AutoSecure

Saldırganlar cihaz üzerinde kullanılan servislerin veya protokollerin zayıflıklarını kullanarak saldırılarını gerçekleştiriyor. Zafiyetlere sahip bu özellikler cihazlarda varsayılanda açık gelebiliyor. Bu durum cihazları saldırılara açık hale getiriyor. Varsayılanda açık gelen özelliklere bakıldığında;

- Cisco Discovery Protocol (CDP) - Packet assembler/disassembler (PAD) service - TCP and User Datagram Protocol (UDP) minor services - Maintenance Operation Protocol (MOP) service - Simple Network Management Protocol (SNMP) - HTTP or HTTPS configuration and monitoring - Domain Name System (DNS) - Internet Control Message Protocol (ICMP) redirects - IP source routing - Finger service - ICMP unreachable notifications - IP identification service - Gratuitous ARP (GARP) - Proxy ARP

Cihazlar üzerindeki güvenliği arttırmak adına cihaz üzerinde kullanılmayan özelliklerin kapatılması, kullanılması gereken özellikler için de belirli kısıtlamaların tanımlanması gerekiyor. Bu doğrultuda cihazda kullanılan bazı özellikler için tavsiye edilen kullanım şekli;

- **Cisco Discovery Protocol (CDP),** varsayılanda açık geliyor. İhtiyaç duyuluyorsa istemci bağlı portlarda kapatılması, ihtiyaç duyulmuyorsa cihaz genelinde kapatılması öneriliyor.
- **Link Layer Discovery Protocol (LLDP),** varsayılanda kapalı geliyor. İhtiyaç duyuluyorsa istemci bağlı portlarda kapatılması, ihtiyaç duyulmuyorsa cihaz genelinde kapatılması öneriliyor.
- **Configuration autoloading,** varsayılanda kapalı geliyor. İhtiyaç duyulmadığı durumlarda devre dışı bırakılması öneriliyor.
- **FTP server,** varsayılanda kapalı gelmektedir. Kullanılmadığı durumlarda devre dışı bırakılmalıdır.
- **TFTP server,** varsayılanda kapalı gelmektedir. Kullanılmadığı durumlarda devre dışı bırakılmalıdır.
- **Network Time Protocol (NTP) service,** varsayılanda kapalı gelmektedir. Kullanılmadığı durumlarda devre dışı bırakılmalıdır.
- **Packet assembler/disassembler (PAD) service,** varsayılanda açık gelmektedir. Kullanılmadığı durumlarda devre dışı bırakılmalıdır.
- **TCP and User Datagram Protocol (UDP) minor services,** yeni model cihazlarda açık gelmektedir. Bu hizmet mutlaka devre dışı bırakılmalıdır.
- **Maintenance Operation Protocol (MOP) service,** genelde Ethernet arayüzlerinde açık halde geliyor. Kullanılmadığı durumlarda mutlaka devre dışı bırakılmalıdır.
- **Simple Network Management Protocol (SNMP),** varsayılanda daçık geliyor. Kullanılmadığı durumlarda devre dışı bırakılmalıdır.
- **HTTP or HTTPS configuration and monitoring,** açık olup olmaması cihaz modeline göre değişebiliyor. Kullanılmadığı durumlarda devre dışı bırakılmalıdır. Kullanılması durumunda ACL'ler kullanılarak hizmetlere erişimler kısıtlanmalıdır.
- **Domain Name System (DNS),** varsayılanda açık gelmektedir. Kullanılmadığı durumlarda devre dışı bırakılmalıdır. Kullanılması gerekiyorsa DNS sunucu adresinin ayarlandığından emin olunmalıdır.
- **Internet Control Message Protocol (ICMP) redirects,** varsayılanda açık gelmektedir. Kullanılmadığı durumlarda devre dışı bırakılmalıdır.
- **IP source routing,** varsayılanda açık gelmektedir. Kullanılmadığı durumlarda devre dışı bırakılmalıdır.

- **Finger service,** varsayılanda açık gelmektedir. Kullanılmadığı durumlarda devre dışı bırakılmalıdır.
- **ICMP unreachable notifications,** varsayılanda açık gelmektedir. Güvenilmeyen networklere bağlı olunan arayüzlerde devre dışı bırakılması gerekiyor.
- **ICMP mask reply,** varsayılanda kapalı geliyor. Güvenilmeyen networklere bağlı olunan arayüzlerde devre dışı bırakılması gerekiyor.
- **IP identification service,** varsayılanda açık gelmektedir. Mutlaka devre dışı bırakılmalıdır.
- **TCP keepalives,** varsayılanda kapalı gelmektedir. TCP bağlantılarını yönetmek ve belirli (DoS) saldırılarını önlemek için cihaz genelinde etkinleştirilmelidir. Gerekli olmadığı durumlarda devre dışı bırakılmalıdır.
- **Gratuitous ARP (GARP),** varsayılanda açık gelmektedir. Gerek duyulmadığı taktirde arayüzlerde devre dışı bırakılmalıdır.
- **Proxy ARP,** varsayılanda açık gelmektedir. Kullanılmıyorsa bu özellik devre dışı bırakılmalıdır.

