predetermined task template 200, the task

manager module 302 may be configured to arrange tasks therein, for example, according to their priority, thereby forming a task queue 304.

[64] Finally, as it can be appreciated, the task manager module 302, may be configured to transmit the tasks from the task queue 304 to one of a plurality of scanning modules, such as a given scanning module 306.

[65] According to certain non-limiting embodiments of the present technology, the given scanning module 306 may be scaled up for different networks and operating frameworks; it also may be scaled up for different ranges of network architecture elements.

[66] In some non-limiting embodiments of the present technology, scalability of the scanning system 300 may be controlled by the task manager module 302 and by tasks running on scanning modules. For example, the scalability of the scanning system 300 may be achieved by isolating the task manager module 302 from each of the scanning modules. Besides, the scanning modules may be associated with a plurality scanning tools, therefore it would be possible to use a large number of commercial, open source, proprietary, and other tools to scan the network for vulnerabilities. By doing so, certain non-limiting embodiments of the present technology may allow improving flexibility of the scanning system 300, as well as reducing scanning time, thereby saving computational resources of the scanning system 300 and the processor.

[67] Thus, according to certain non-limiting embodiments of the present technology, in order to execute one or more tasks received from the task manager module 302, the given scanning module 306 may be configured, by the processor, to execute (or otherwise, have access to) one or more network security tools.

[68] Below, there is provided an example list of network security tools executable by the given scanning module 306 for executing one or more tasks, according to certain non-limiting embodiments of the present technology. It should be expressly understood that the present example list of network security tools is not exhaustive, and in additional non-limiting embodiments of the present technology, may include other network security tools currently used for executing tasks associated with scanning networks for vulnerabilities.

[69] Network Mapper (Nmap) may be used at the data collection stage to scan in real time for currently active systems within a given network. Nmap also allows locating a access control list (ACL) of a router or firewall rules by checking an associated acknowledgment flag (ACK) and using other methods. At the binding and evaluation stages, Nmap may be used to scan network

ports, to enumerate identified services and their version numbers, and to collect information on operating systems (insecure.org/nmap).

[70] Patator is a multipurpose and flexible brute-force tool with modular architecture. One of specific features of this tool: a reduced number of false positives due to decisions being based upon the following attributes: a response status code, a response size, matching a string or a regular expression in the response. Also, this network security tool has a modular design, and thus may be scaled up; supports interactive execution; uses permanent connections; multithreading (github.com/lanjelot/patator).

[71] OpenVAS is a network security tool relating to vulnerability scanners. This network security tool uses its own CVE database to scan networks and systems for possible vulnerabilities. OpenVAS may be said to be a primary service with full control over vulnerabilities, with policy management, scanning schedule, detection of false positives, and generating reports in various formats (XML, HTML, LaTeX, etc.). Scanners are managed using the OTP protocol (OpenVAS Transfer Protocol). The tool itself may also receive commands using an XML-like OpenVAS Management Protocol (OMP). All settings and all collected data may be stored in a centralized SQL database (SQLite) (openvas.org).

[72] Web-scout (WS) is a toolset of network security tools to collect information about web applications and websites during penetration testing. It is distributed under the MIT license. This tools may be used for: search for subdomains (dictionary lookup, wildcard lookup or both, in regular zones, in wildcard zones (by ignoring the IP address or based upon a HTTP request)); search for URLs: dictionary lookup, wildcard lookup or both, or using permutations of known URLs; simple queries (GET/POST/HEAD); with various "not found" codes (!=404); determine positive/negative results using regular expressions, determine the "not found" response by its size; use a real browser to circumvent anti-bot protection; use proxy servers or TOR; search for URL parameters (in GET/POST/FILES/COOKIE, dictionary lookup, wildcard lookup or both, with various "not found" codes (!=404), determine negative responses using regular expressions, determine the "not found" response by its size); iterate through forms: regular POST, use a real browser to circumvent anti-bot protection; search for virtual hosts (dictionary lookup, wildcard lookup or both); fuzzing URL parameters and HTTP headers (github.com/AntonKuzminRussia/webscout/blob/master/README_RU.md).

