OPSWG
Internet-Draft
Intended status: Standards Track
Expires: September 7, 2020
March 06, 2020

J. Yang
L. Xia
Huawei

Active-Scanning profiles for IoT devices
draft-yang-opsawg-iot-devices-active-scanning-00

Abstract

This draft extends MUD [RFC8520] model for the active scanning during the end host device on-boarding. The according features include TCP/UDP port scanning, weak password detection, mandatory and hazardous services detection, etc, which can help administrator to discover system security vulnerabilities in advance.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

IoT devices use a large number of open-source software and application components, and the system iteration is fast. Therefore, various security vulnerabilities may exist. When an IoT device is on boarding, the network administrator can quickly learn about the security settings and technical support services of the device through active scanning, detect security vulnerabilities in a timely manner, objectively evaluate the network risk level, and rectify network security vulnerabilities and incorrect configurations to prevent hacker attacks. If we look firewalls and network monitoring systems as passive means of defense, then security scanning can look as an active preventive measure, which can effectively prevent hacker attacks.

This document extends MUD RFC8520 to model the functions and parameters of active scanning, including TCP/UDP port scanning, weak password detection, mandatory and hazardous services detection, etc. By using this scanning profile, the MUD-enabled active scanner can obtain a lot of useful information to discover system security vulnerabilities.

2. Overview of Active Scanning IoT devices

2.1. Port-Scanning

A port is a potential communication channel, that is, an intrusion channel. Port scanning on IoT devices can obtain a lot of useful information, which can be used to discover system security vulnerabilities. The following scanning types are widely used:

- TCP SYN scanning: also called half-open scanning. In this mode, the SYN packet is sent to the destination port. If the SYN/ACK response is received, the port is open. If an RST packet is received, it indicates that the port is disabled. If no reply is received, it is determined that the port is filtered (Filtered). In this mode, SYN packets are sent only to specific ports of the target host, but no complete TCP connection is established. Therefore, this mode is relatively covert and efficient. On a fast network without intrusion firewalls, thousands of ports can be scanned per second, and this mode is widely applicable.

- TCP connect scanning: Use the system network API to connect to the port of the target device. If the connection fails, the port is disabled. This scanning speed is slow. In addition, because the complete TCP session will leave the connection information on the target device, so this scanning mode is not hidden. Therefore, TCP connect is considered only when TCP SYN cannot be used.

- UDP scanning: used to determine the UDP port status. Send a probe packet to the UDP port of the target device. If the "ICMP port unreachable" message is returned, the port is disabled. If no reply is received, the UDP port may be open or blocked. Therefore, the reverse exclusion method is used to determine which UDP ports may be open. Although major services on the Internet run over TCP, but there are still many UDP services, like DNS, SNMP, and DHCP (the registered ports are 53, 16, 162, and 67/68), and network attacks will not ignore these protocols.

The port scanning range can be selected or specified based on service requirements, and widely be divided into the following modes:

- Standard: 4K port range, and usually the default mode.

- Fast: port range including all mainstreamed ports, including 21(ftp), 22(ssh), ...

- All: the port range of 0 to 65535.

- Specified: the customized port range, for example, 22 and 1100 to 1124

2.2. Service Discovery

When a IoT device is installed, some necessary services are usually enabled for supporting the later use. For example, if the IoT device need to access the Internet, HTTPS service must be enabled. In addition, due to device performance or service requirements, some services must be disabled. By MUD extension of scanning services running on the device, the administrator have a knowledge of the devices’ services, which are mandatory and hazardous, furtherly to discover the potential vulnerabilities.

2.3. Weak-password Cracking

A weak password is a password that contains only digits and letters, for example, 123456, abcdef, 123abc, admin, and root, which can be guessed or cracked easily. If the IoT device uses these weak passwords, it is like putting the door key under the mat of the door. This behavior is very dangerous.

Well-known protocols and databases, such as Telnet, FTP, SSH, POP3, SNMP, Oracle, MySQL, DB2, and MongoDB, have massive default password dictionaries, even we can also upload a customized dictionary library. By active scanning these passwords of dictionaries, the administrator can identify vulnerabilities and risks of IoT devices in advance.

The password dictionary refers to the dictionary library for weak password scanning. There are three types of dictionary: single user-name mode, single password mode, and combination user-name-and-password mode, which can be applied based-on customer’s requirements:

- o Single user-name mode: only scan the user name based-on user’s dictionary. For example: telnet_user_dictionary.txt contain "root; admin; test; guest;"

- o Single password mode: only scan the password based-on password’s dictionary. For example: telnet_password_dictionary.txt contain "111111; 112233; 123123; 123321; 123456; abcdef; admin; password;"

- o Combination mode: scan the user name and password together based-on combination’s dictionary. For example, telnet_conbination_dictionary.txt contain "root:test; root:admin; root:private; root:1234; root:root;"

2.4. Frequency and Result of active scanning

The execution mode of the active scanning, can be set with the following:

- o Immediate: active scanning will be executed immediately.

