CYBER DEFENSE

❖ حسین ملک زاده

مشاور و تحلیل گر ارشد امنیت سایبری

کارشناس ارشد امنیت اطلاعات ازدانشگاه Sapienza Universityرم – ایتالیا

مدرس و عضو هیات علمی دانشگاه بین المللی نورث وست Northwest International University

مدرس و عضو هیات علمی دانشگاه نیوجرسی New Jersey International Open University

مدرس و عضو هیات علمی موسسه دانشگاهی DEI Institute - Online Universityآفریقا

دارای مدرک دکترا مدیریت امنیت سایبری DBA - Cyber Security Management از دانشگاه بین المللی نورث وست

ممیز و سرممیز امنیت اطلاعات ISMS ISO27001-2013

دارای مدارک سطح عالی امنیت اطلاعات CISSP , CISA

دارای مدرک مشاور ارشد امنیت سیستمی SSCP

طراح – مشاور و مجری پروژه¬های شبکه و امنیت اطلاعات ISMS , SOC , NOC

دارای بیش از ۲۴ سال سابقه آموزشی – اجرایی و مدیریتی درزمینه پروژه¬های شبکه و امنیت در داخل و خارج از کشور

مدرس دوره¬های تخصصی شبکه و امنیت با بیش از دوازده هزارساعت تدریس درموسسات داخلی و بین المللی

دارای تحصیلات و مدارک بین المللی :

MCSE , CCNA ,CCNA Security , CCNP , CEH , CISSP , CWNA , ISMS , SSCP, GSNA

عضوانجمن مهندسین کامپیوتر و فناوری آمریکا IEEE , ACM

مولف کتاب هنر هک کردن انسان در حوزه امنیت در مهندسی اجتماعی Social engineering

www.Hosseinmalekzadeh.com

Mobile: 09153133217

E-mail: Hoseeinmalekzadeh@Gmail.com

Telegram Channel : https://t.me/HosseinMalekzadeh

http://www.linkedin.com/in/hosseinmalekzadeh

@HOSSEINMALEKZADEH2015

@HOSSEINMALEKZADEH

By. Hossein Malekzadeh

Cyber Security Consultant and Manager

www.Hosseinmalekzadeh.com

Mobile : 09153133217

نقشه شبکه سازمان (دفتر مرکزی)

سناریوی سازمان

یک سازمان متوسط با حدود ۵۰۰ کارمند
دارای دفتر مرکزی و دو شعبه
خدمات اصلی سازمان شامل:

