|  |  |
| --- | --- |
|  |  |
| Cisco ASA 5505 Firewall Reset |  |
|  |  |
|  | 09/13/2021CISCO 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.

**Lab Summary**

1. Established console connection between pc and the ASA firewall.
2. Console into the firewall with putty software on pc.
3. Force the firewall into rommon mode to reset password.
4. Restart the device.
5. Enter new configurations.
6. Factory reset the device using commands.
7. Check the configurations after the device automatically restarts.

**Lab Commands**

Confreg – see configuration register

Reload – reboot the device

Boot – boot the device

Copy startup-config running-config – load startup configs

Enable password – password for privileged mode

No config-register – load default configuration registration number

Config factory-default – factory reset

Reload save-config noconfirm – restart the device without saving configurations

**Network Diagrams**

Cisco

ASA

5505

PC

**Configuration**

ASA:

*ciscoasa# show run*

*: Saved*

*:*

*: Serial Number: JMX1237Z0B2*

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

*:*

*ASA Version 9.2(4)*

*!*

*hostname ciscoasa*

*enable password 8Ry2YjIyt7RRXU24 encrypted*

*names*

*!*

*interface Ethernet0/0*

*switchport access vlan 2*

*!*

*interface Ethernet0/1*

*!*

*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*

*nameif outside*

*security-level 0*

*ip address dhcp setroute*

*!*

*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*

*!*

*object network obj\_any*

*nat (inside,outside) dynamic interface*

*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*