[73] In some non-limiting embodiments of the present technology, certain network security tools listed above may be used as scanning modules. In these embodiments, the network security tools

can be stored in Docker containers on a remote server (not depicted) and may be accessed by the processor as needed.

[74] In specific non-limiting embodiments of the present technology, the network security tools may be stored on the remote server based on their functionality. In other non-limiting embodiments of the present technology, the network security tools may be stored on the remote server based on associated predetermined task templates.

[75] Needless to say that, in various non-limiting embodiments of the present technology, the given scanning module 306 may be configured to access more than one network security tools simultaneously – that is, a predetermined combination thereof.

[76] With continued reference to Figure 3, according to certain non-limiting embodiments of the present technology, the task manager module 302 processes the predetermined task template 200 to select scanning modules corresponding to the tasks included therein. Further, the task manager module 302 may be configured to transmit the tasks to each of the associated scanning modules – such as the given scanning module 306.

[77] In some non-limiting embodiments of the present technology, the task manager module 302 may store a list of scanning modules coupled therewith as well as data about their current utilization. The data about utilization of the scanning modules can be, in turn, provided by the scanning modules. According to certain non-limiting embodiments of the present technology, if there is at least one scanning module with less than 100% utilization, the task manager module 302 would add tasks to the task queue 304. Then, available scanning modules may be configured to request the tasks from the task queue 304 based on the “first come, first served” principle, and execute the task by using one or more network security tools as described above.

[78] As also mentioned above, the predetermined task template 200 may include one or more tasks depending on an associated type of the given network architecture element to be scanned. Below, there is provided an example non-exhaustive list of types of tasks that may be associated with the predetermined task template 200.

[79] 1. Tasks for identifying subdomain names. According to certain non-limiting embodiments of the present technology, these tasks may include tasks for dictionary-based search for subdomains (sets of names as text lists) and for wildcard-based search (all possible combinations of certain groups of characters, with certain length e. g. a-z + 0-9, 1 to 4 characters long).

[80] Typically, in certain non-limiting embodiments of the present technology, there are two ways to run this scanning:

- A regular query for subdomains on DNS servers. This method may be used when a DNS zone sends a negative response to non-existing names.
- A query to a DNS server followed by a HTTP request to a returned IP address. This method may be used for wildcard zones when any subdomain query returns a positive response.

[81] 2. Tasks for identifying URLs. According to certain non-limiting embodiments of the present technology, these tasks may include tasks for dictionary-based search for URLs (sets of names as text lists) and for wildcard-based search (all possible combinations of certain groups of characters, with certain length e. g. a-z + 0-9, 1 to 4 characters long).

[82] Also, the tasks for identifying URLs may be based on the sets which are generated using the known URLs of a website (e.g. if the last character of a URL is a digit, all its versions with the modified last digit are going to be checked).

[83] 3. Tasks for identifying open network ports. According to certain non-limiting embodiments of the present technology, to execute such tasks, the processor may be configured to use a standard TCP connection.

[84] 4. Tasks for retrieving information of at least one web service associated with the open network ports. According to certain non-limiting embodiments of the present technology, to run these tasks, the processor may be configured to query each of the services to determine their respective versions and other data.

[85] 5. Tasks for brute-force password mining (similar to the aforementioned). In some non-limiting embodiments of the present technology, if a given service has been previously identified, the processor may be configured to attempt to connect with it and authorize therewith using a pre-determined list of usernames and passwords.

[86] 6. Tasks for identifying vulnerabilities associated with the at least one web service. These tasks may be used once a version of the at least one web service and the other data are received. According to certain non-limiting embodiments of the present technology, this data may further be verified against databases of the web resource vulners.com, which may return information about potential vulnerabilities associated with the at least one web service. Finally, according to certain

non-limiting embodiments of the present technology, the information about the vulnerabilities may be recorded in the database of network architecture elements.

[87] The method 100 thus proceeds to step 110.

[88] STEP 110: IS AN OTHER NETWORK ARCHITECTURE ELEMENT IS DETECTED?

[89] At step 110, according to certain non-limiting embodiments of the present technology, the processor may be configured retrieve results from scanning modules (such as the given scanning module 306) indicative of the identified vulnerabilities associated with the given network architecture element. Further, the processor may be configured to determine whether the results include any data indicative of at least one another network architecture element associated with the given one. In other words, the processor may be configured to determine if at least one identified vulnerability associated with the given network architecture element provides access to the at least one another network architecture element.