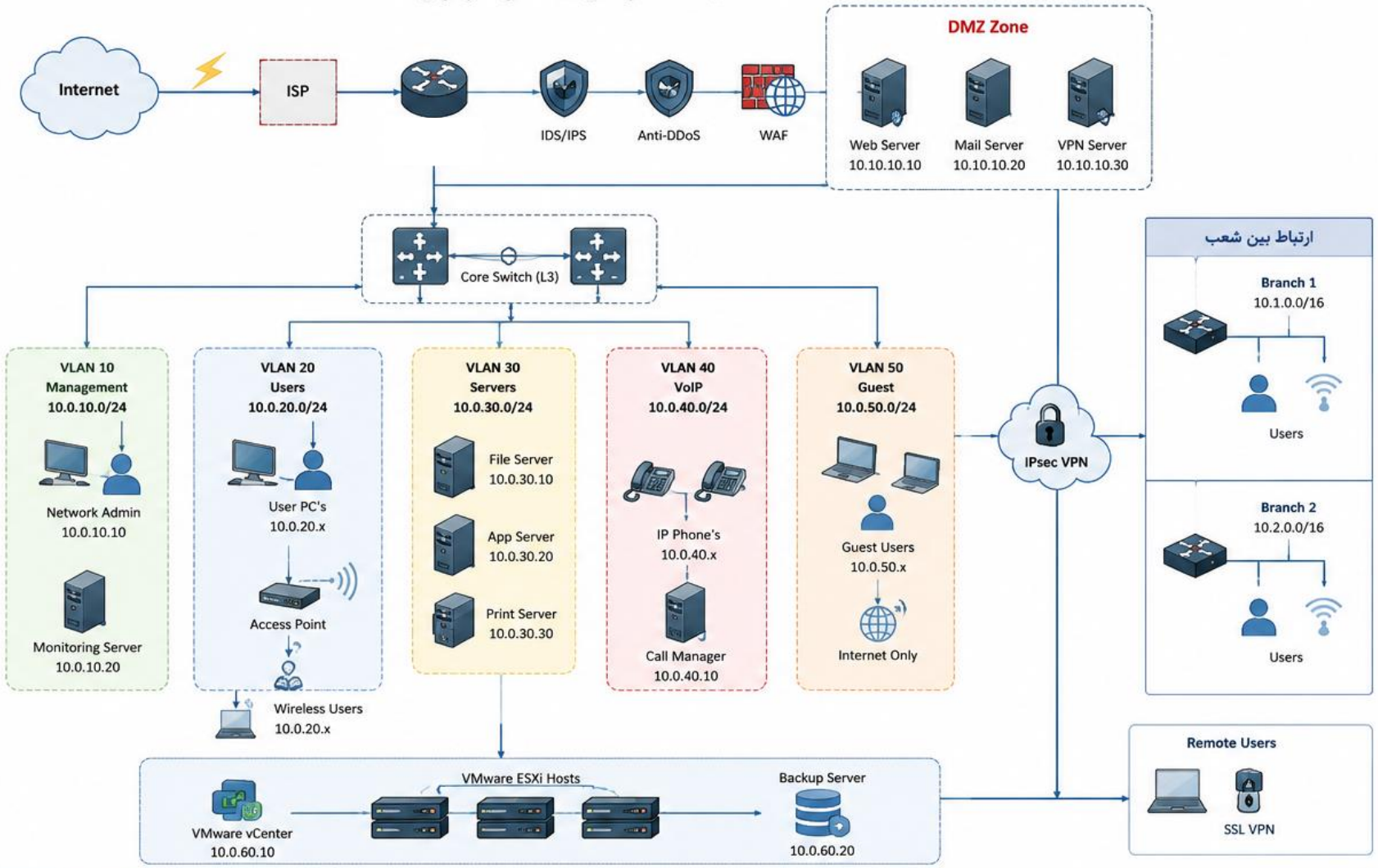
- سرویس های دایرکتوری (Active Directory)
- سرورهای فایل و پرینت
- سرور برنامه کاربردی تحت وب
- سیستم تلفنی تحت شبکه (VoIP)
- دسترسی کاربران به اینترنت
- ارتباط امن بین شعب از طریق VPN
- زیرساخت مجازی سازی با VMware

اهداف امنیتی

- حفاظت لایه به لایه از اطلاعات و سرویس ها
- جلوگیری از دسترسی غیرمجاز
- جلوگیری از حرکت جانبی مهاجم در شبکه
- مانیتورینگ و پاسخ به رخدادها
- پشتیبان گیری و تداوم کسب و کار

چالش ها / تهدیدات

- حملات اینترنتی (Brute Force, Exploit, DDoS)
- فیشینگ و مهندسی اجتماعی
- بدافزار و باج افزار
- تهدیدات داخلی و دسترسی بیش از حد
- نشت اطلاعات
- خرابی تجهیزات و از دسترس خارج شدن سرویس ها



راهنمای نمادها

اینترنت — کلاینت — فایروال / روتر
سیستم امنیتی — تلفن تحت شبکه — سوئیچ لایه ۳
دسترسی بی سیم — سرور

نکات طراحی امنیتی (Defense in Depth)

- لایه محیطی: فایروال, IDS/IPS, Anti-DDoS, WAF
- لایه شبکه: تقسیم بندی VLAN, Private VLAN, Private VLAN Security
- لایه سیستم: هاردنینگ سررورها و کلاینت ها، بروزرسانی Patch Management
- لایه هویت و دسترسی: Mtive Directory Security, Least Privilege Security
- لایه مانیتورینگ: جمع آوری و تحلیل لاگ ها در SIEM
- لایه داده: رمزنگاری: DLP, Backup منظم
- لایه پنجم پاسخ: Incident Response Plan و تمرین دوره ای

