|  |  |
| --- | --- |
|  |  |
| Cisco ASDM Setup |  |
|  |  |
|  | 09/21/2021CISCO Cybersecurity |
|  | Guanzhen Qian |

**Purpose**

In this lab, we will reset the password of the Cisco Adaptive Security Appliance (ASA) firewall with console connection. After that, we will reset the ASA firewall to factory setting. The purpose of this lab is to understand how to get into an ASA firewall and exploit it with physical connection. This is lab shows how hackers may hack a CISCO firewall with physical access to it, thus it is important to protect the networking appliances from physical access.

**Background**

ASA firewall protects corporate networks and data centers of all sizes. A firewall is a security system designed to block unauthorized access to a network and malicious software. Firewalls analyze network traffics, and it is configured to only accept authorized traffic. Firewalls can be software or hardware. A software firewall is a program on a device that works through ports and applications. A hardware firewall is a physical device placed between network and gateway or network and end devices. Without a firewall, end devices accept every connection into networks.

Cisco Adaptive Security Device Manager (ASDM) graphic user interface tool (GUI) used to manage Cisco ASA security appliances. GUI provides a visual representation of files present and shows live details about systems in infographics. ASDM can be downloaded from Cisco’s website or from ASA’s admin page. ASDM can access the router with its admin username and password. ASDM is convenient at quickly configure, monitor, and troubleshoot Cisco ASAs.

**Lab Summary**

1. Established console connection between pc and the ASA firewall.
2. Console into the firewall with putty software on pc.
3. Configure ASA with IP address and HTTPS
4. Connect ASA with ethernet and login with admin
5. Download ASDM
6. Install ASDM
7. Configure necessary settings for ASDM.

**Lab Commands**

Int – Enter a chosen interface

Nameif – Specify name of an interface

IP address – Set IP address

Switchport access vlan – Issue a vlan to a port

Username password – Set username and password for admin

Http server enable – Enable the HTTPS server

Http – Identify IP address for HTTPS connections

**Network Diagrams**

  Console

PC

CISCO

ASA

Ethernet

**Configuration**

ASA:

*: Saved*

*:*

*: Serial Number: JMX1237Z0B2*

*: Hardware: ASA5505, 1024 MB RAM, CPU Geode 500 MHz*

*:*

*ASA Version 9.2(4)*

*!*

*hostname ciscoasa*

*enable password Q6PcEw0JPNC8SDNU encrypted*

*names*

*!*

*interface Ethernet0/0*

*switchport access vlan 2*

*!*

*interface Ethernet0/1*

*switchport access vlan 10*

*!*

*interface Ethernet0/2*

*!*

*interface Ethernet0/3*

*!*

*interface Ethernet0/4*

*!*

*interface Ethernet0/5*

*!*

*interface Ethernet0/6*

*!*

*interface Ethernet0/7*

*!*

*interface Vlan1*

*nameif inside*

*security-level 100*

*ip address 192.168.1.1 255.255.255.0*

*!*

*interface Vlan2*

*no nameif*

*security-level 0*

*ip address dhcp setroute*

*!*

*interface Vlan10*

*nameif outside*

*security-level 0*

*ip address 192.168.2.1 255.255.255.0*

*!*

*ftp mode passive*

*object network obj\_any*

*subnet 0.0.0.0 0.0.0.0*

*pager lines 24*

*logging asdm informational*

*mtu inside 1500*

*mtu outside 1500*

*icmp unreachable rate-limit 1 burst-size 1*

*no asdm history enable*

*arp timeout 14400*

*no arp permit-nonconnected*

*timeout xlate 3:00:00*

*timeout pat-xlate 0:00:30*

*timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02*

*timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00*

*timeout sip 0:30:00 sip\_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00*

*timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute*

*timeout tcp-proxy-reassembly 0:01:00*

*timeout floating-conn 0:00:00*

*dynamic-access-policy-record DfltAccessPolicy*

*user-identity default-domain LOCAL*

*http server enable*

*http 192.168.1.0 255.255.255.0 inside*

*http 192.168.2.0 255.255.255.0 outside*

*no snmp-server location*

*no snmp-server contact*

*crypto ipsec security-association pmtu-aging infinite*

*crypto ca trustpool policy*

*telnet timeout 5*

*no ssh stricthostkeycheck*

*ssh timeout 5*

*ssh key-exchange group dh-group1-sha1*

*console timeout 0*

*dhcpd auto\_config outside*

*!*

*dhcpd address 192.168.1.5-192.168.1.36 inside*

*dhcpd enable inside*

*!*

*threat-detection basic-threat*

*threat-detection statistics access-list*

*no threat-detection statistics tcp-intercept*

*username cisco password eeH8sl9M4wy/URjZ encrypted privilege 15*

*!*

*class-map inspection\_default*

*match default-inspection-traffic*

*!*

*!*

*policy-map type inspect dns preset\_dns\_map*

*parameters*

*message-length maximum client auto*

*message-length maximum 512*

*policy-map global\_policy*

*class inspection\_default*

*inspect dns preset\_dns\_map*

*inspect ftp*

*inspect h323 h225*

*inspect h323 ras*

*inspect rsh*

*inspect rtsp*

*inspect esmtp*

*inspect sqlnet*

*inspect skinny*

*inspect sunrpc*

*inspect xdmcp*

*inspect sip*

*inspect netbios*

*inspect tftp*

*inspect ip-options*

*!*

*service-policy global\_policy global*

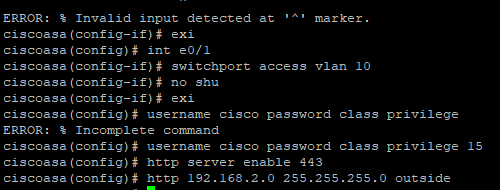
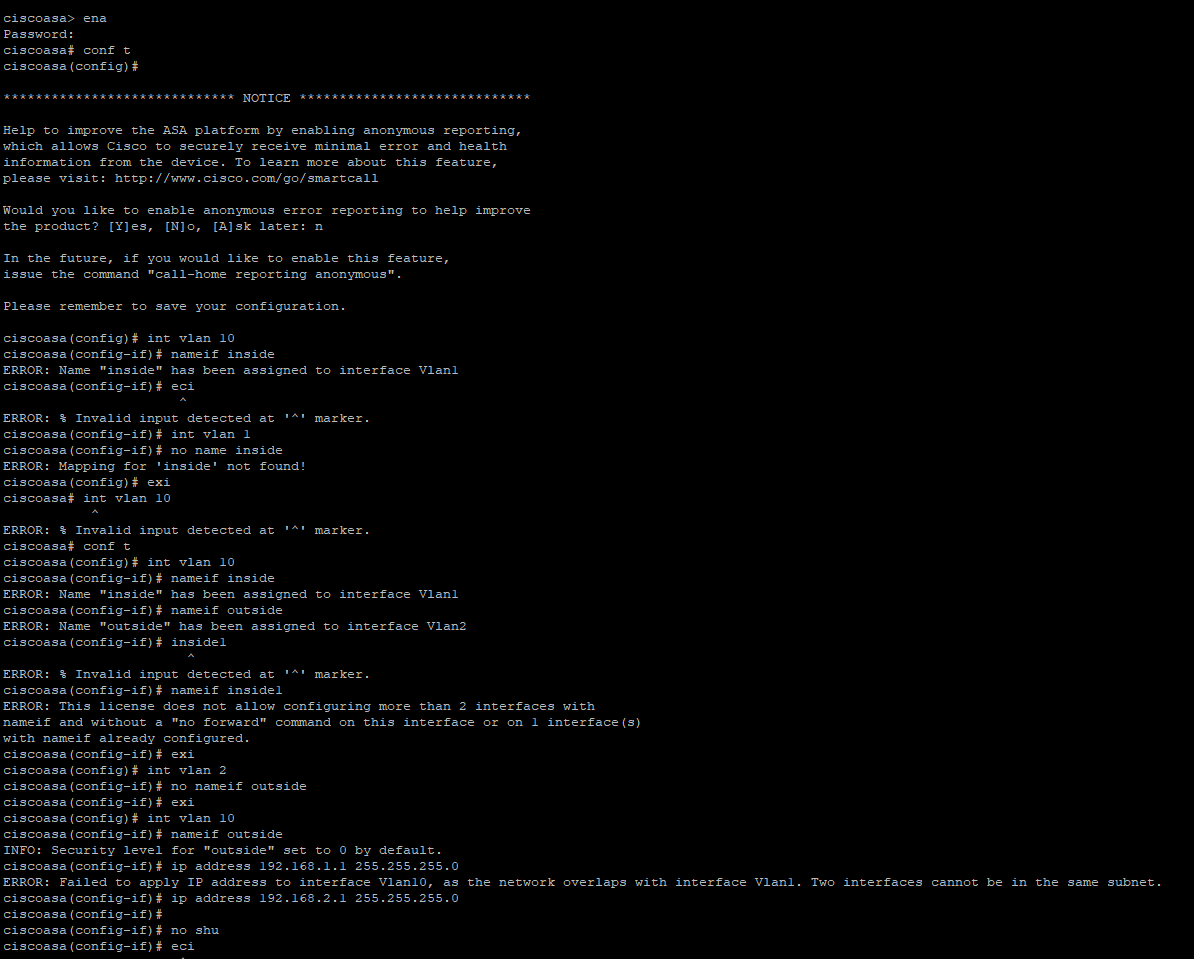
*prompt hostname context*