Cihazlarda güvenlik zafiyeti oluşturabilecek özellikler ve durumlar tespit edilip gerekli önlemler manuel olarak alınabiliyor. Cisco marka cihazlarda bu süreci hızlandırmak adına işlemlerin bir kısmını otomatize halde gerçekleştirebilen AutoSecure özelliği bulunmaktadır.

AutoSecure, cihaz üzerinde güvenlik zafiyeti oluşturabilecek belirli özellikleri ve durumları tespit ederek önlem alma sürecini otomatize hale getiren bir özelliktir. Bu süreci Interactive ve Non-Interactive olmak üzere iki farklı modda uygulayabiliyor.

- Interactive Mode, özelliklerin devreye alınması veya devre dışı bırakılması için veya parola atamalarının gerektiği yerde kararın kullanıcıya bırakıldığı moddur. Privileged Exec modunda "**auto secure**" komutu kullanıldığında Interactive modda çalışıyor.
- Non-Interactive Mode, AutoSecure özelliğinde varsayılanda gelen güvenlik ayarlamaları otomatik olarak uygulanır. Bu süreçte uygulanan hiçbir güvenlik önlemi kararı kullanıcıya bırakılmaz. Privileged Exec modunda "**auto secure no-interactive**" komutu kullanıldığında Interactive modda çalışıyor.

AutoSecure özelliği çalıştırıldığında cihazda alınan güvenlik önlemleri;

1 - Aşağıdaki hizmetleri devre dışı bırakır

- Finger
- PAD
- Small Servers
- Bootp
- HTTP service
- Identification Service
- CDP
- NTP
- Source Routing

2 - Aşağıdaki hizmetleri etkinleştirir

- Password-encryption service
- Tuning of scheduler interval/allocation
- TCP synwait-time
- TCP-keepalives-in and tcp-kepalives-out
- SPD configuration
- No ip unreachables for null 0

3 – Cihazın arayüzlerinde aşağıdaki hizmetleri devre dışı bırakır

- ICMP
- Proxy-Arp
- Directed Broadcast
- Disables MOP service
- Disables icmp unreachables
- Disables icmp mask reply messages

4 - Güvenlik için Log kayıtlarında aşağıdaki özellikleri devreye alır

- Enables sequence numbers & timestamp
- Provides a console log
- Sets log buffered size
- Provides an interactive dialogue to configure the logging server ip address

5 – Cihaza erişimi sürecinde kullanılan çeşitli mekanizmaları güvence altına alır

- Checks for a banner and provides facility to add text to automatically configure:
- Login and password
- Transport input & output
- Exec-timeout
- Local AAA
- SSH timeout and ssh authentication-retries to minimum number
- Enable only SSH and SCP for access and file transfer to/from the router
- Disables SNMP If not being used

6 - Forwarding/Data Plane için aşağıdaki güvenlik önlemlerini ugular.

- Enables Cisco Express Forwarding (CEF) or distributed CEF on the router, when available
- Anti-spoofing
- Blocks all IANA reserved IP address blocks
- Blocks private address blocks if customer desires
- Installs a default route to NULL 0, if a default route is not being used
- Configures TCP intercept for connection-timeout, if TCP intercept feature is available and the user is interested
- Starts interactive configuration for CBAC on interfaces facing the Internet, when using a Cisco IOS Firewall image
- Enables NetFlow on software forwarding platforms

AutoSecure Konfigürasyonu

- AutoSecure özelliğiyla cihaz genelinde Intreractive modda çalıştırmak için Privileged Exec modunda “auto secure” komutu kullanılıyor. Bu komut kullanıldıktan sonra cihaz üzerinde güvenlik önlemleri alınırken parola belirleme, banner ekleme gibi işlemler için kullanıcı girişleri gerkecektir. AuroSecure özelliği Interactive modunda çalıştırıldığında;
    - İlk olarak arayüzlerden giriş bilgisi topluyor.
    -