جدول آدرس دهی

VLAN	Network	Gateway	Description
10	10.0.10.0/24	10.0.10.1	Management
20	10.0.20.0/24	10.0.20.1	Users
30	10.0.30.0/24	10.0.30.1	Servers
40	10.0.40.0/24	10.0.40.1	VoIP
50	10.0.50.0/24	10.0.50.1	Guest
60	10.0.60.0/24	10.0.60.1	Virtualization/Backup
DMZ	10.10.10.0/24	10.10.10.1	DMZ Zone

- یکی از کاربردی‌ترین و مهمترین مصرف‌های دستور tcpdump نحوه استفاده از آن برای اسنیف پکت‌های یک IP خاص می‌باشد.
- برای اسنیف یک IP خاص از پارامتر زیر استفاده می‌شود.
- اسنیف یک IP از مبدا
- tcpdump -i eth0 src 192.168.100.60

```
┌──(root㉿kali)-[/home/hesam/Desktop/log]
└─# tcpdump -i eth0 src 192.168.100.150
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
04:35:44.082965 IP 192.168.100.150.46199 > dns.google.domain: 48772+ A? location.services.mozilla.com. (47)
04:35:44.083209 IP 192.168.100.150.46199 > dns.google.domain: 23681+ AAAA? location.services.mozilla.com. (47)
04:35:44.146597 IP 192.168.100.150.41709 > dns.google.domain: 5498+ PTR? 8.8.8.8.in-addr.arpa. (38)
04:35:44.170538 IP 192.168.100.150.57218 > ec2-44-237-156-211.us-west-2.compute.amazonaws.com.https: Flags [S], seq 11733
60531, win 64240, options [mss 1460,sackOK,TS val 1065633301 ecr 0,nop,wscale 7], length 0
04:35:44.215064 IP 192.168.100.150.46737 > dns.google.domain: 51333+ PTR? 150.100.168.192.in-addr.arpa. (46)
04:35:44.266390 IP 192.168.100.150.47581 > dns.google.domain: 45756+ PTR? 211.156.237.44.in-addr.arpa. (45)
04:35:44.422185 IP 192.168.100.150.57222 > ec2-44-237-156-211.us-west-2.compute.amazonaws.com.https: Flags [S], seq 40871
03859, win 64240, options [mss 1460,sackOK,TS val 1065633553 ecr 0,nop,wscale 7], length 0
04:35:44.548819 IP 192.168.100.150.57218 > ec2-44-237-156-211.us-west-2.compute.amazonaws.com.https: Flags [.], ack 11568
0704, win 502, options [nop,nop,TS val 1065633679 ecr 1068995761], length 0
04:35:44.553260 IP 192.168.100.150.57218 > ec2-44-237-156-211.us-west-2.compute.amazonaws.com.https: Flags [P.], seq 0:51
7, ack 1, win 502, options [nop,nop,TS val 1065633684 ecr 1068995761], length 517
04:35:44.855323 IP 192.168.100.150.57222 > ec2-44-237-156-211.us-west-2.compute.amazonaws.com.https: Flags [.], ack 21379
79271, win 502, options [nop,nop,TS val 1065633986 ecr 1068996081], length 0
04:35:44.858661 IP 192.168.100.150.57222 > ec2-44-237-156-211.us-west-2.compute.amazonaws.com.https: Flags [P.], seq 0:51
7, ack 1, win 502, options [nop,nop,TS val 1065633989 ecr 1068996081], length 517
04:35:44.917949 IP 192.168.100.150.57218 > ec2-44-237-156-211.us-west-2.compute.amazonaws.com.https: Flags [.], ack 1289,
 win 501, options [nop,nop,TS val 1065634049 ecr 1068996183], length 0
```