[90] Further, according to certain non-limiting embodiments of the present technology, in response to receiving, from the given scanning module 306, the data indicative of the at least one another network architecture element, the processor may be configured to identify further vulnerabilities associated therewith. To that end, in some non-limiting embodiments of the present technology, the processor may be configured to store the at least one another network architecture element in the database of network architecture elements. Further, the processor may be configured to repeat at least some of the steps 102, 104, 106, 108, and 110 of the method 100 in respect of the newly identified, the at least one another network architecture element, in order to identify further vulnerabilities associated therewith. By doing so, the processor may be configured to loop the method 100 back to the beginning thereof every time a new network architecture element is uncovered.

[91] To that end, based on a type of the at least one another network architecture element, in some non-limiting embodiments of the present technology, the processor may further be configured to apply a same predetermine task template, that is, the predetermined task template 200. However, in other non-limiting embodiments of the present technology, in order to determine further vulnerabilities associated with the at least one another network architecture element, the processor may be configured to apply at least partially different predetermined task template (that is, another predetermined task template) from the predetermined task template 200.

[92] By doing so, in certain non-limiting embodiments of the present technology, the processor may be configured to iteratively scan the network, selectively applying one of predetermined task templates depending on a specific type of a next network architecture element, to identify vulnerabilities associated therewith until no further vulnerability can be identified.

[93] In some non-limiting embodiments of the present technology, the processor may be configured to use a decision tree for determining a sequence of tasks for scanning the network based on the at least one another network architecture element and the given network architecture element.. In these embodiments, the decision tree may split a given task for scanning a network architecture element into a sequence of tasks. Accordingly, by using the decision tree defining certain conditions for executing the tasks, the processor may be configured to selectively switch among scanning modules in the scanning system 300, whereby improved efficiency of the scanning system 300 may be achieved. In additional non-limiting embodiments of the present technology, the processor may be configured to use the decision tree for creating sequences of operations required to solve specific issues based on received data. Accordingly, in some non-limiting embodiments of the present technology, the processor may be configured to generate predetermined task templates dynamically based on results rendered by execution of tasks associated with a previously used predetermined task template and newly identified network architecture elements.

[94] The method thus proceeds to step 112.

STEP 112: GENERATING AN INTERMEDIATE REPORT INCLUDING DATA OF THE AT LEAST ONE VULNERABILITY

[95] According to certain non-limiting embodiments of the present technology, if, at step 110, the processor has not received any data indicative of the at least one another network architecture element, at step 112, the processor may be configured to generate an intermediate report 308 including data of currently identified vulnerabilities on the network – that is, for example, the vulnerabilities associated with the given network architecture element. Further, the processor may be configured to cause task manager module 302 to switch to a waiting mode until any change associated with network architecture elements of the network occurs.

[96] In some non-limiting embodiments of the present technology, irrespective of absence of the data indicative of the at least one another network architecture element, the processor may be configured to generate, at each iteration of executing the method 100, the intermediate report 308 including the data of the currently identified vulnerabilities on the network. Accordingly, based on intermediate reports aggregated over a predetermined number of iterations of executing the method

100, the processor may be configured to generate a timeline of changes associated with the given network architecture element.

[97] In certain non-limiting embodiments of the present technology, the processor may further be configured to present (for example, via outputting them on a computer screen) the intermediate reports to the operator of the scanning system 300 for further analyzing changes associated with network architecture elements – for example, how the structure of the given network architecture element has changed over time: new and deleted associated hyperlinks, changes in availability of services at a given IP address, changed associated subdomain names, and the like.

[98] As mentioned earlier, in some non-limiting embodiments of the present technology, the intermediate reports including the data indicative of all currently identified vulnerabilities may be stored in the database of network architecture elements; in these embodiments, the data may include: all IP addresses, domain names, web sites and their URLs, and also all the discovered authorization options (if any valid passwords were discovered) as well as vulnerabilities in all associated network architecture elements.