- AutoSecure özelliği özelleştirilerek çalıştırılmak istendiğinde “**auto secure {no-interact | full} [forwarding | management] [ntp | login | ssh | firewall | tcp-intercept]”** komutu kullanılır. Bu parametrelerin açıklammalarına bakıldığında;
    - no-interactive, kulanıcı etkileşimi gerektiren güvenlik önlemlerinin alınmamasını sağlayan parametredir (sadece varsayılanda gelen güvenlik önlemleri alınıyor. Örnek olarak bir banner eklenmiyor veya enable girişine parola ataması yapılmıyor).
    - full, kullanıcı etkileşimli güvenlik önlemleri de dahil olmak üzere tanımlı bütün güvenlik önlemlerinin alınması için kullanılan komuttur. Aynı zamanda varsayılan ayardır. Yani “**auto secure**” komutuna herhangi bir parametre verilmediğinde de bu özellik çalışmaktadır.
    - forwarding, sadece Data/Forwarding Plane için güvenlik önlemlerinin alındığı parametredir.

```
R1#auto secure forwarding ?
  firewall       AutoSecure Firewall
  full           Interactive full session of AutoSecure
  no-interact    Non-interactive session of AutoSecure
  tcp-intercept  AutoSecure TCP Intercept
  <cr>
```

    - management, sadece Management Plane için güvenlik önlemlerinin alındığı parametredir.

```
R1#auto secure management ?
  full         Interactive full session of AutoSecure
  login        AutoSecure Login
  no-interact  Non-interactive session of AutoSecure
  ntp          AutoSecure NTP
  ssh          AutoSecure SSH
  <cr>
```

    - ntp, AutoSecure özelliği içerisinde NTP protokolü için tanımlanan güvenlik önlemlerinin uygulandığı parametredir.
    - login, AutoSecure özelliği içerisinde oturum açma işlemleri için tanımlanan güvenlik önlemlerinin uygulandığı parametredir.

```
Enable secret is either not configured or
 is the same as enable password
Enter the new enable secret:
Confirm the enable secret :
Enter the new enable password:
Confirm the enable password:

Configuration of local user database
Enter the username: SecLab
Enter the password:
Confirm the password:
Configuring AAA local authentication
Configuring Console, Aux and VTY lines for
local authentication, exec-timeout, and transport
Securing device against Login Attacks
Configure the following parameters

Blocking Period when Login Attack detected: [redacted]

Maximum Login failures with the device: [redacted]

Maximum time period for crossing the failed login attempts: [redacted]
```

```
This is the configuration generated:

enable secret 5 $1$8pXQ$8hDk[redacted]
enable password 7 135445415[redacted]
username SecLab password 7 11584B564[redacted]
aaa new-model
aaa authentication login local_auth local
line con 0
 login authentication local_auth
 exec-timeout 5 0
 transport output telnet
line aux 0
 login authentication local_auth
 exec-timeout 10 0
 transport output telnet
line vty 0 4
 login authentication local_auth
 transport input telnet
login block-for [redacted] attempts [redacted] within [redacted]
!
end
```

- ssh, AutoSecure özelliği içerisinde SSH özelliği için tanımlanan güvenlik önlemlerinin uygulandığı parametredir.

```
Configure SSH server? [yes]: y
Enter the domain-name: Seclab.y

This is the configuration generated:

ip domain-name Seclab.y
crypto key generate rsa general-keys modulus 1024
ip ssh time-out 60
ip ssh authentication-retries 2
line vty 0 4
 transport input ssh telnet
!
end
```

- firewall, AutoSecure özelliği içerisinde güvenlik duvarı için tanımlanan yapılandırmaların uygulandığı parametredir.

```
This is the configuration generated:

ip inspect audit-trail
ip inspect dns-timeout 7
ip inspect tcp idle-time 14400
ip inspect udp idle-time 1800
ip inspect name autosec_inspect cuseeme timeout 3600
ip inspect name autosec_inspect ftp timeout 3600
ip inspect name autosec_inspect http timeout 3600
ip inspect name autosec_inspect rcmd timeout 3600
ip inspect name autosec_inspect realaudio timeout 3600
ip inspect name autosec_inspect smtp timeout 3600
ip inspect name autosec_inspect tftp timeout 30
ip inspect name autosec_inspect udp timeout 15
ip inspect name autosec_inspect tcp timeout 3600
ip access-list extended autosec_firewall_acl
 permit udp any any eq bootpc
 deny ip any any
!
end
```

- tcp-intercept, AutoSecure özelliği içerisinde TCP-Intercept özelliği için tanımlanan konfigürasyonların uygulandığı parametredir.

```
Tcp intercept feature is used prevent tcp syn attack
on the servers in the network. Create autosec_tcp_intercept_list
to form the list of servers to which the tcp traffic is to
be observed


Enable tcp intercept feature? [yes/no]: y

This is the configuration generated:

ip tcp intercept list autosec_tcp_intercept_list
ip tcp intercept drop-mode random
ip tcp intercept watch-timeout 15
ip tcp intercept connection-timeout 3600
ip tcp intercept max-incomplete low 450
ip tcp intercept max-incomplete high 550
!
end
```