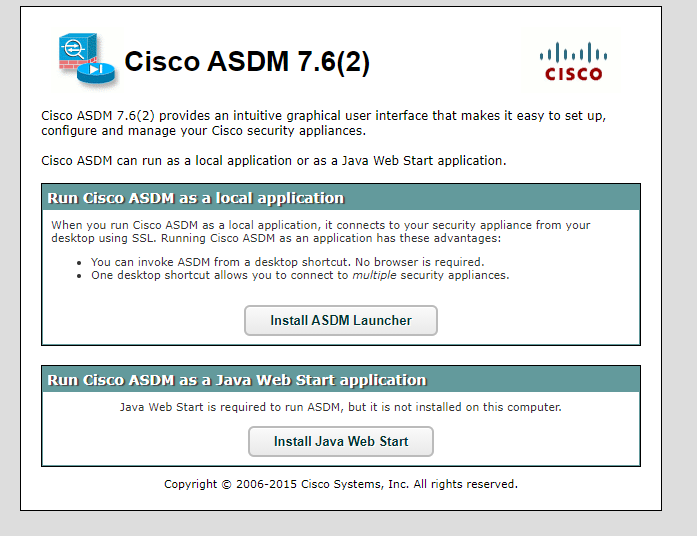
*no call-home reporting anonymous*

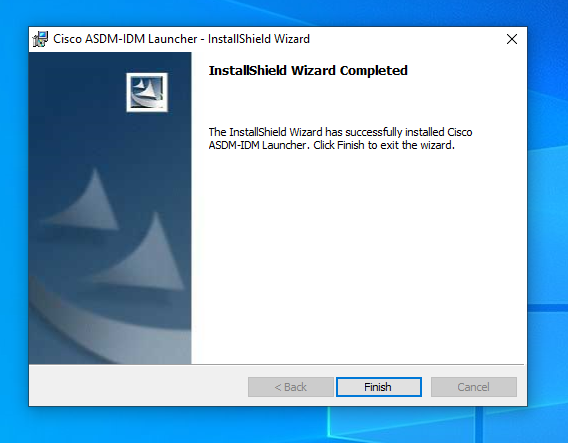
*Cryptochecksum:81d220722758c50f4c9cc6b2e3cf3349*