[99] Thus, certain embodiments of method 100 allow the scanning system 300 to operate continuously, that is, the search for further vulnerabilities on the network never stops. For example, if no new vulnerabilities have been identified on the network by a given moment in time using a given task, the scanning system 300 may be configured to intermittently re-execute the given task. As soon as a requested service would appear for a targeted network architecture element (and/or a new dependent service, which would be considered as an associated network architecture element), it will be analyzed using the given task. Prior art scanners known to the developers of the present technology typically run only once, provide a report on results without conducting additional searches. However, some of prior art scanners may optionally operate on a fixed schedule, that is, they may repeatedly scan for a network architecture element in question.

[100] Accordingly, one of advantages of the present technology may be that it can enable to monitor historical changes in data of the given network architecture element because at each iteration executed tasks and received results are recorded.

[101] For example, let us consider a case wherein a target subnet all SSH keys have been replaced at once. In response to this event, the scanning system 300 may be configured to conclude that the bulk replacement of the SSH keys may have been caused by a bulk re-installation of the OS, which may indicate an incident within this subnet. In another example: based on one or more intermediate reports, the scanning system 300 may be configured to register availability of a certain service, for

example, once a week at certain time. The scanning system 300 may thus be configured to interpret this event as important because this behavior is likely to be related with backing up the system or similar activities.

[102] In addition, the database of network architecture elements may also be configured to store a scanning frequency and time settings to look for new associated network architecture elements at a predetermined regularity. Also, in specific non-limiting embodiments of the present technology, the scanning frequency and the time settings may be set (or otherwise, modified) by the operator of the scanning system 300. Additionally, these settings may be stored in a respective predetermined task template for a specific network architecture element based on accumulated experience.

[103] The examples below are given so as to illustrate the practice of various embodiments of the present disclosure. It is not intended to limit or define the entire scope of this disclosure.

EXAMPLES

[104] The scanning system 300 may receive an URL <http://site.com/auth/>. The scanning system 300 then queries this URL to get basic information. At this stage, the scanning system 300 finds out that the web server responds to its query with the 401-response code (http basic auth). A brute force password mining task is created for this URL based on a predetermined task template for “http basic auth”. When this task is executed, a valid username and password pair may be received (for example, admin:qwerty), these credentials are recorded in a respective intermediate report.

[105] In another example, an URL <http://site.com/> may be received as input data. The scanning system 300 then creates predetermined task templates configured to search for subdomains for *.site.com. At the scanning stage, the auth.site.com subdomain may be uncovered. It is then necessary to check if this subdomain is a website. In case this check is completed successfully, the scanning system 300 may further receive additional data at <http://auth.site.com/>. At this stage the scanning system 300 may receive, on a respective request, a response from a web server including a response code 401 (http basic auth). Then, just as in the previous example, a brute force password mining task is created for this URL based on the "http basic auth" predetermined task template. When this task is executed, a valid username and password pair may be received (for example, admin:qwerty), these credentials are recorded in a respective intermediate report. At the same time, certain tasks can be created to search for URL addresses, which may result in receiving a link <http://auth.site.com/backup.zip>.

COMPUTING ENVIRONMENT

[106] With reference to Figure 4, there is depicted an example functional diagram of the computing device 400 configurable to implement certain non-limiting embodiments of the present technology.

[107] In some non-limiting embodiments of the present technology, the computing device 400 may include: the processor comprising one or more central processing units (CPUs) 401, at least one non-transitory computer-readable memory 402, a storage 403, input/output interfaces 404, input/output peripherals 405, connectivity hardware 404.

[108] According to some non-limiting embodiments of the present technology, the one or more CPUs 401 may be configured to execute specific program instructions the computations as required for the computing device 400 to function properly or to ensure the functioning of one or more of its components. The one or more CPUs 401 may further be configured to execute specific machine-readable instructions stored in the at least one non-transitory computer-readable memory 402, for example, those causing the computing device to execute one of the method 200 and the method 300.

[109] In some non-limiting embodiments of the present technology, the machine-readable instructions representative of software components of disclosed systems may be implemented using any programming language or scripts, such as C, C++, C#, Java, JavaScript, VBScript, Macromedia Cold Fusion, COBOL, Microsoft Active Server Pages, Assembly, Perl, PHP, AWK, Python, Visual Basic, SQL Stored Procedures, PL/SQL, any UNIX shell scripts or XML. Various algorithms are implemented with any combination of the data structures, objects, processes, procedures and other software elements.