- o Scheduled: active scanning will be executed in the scheduled time.

- o Daily: active scanning will be executed periodically every day in the scheduled time.

- o Weekly: active scanning will be executed periodically every week in the scheduled time.

- o Monthly: active scanning will be executed periodically every month in the scheduled time.

In addition, the scanning results can be saved with logs, and the ending notification can be sent to somebody by email or SMS message, which can notify the scanning completion to administrators in time.

3. The ietf-mud-active-scanning model extension

This document augments the "ietf-mud" MUD YANG module defined in [RFC8520] for signaling the IoT device active scanning profile. This document defines the YANG module "ietf-mud-active-scanning", which has the following tree structure:

```
module: ietf-mud-active-scanning
   augment /ietf-mud:mud:
      +--rw active-scanning
         +--rw log-save-uri                  inet:uri
         +--rw scanning-frequency?           scanning-frequency
         +--rw start-time?                   yang:timestamp
         +--rw notification-receiver-email?  string
         +--rw notification-receiver-sms?    string
         +--rw port-scanning* \[scanning-type\]
            +--rw scanning-type              port-scanning-type
            +--rw scanning-mode?             port-scanning-mode
            +--rw scanning-range?            uint16
         +--rw mandatory_service-scanning*   string
         +--rw hazardous_service-scanning*   string
         +--rw weak-login-scanning* \[service-name\]
            +--rw service-name               string
            +--rw dictionary-type?           dictionary-type
            +--rw user-dictionary?           string
            +--rw password-dictionary?       string
            +--rw combination-dictionary?    string
```

3.1. The mud-active-scanning YANG model

```
 module ietf-mud-active-scanning {
    yang-version 1.1;
    namespace
       "urn:ietf:params:xml:ns:yang:ietf-mud-active-scanning";
    prefix ietf-mud-active-scanning;

    import ietf-mud {
       prefix mud;
```

```
        reference
           "RFC 8520";
     }

     import ietf-inet-types {
        prefix inet;
        reference
           "RFC 6991";
     }

     import ietf-yang-types {
        prefix yang;
        reference
           "RFC 6991";
     }

     organization
        "IETF OPSAWG (Ops Area) Working Group";
     contact
        "WG Web: http://tools.ietf.org/wg/opsawg/
         WG List: opsawg@ietf.org
         Author: Jie Yang
         jay.yang@huawei.com
        ";

     description
        "This module contains YANG definition for the IoT device
        active scanning profile.

        Copyright (c) 2019 IETF Trust and the persons identified as
        authors of the code. All rights reserved.

        Redistribution and use in source and binary forms, with or
        without modification, is permitted pursuant to, and subject
        to the license terms contained in, the Simplified BSD License
        set forth in Section 4.c of the IETF Trust’s Legal Provisions
        Relating to IETF Documents
        (http://trustee.ietf.org/license-info).

        This version of this YANG module is part of RFC XXXX; see
        the RFC itself for full legal notices.";

     revision 2020-03-12 {
        description
           "Initial proposed standard.";
     }

     typedef scanning-frequency {
        type enumeration {
           enum immediate {
              description
                 "Immediate scanning.";
           }
           enum daily {
              description
                 "Scanning at an accurate time of every day.";
           }
           enum weekly {
              description
                 "Scanning at an accurate time of every week.";
           }
           enum monthly {
              description
                 "Scanning at an accurate time of every month.";
           }
        }
        default "monthly";
        description
           "The execution mode of the active scanning,
            called with the scanning frequency.";
     }

     typedef port-scanning-type {
        type enumeration {
           enum tcp-syn;
           enum tcp-connect;
           enum udp;
        }
        default "tcp-syn";
        description
           "Widest port scanning type.";
     }

     typedef port-scanning-mode {
        type enumeration {
           enum standard {
              description
                 "Standard mode with scanning the ports
                  in range 0..4096.";
           }
           enum fast {
              description
                 "Fast mode with sanning the ports in
                  range 20|21|23|25|37|53|67|68|69|80|110
                  |115|123|143|161|443|873.";
           }
           enum all {
              description
                 "All mode with scanning all ports in range 0..65535";
           }
           enum specified {
              description
                 "Specified mode with scanning the ports customized,
                  like in range 22|50..66|110";
           }
        }
        default "standard";
        description
           "Widest port scanning mode.";
     }

     typedef dictionary-type {
        type enumeration {
           enum only-user-name;
           enum only-password;
           enum user-name-and-password;
        }
        default "user-name-and-password";
        description
           "Widest type of weak login dictionary.";
     }

     augment "/mud:mud/mud:" {
        container active-scanning {
           description
              "Active scanning profiles supported by the device";
           leaf log-save-uri {
              type inet:uri;
              description
                 "Log URI where saving active scanning results.";
           }
           leaf scanning-frequency {
              type scanning-frequency;
              description
                 "Active scanning frequency.";
           }
           leaf start-time {
              type yang:timestamp;
              description
                 "The accurate scanning time.
                  For example, scanning-frequency with monthly like
                  xxxx-03-12T02:00:00.00+08:00";
           }
           leaf receiver-email-notification {
              type string;
              description
                 "E-mail address which receive the ending notification
                  of active scanning.";
           }
           leaf receiver-sms-notification {
              type string;
              description
                 "SMS address which receive the ending notification
                  of active scanning.";
           }
           list port-scanning {
              key "scanning-type";
              description
                 "Active scanning ports.";
              leaf scanning-type {
                 type port-scanning-type;
                 description
                    "Port scanning type.";
              }
              leaf scanning-mode {
                 type port-scanning-mode;
                 description
                    "Port scanning mode.";
              }
              leaf scanning-range {
                 type uint16;
                 description
                    "Port scanning range. For example, scanning-mode
                     with standard is 0..4096";
              }
           }
           leaf mandatory_service-scanning {
              type string;
              description
                 "Scanning mandatory services on the devices,
                  which must be installed.";
           }
           leaf hazardous_service-scanning {
              type string;
              description
                 "Scanning hazardous services on the devices,
                  which mustn’t be installed.";
           }
           list weak-login-scanning {
              key "service-name";
              description
                 "Active scanning weak login with user’s name
```

```
                  and/or password.";
              leaf service-name {
                 type string;
                 description
                    "The name of service on the device.";
              }
              leaf dictionary-type {
                 type dictionary-type;
                 description
                    "The dictionary type for scanning weak login.";
              }
              leaf user-dictionary {
                 when "./dictionary-type=only-user-name";
                 type string;
                 description
                    "The context in user-name’s dictionary.
                     For example: root,admin,test,guest, ";
              }
              leaf password-dictionary {
                 when "./dictionary-type=only-password";
                 type string;
                 description
                    "The context in password’s dictionary.
                     For example: 111111, 112233, admin, password,";
              }
              leaf combination-dictionary {
              while "./dictionary-type=user-name-and-password";
              type string;
                 description
                    "The context in user-name-and-password’s dictionary.
                     For example: root:test, root:admin, root:1234,";
              }
           }
        }
     }
  }
```