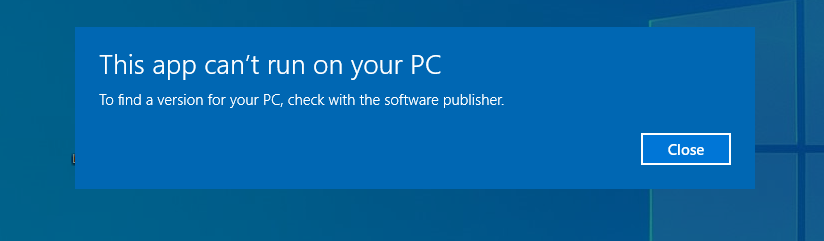
*: end*

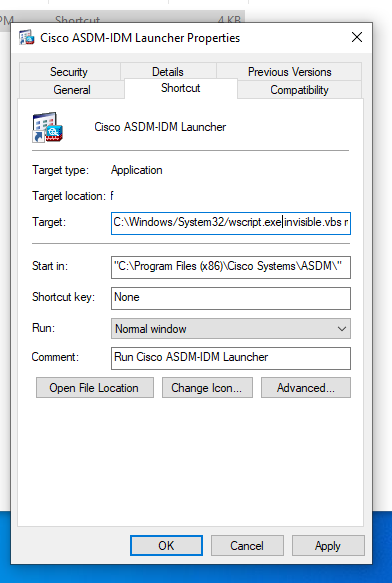
**Screenshots**

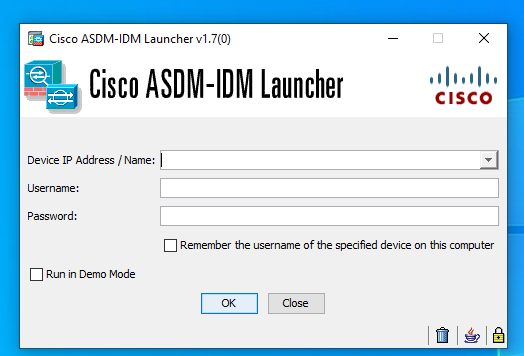




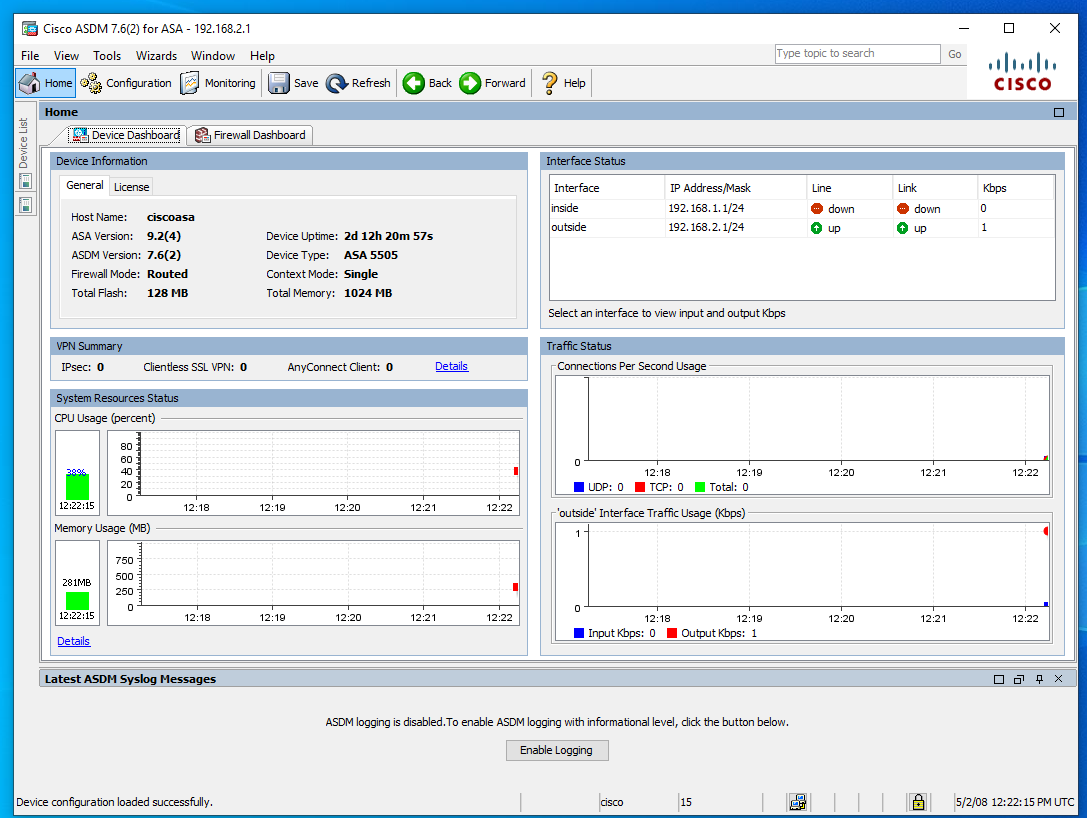












**Problems**

When we downloaded the ASDM on our pc, the application failed to launch with an error message that says, “the app can’t run on your pc”. We solved the problem by changing the application launch target to a correct one. It has a wrong on one default. After that, we failed to connect ASA with ASDM. We found that the problem was java on our computer does not use tls as default. We enabled tls and successfully connected to the ASA with ASDM

**Conclusion**

In this lab, we downloaded and installed ASDM from ASA instead of from cisco.com. We installed java to for ASDM. In ASDM, we can see the resources, interfaces, traffics, and device information of the ASA.

**Teacher Signoff**