[110] The at least one non-transitory computer-readable memory 402 may be implemented as RAM and contains the necessary program logic to provide the requisite functionality.

[111] The storage 403 may be implemented as at least one of an HDD drive, an SSD drive, a RAID array, a network storage, a flash memory, an optical drive (such as CD, DVD, MD, Blu-ray), etc. The storage 403 may be configured for long-term storage of various data, e.g., the aforementioned documents with user data sets, databases with the time intervals measured for each user, user IDs, etc.

[112] The interfaces input/output 404 may comprise various interfaces, such as at least one of USB, RS232, RJ45, LPT, COM, HDMI, PS/2, Lightning, FireWire, etc.

[113] The input/output peripherals 405 may include at least one of a keyboard, joystick, (touchscreen) display, projector, touchpad, mouse, trackball, stylus, speakers, microphone, and the like. A communication link between each one of the input/output peripherals 405 can be wired (for example, connecting the keyboard via a PS/2 or USB port on the chassis of the desktop PC) or wireless (for example, via a wireless link, e.g., radio link, to the base station which is directly connected to the PC, e.g., to a USB port).

[114] The connectivity hardware 404 may be selected based on a particular implementation of the network 120, and may comprise at least one of: an Ethernet card, a WLAN/Wi-Fi adapter, a Bluetooth adapter, a BLE adapter, an NFC adapter, an IrDa, a RFID adapter, a GSM modem, and the like. As such, the connectivity hardware 404 may be configured for wired and wireless data transmission, via one of WAN, PAN, LAN, Intranet, Internet, WLAN, WMAN, or GSM networks.

[115] These and other components of the computing device 400 may be linked together using a common data bus 410.

[116] It should be expressly understood that not all technical effects mentioned herein need to be enjoyed in each and every embodiment of the present technology.

[117] Modifications and improvements to the above-described implementations of the present technology may become apparent to those skilled in the art. The foregoing description is intended to be exemplary rather than limiting. The scope of the present technology is therefore intended to be limited solely by the scope of the appended claims.

CLAIMS

What is claimed is:

1. A method for determining vulnerabilities on a network, the method being executable by a processor, the method comprising:

receiving, by the processor, data indicative of a first network architecture element;

determining, by the processor, based on the data indicative of the first network architecture element, a respective one of a plurality of predetermined task templates,

the respective one of the plurality of predetermined task templates including one or more tasks executable for identifying respective vulnerabilities associated with the first network architecture element;

in response to identifying, based on the respective one of the plurality of predetermined task templates, at least one vulnerability associated with the first network architecture element:

determining, by the processor, based on the at least one vulnerability, a second network architecture element associated with the first network architecture element, the at least one vulnerability providing access to the second network architecture element;

determining, by the processor, data indicative of the second network architecture element;

storing, by the processor, the data indicative of the second network architecture element in a database; and

using, by the processor, the data indicative of the second network architecture element for identifying further vulnerabilities on the network.

2. The method of claim 1, wherein the first network architecture element is associated with a first network architecture element type comprising at least one of: an IP address, a website, a Uniform Resource Locator(URL), a domain name, and a network port.
3. The method of claim 2, wherein, if the first network architecture element type is the domain name, the method further comprises verifying, by the processor, availability of the domain name using a WHOIS web service.

4. The method of claim 3, wherein the method further comprises determining, by the processor, using the WHOIS web service, registration data associated with an owner of the domain name.
5. The method of claim 3, the verifying the availability of the domain name further comprises analyzing, by the processor, data responsive to requests for random subdomain names associated with the domain name.
6. The method of claim 2, wherein, if the first network architecture element type is the website, the method further comprises verifying, by the processor, availability of the website, the verifying comprising establishing a connection with the website, the connection being one of a direct connection and a connection via a proxy server.
7. The method of claim 2, wherein if the first network architecture element type is the URL, the method further comprises verifying availability of the URL, the verifying comprising transmitting, by the processor, at least one request to a webserver associated with the URL, and the verifying further comprising at least one of: analyzing a response code of a response received from the webserver associated with the URL; a content associated with the response; a header of the response; and a type of the URL, wherein the type of the URL is associated with one of a file, a directory, and underdetermined.
8. The method of claim 7, wherein the verifying the availability of the URL further comprises determining at least one of:
 - if the URL is responsive to requests for non-existing files;
 - if the URL is associated with a predetermined exclusion template;
 - if the webserver associated with the URL is configured to redirect the at least one request to at least one another URL, and determining the at least one another URL.
9. The method of claim 1, wherein the data indicative of the first network architecture elements are received from one of: a user input and the database.
10. The method of claim 1, wherein the respective one of the plurality of predetermined task templates is associated with a plurality of network architecture element types, to which the respective one of the plurality of predetermined task templates is applicable.
11. The method of claim 10, wherein the one or more tasks comprise at least one of:

tasks for identifying subdomain names;

tasks for identifying URLs;

tasks for identifying open network ports;

tasks for retrieving information of at least one web service associated with the open network ports;

tasks for password mining for accessing the at least one web service associated with the open network ports; and

tasks for identifying vulnerabilities associated with the at least one web service.

12. The method of claim 1, further comprising:

receiving, by the processor, the data indicative of the second network architecture element;

determining, by the processor, based on the data indicative of the second network architecture element, another one of the plurality of predetermined task templates,

the other one of the plurality of predetermined task templates including one or more tasks executable for identifying respective vulnerabilities associated with the second network architecture element;

in response to identifying, based on the other one of the plurality of predetermined task templates, at least one vulnerability associated with the second network architecture element, the at least one vulnerability providing access to a third network architecture element associated with the second network architecture element:

determining, by the processor, data indicative of the third network architecture element;

storing, by the processor, the data indicative of the third network architecture element in the database; and

using, by the processor, the data indicative of the third network architecture element for identifying further vulnerabilities on the network.

13. The method of claim 12, further comprising iteratively repeating at least the steps of the receiving data and the determining a predetermined task template until no further vulnerability is identified.
14. The method of claim 13, further comprising generating, at each iteration, an intermediate report including data of vulnerabilities having been identified on the network.
15. The method of claim 12, wherein the other one of the plurality of predetermined task templates is a same as the respective one of the plurality of predetermined task templates.
16. The method of claim 12, wherein the other one of the plurality of predetermined task templates is at least partially different from the respective one of a plurality of predetermined task templates.
17. A system for determining vulnerabilities on a network, the system comprising a computing device, the computing device further comprising:
 - a processor;
 - a non-transitory computer-readable medium comprising instructions;
 - the processor, upon executing the instructions, being configured to:
 - receive data indicative of a first network architecture element;
 - determine based on the data indicative of the first network architecture element, a respective one of a plurality of predetermined task templates,
 - the respective one of the plurality of predetermined task templates including one or more tasks executable for identifying respective vulnerabilities associated with the first network architecture element;
 - in response to identifying, based on the respective one of the plurality of predetermined task templates, at least one vulnerability associated with the first network architecture element:
 - determine, based on the at least one vulnerability, a second network architecture element associated with the first network architecture element, the at least one vulnerability providing access to the second network architecture element;

determine data indicative of the second network architecture element;

store the data indicative of the second network architecture element in a database; and

use the data indicative of the second network architecture element for identifying further vulnerabilities on the network.

18. The system of claim 17, wherein the processor is further configured to:

receive the data indicative of the second network architecture element;

determine, based on the data indicative of the second network architecture element, another one of the plurality of predetermined task templates,

the other one of the plurality of predetermined task templates including one or more tasks executable for identifying respective vulnerabilities associated with the second network architecture element;

in response to identifying, based on the other one of the plurality of predetermined task templates, at least one vulnerability associated with the second network architecture element, the at least one vulnerability providing access to a third network architecture element associated with the second network architecture element:

determine data indicative of the third network architecture element;

store the data indicative of the third network architecture element in the database; and

use the data indicative of the third network architecture element for identifying further vulnerabilities on the network.

19. The system of claim 18, wherein the processor is further configured to iteratively repeat at least the steps of the receiving data and the determining a predetermined task template until no further vulnerability is identified.

20. The system of claim 19, wherein the processor is further configured to generate, at each iteration, an intermediate report including data of vulnerabilities having been identified on the network.