4. MUD File Example

This example below contains active scanning for a IoT device. JSON encoding of YANG modelled data {{RFC7951}} is used to illustrate the example.

```
{
   "ietf-mud:mud": {
   "mud-version": 1,
   "mud-url": "https://example.com/IoTDevice",
   "last-update": "2020-03-12T02:00:00.00+08:00",
   "cache-validity": 100,
   "is-supported": true,
   "systeminfo": "IoT device name",
   "active-scanning": {
      "log-save-uri" : "d:/mud-scanning-log/",
      "scanning-frequency" : immediate,
      "receiver-email-notification" : "admin@device.com,
                                       123@device.com,",
      "receiver-sms-notification" : "008613812345679,
                                     0086133123456,",
      "port-scanning" : {
         "scanning-type" : tcp-syn,
         "scanning-mode" : standard,
      }
      "weak-login-scanning" : {
         "service-name" : "telnet",
         "dictionary-type" : user-name-and-password,
         "combination-dictionary" : "root:test; root:1234; root:root;"
      }
   }
}
```

5. Security Considerations

Security considerations in [RFC8520] need to be taken into consideration.

6. IANA Considerations

The IANA is requested to add "active-scanning" to the MUD extensions registry as follows: Extension Name: Active-Scanning Standard reference: This document

7. Acknowledgements

Thanks to ...

8. Informative References

[RFC7951] Lhotka, L., "JSON Encoding of Data Modeled with YANG", RFC 7951, DOI 10.17487/RFC7951, August 2016, <https://www.rfc-editor.org/info/rfc7951>.

[RFC8520] Lear, E., Droms, R., and D. Romascanu, "Manufacturer Usage Description Specification", RFC 8520, DOI 10.17487/RFC8520, March 2019, <https://www.rfc-editor.org/info/rfc8520>.

Authors’ Addresses

Jie Yang
Huawei
101 Software Avenue, Yuhuatai District
Nanjing, Jiangsu 210012
China

Email: jay.yang@huawei.com

Liang Xia (Frank)
Huawei
101 Software Avenue, Yuhuatai District,
Nanjing, Jiangsu 210012
China

Email: frank.xialiang@huawei.com