*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*

*!*

*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*

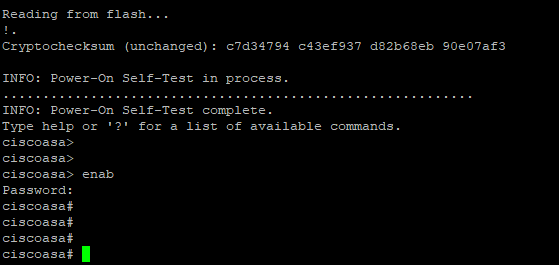
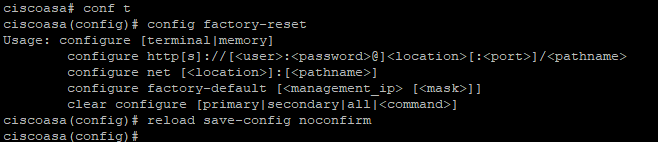
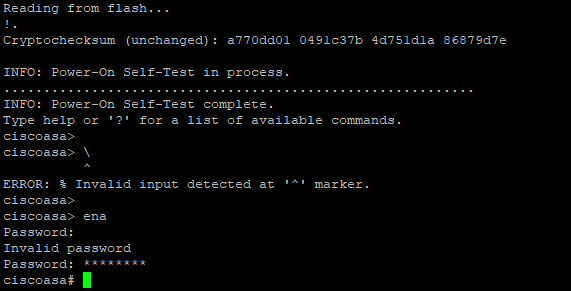
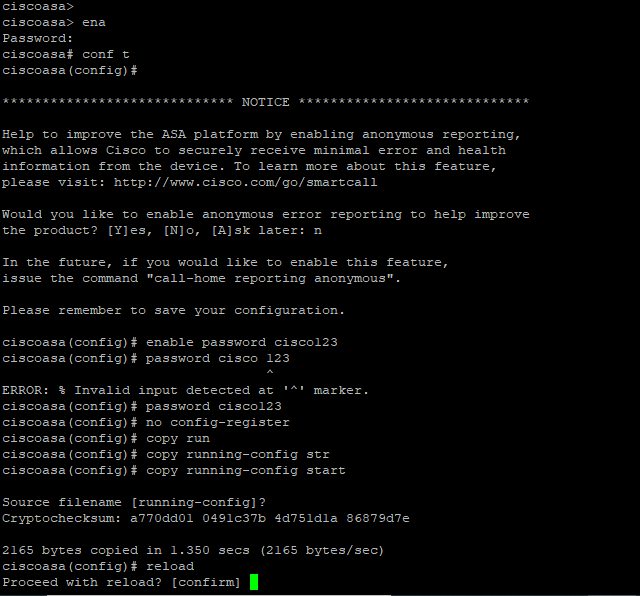
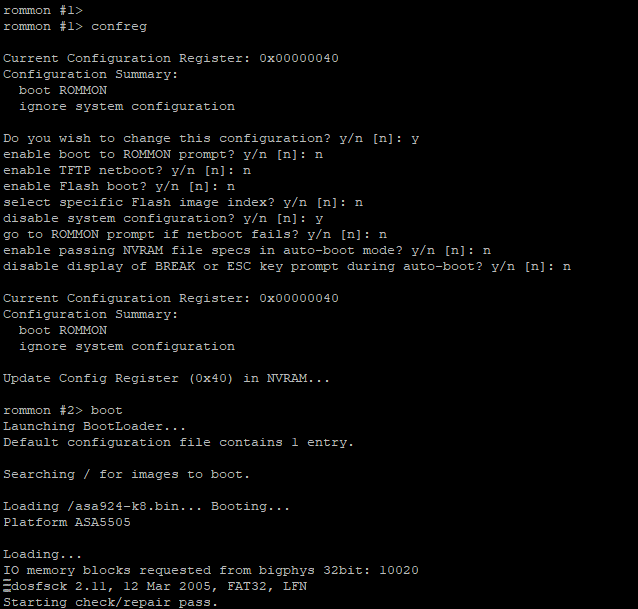
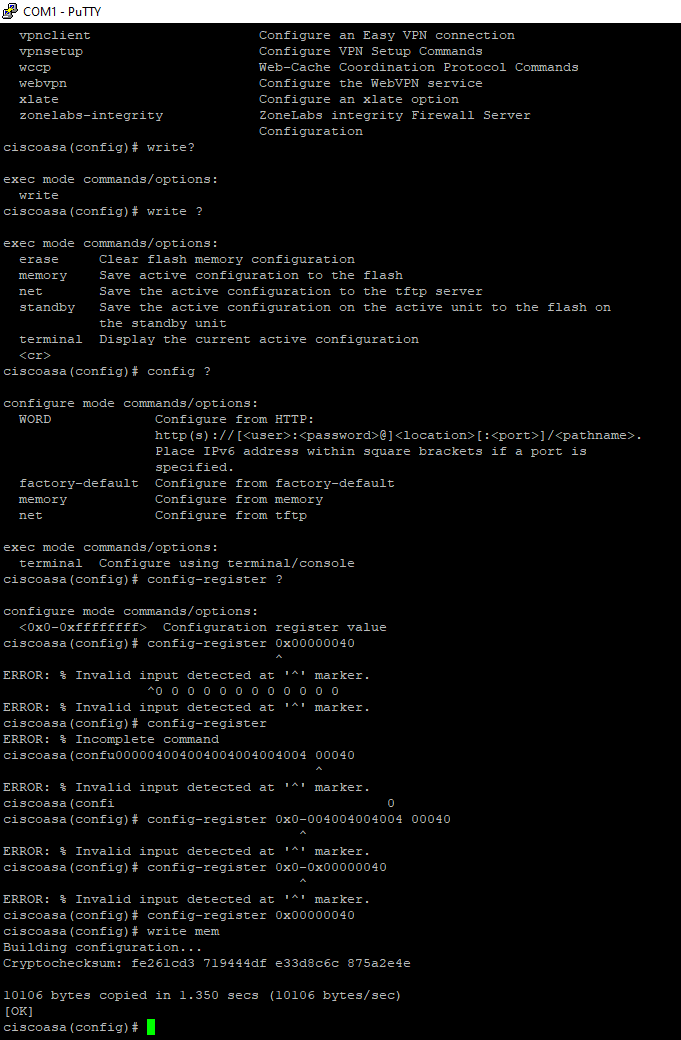
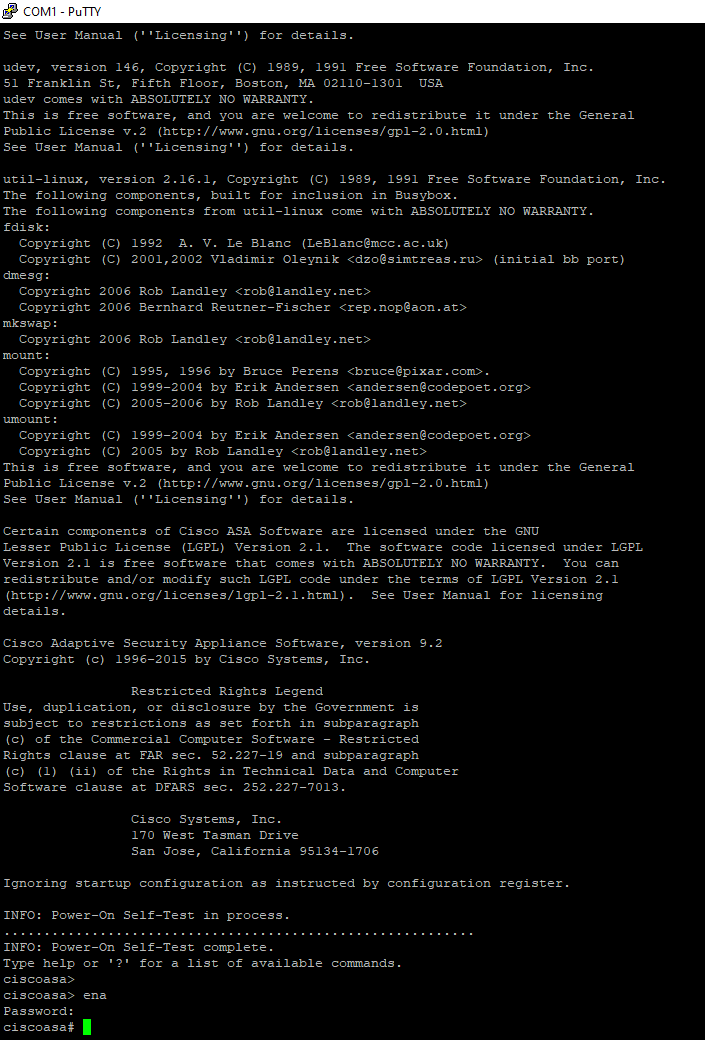
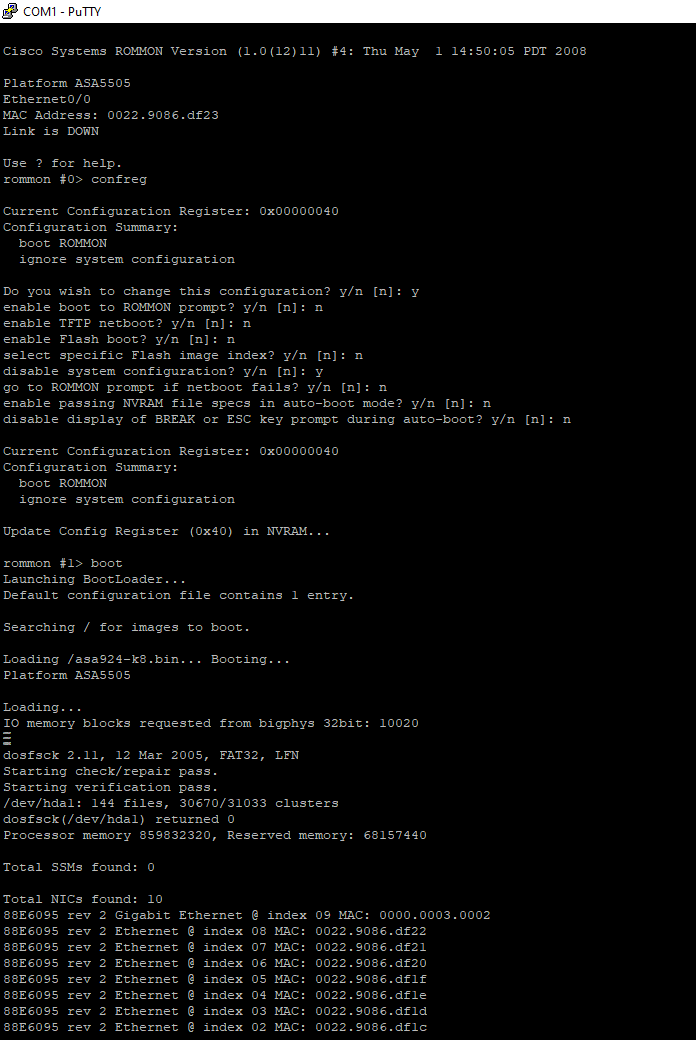
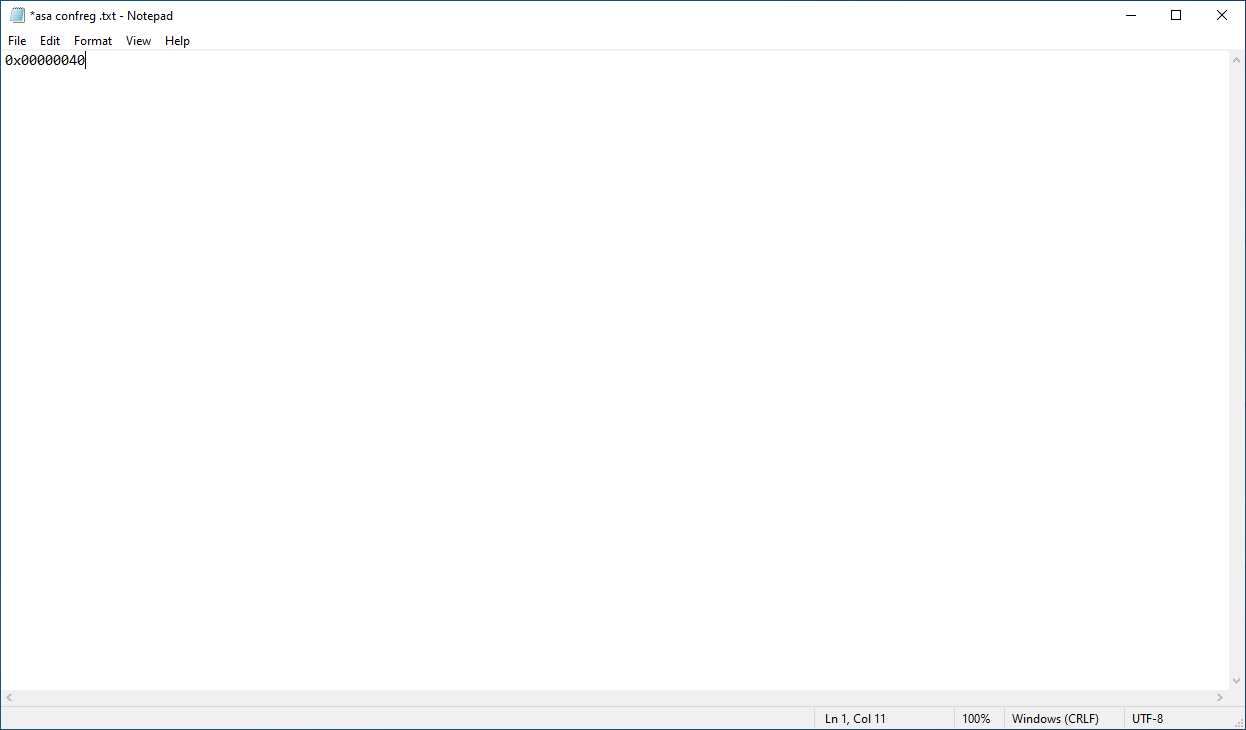
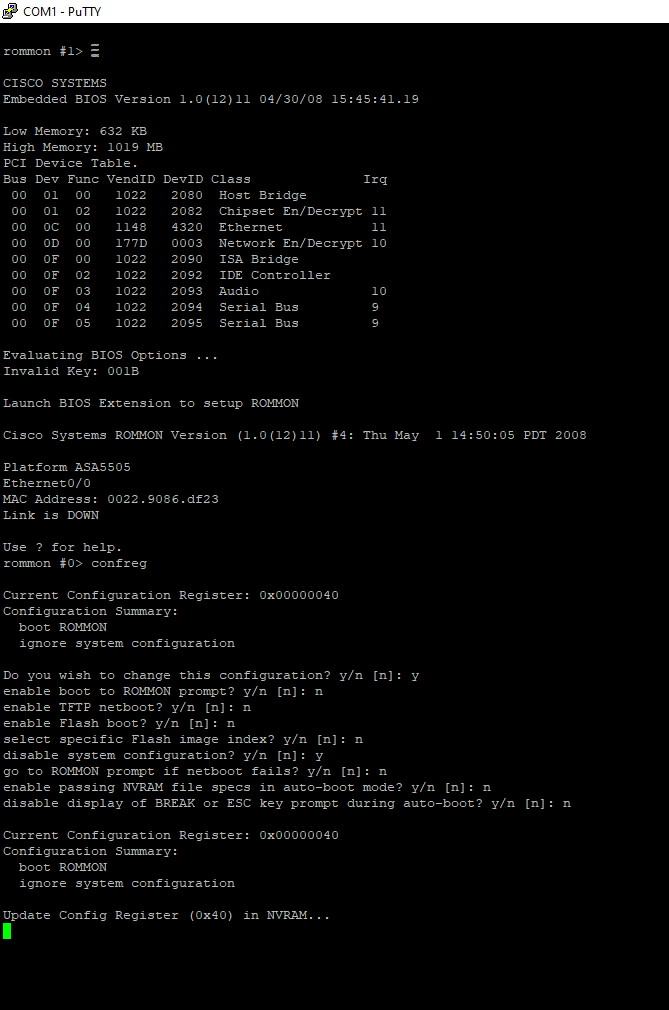
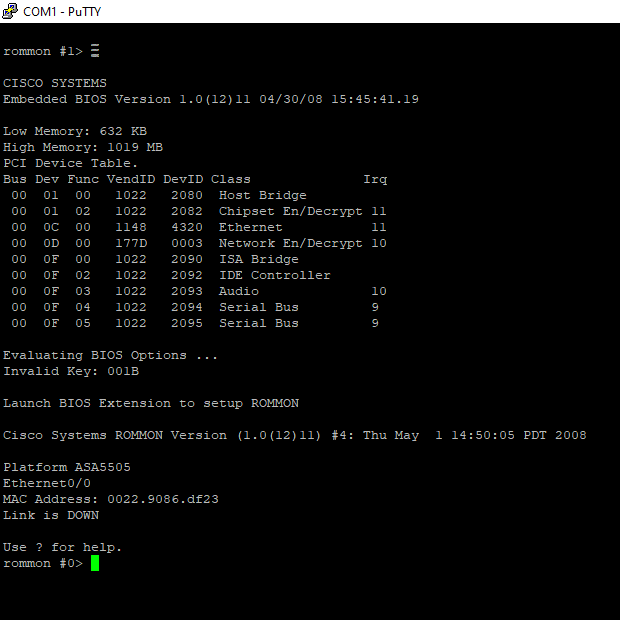
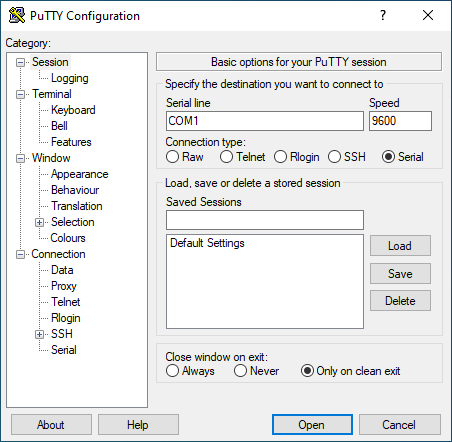
*prompt hostname context*

*Cryptochecksum:c7d34794c43ef937d82b68eb90e07af3*

*: end*

*ciscoasa#*

Screenshots



**Problems**

My first time reset password failed. I believe I may answer no to a question about configurations. I succeeded in the second time.

**Conclusion**

I successfully reset the password, and I confirmed it by seeing there is no password after the reset. I successfully reset the password, and I confirmed it by seeing all my configurations have been cleared after reset.

**Teacher Signoff**