- اسنیف یک ip از مقصد
- tcpdump -i ens33 dst 192.168.100.60
- تمامی پکت‌هایی که به 192.168.100.60 ارسال می‌شود ، اسنیف خواهد شد.

```
┌──(root㉿kali)-[/home/hesam/Desktop/log]
└─# ping 192.168.100.60
PING 192.168.100.60 (192.168.100.60) 56(84) bytes of data.
64 bytes from 192.168.100.60: icmp_seq=1 ttl=128 time=0.285 ms
64 bytes from 192.168.100.60: icmp_seq=2 ttl=128 time=0.261 ms
64 bytes from 192.168.100.60: icmp_seq=3 ttl=128 time=2.15 ms
64 bytes from 192.168.100.60: icmp_seq=4 ttl=128 time=0.298 ms
^C
--- 192.168.100.60 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3064ms
rtt min/avg/max/mdev = 0.261/0.748/2.150/0.809 ms

┌──(root㉿kali)-[/home/hesam/Desktop/log]
└─#
```

Command Prompt

```
(c) Microsoft Corporation. All rights reserved.

C:\Users\hesam>ping 192.168.100.150

Pinging 192.168.100.150 with 32 bytes of data:
Reply from 192.168.100.150: bytes=32 time<1ms TTL=64
Reply from 192.168.100.150: bytes=32 time<1ms TTL=64
Reply from 192.168.100.150: bytes=32 time<1ms TTL=64
Reply from 192.168.100.150: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.100.150:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\hesam>
```

```
┌──(root㉿kali)-[/home/hesam/Desktop/log]
└─# tcpdump -i eth0 dst 192.168.100.60
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
04:42:41.295761 IP 192.168.100.150 > 192.168.100.60: ICMP echo reply, id 1, seq 22, length 40
04:42:42.300523 IP 192.168.100.150 > 192.168.100.60: ICMP echo reply, id 1, seq 23, length 40
04:42:43.313687 IP 192.168.100.150 > 192.168.100.60: ICMP echo reply, id 1, seq 24, length 40
04:42:44.326501 IP 192.168.100.150 > 192.168.100.60: ICMP echo reply, id 1, seq 25, length 40
04:42:46.290933 ARP, Reply 192.168.100.150 is-at 00:0c:29:5f:30:0e (oui Unknown), length 28
04:42:46.461314 ARP, Request who-has 192.168.100.60 tell 192.168.100.150, length 28
```

```
252243 ecr 90099927], length 0
13:26:56.960060 IP 192.168.11.23.ftp > 192.168.11.64.33484: Flags [P.], seq 421:443, ack 181, win 227, options [nop
,nop,TS val 90252873 ecr 90099927], length 22: FTP: 530 Login incorrect.
13:26:56.960372 IP 192.168.11.64.33484 > 192.168.11.23.ftp: Flags [.], ack 443, win 229, options [nop,nop,TS val 90
100567 ecr 90252873], length 0
13:26:56.960618 IP 192.168.11.23.ftp > 192.168.11.64.33484: Flags [F.], seq 443, ack 181, win 227, options [nop,nop
,TS val 90252873 ecr 90100567], length 0
13:26:56.999814 IP 192.168.11.64.33484 > 192.168.11.23.ftp: Flags [.], ack 444, win 229, options [nop,nop,TS val 90
100577 ecr 90252873], length 0
13:27:00.950066 IP 192.168.11.64.33484 > 192.168.11.23.ftp: Flags [P.], seq 181:191, ack 444, win 229, options [nop
,nop,TS val 90101564 ecr 90252873], length 10: FTP: USER dan
13:27:00.950103 IP 192.168.11.23.ftp > 192.168.11.64.33484: Flags [R], seq 1154130863, win 0, length 0
09:49:38.108457 IP 92.242.140.21 > 192.168.11.1: ICMP echo request, id 2994, seq 1, length 64
09:49:38.108945 IP 92.242.140.21 > 192.168.11.2: ICMP echo request, id 2994, seq 1, length 64
09:49:38.109423 IP 92.242.140.21 > 192.168.11.3: ICMP echo request, id 2994, seq 1, length 64
09:49:38.109903 IP 92.242.140.21 > 192.168.11.4: ICMP echo request, id 2994, seq 1, length 64
09:49:38.110401 IP 92.242.140.21 > 192.168.11.5: ICMP echo request, id 2994, seq 1, length 64
09:49:38.110877 IP 92.242.140.21 > 192.168.11.6: ICMP echo request, id 2994, seq 1, length 64
09:49:38.111356 IP 92.242.140.21 > 192.168.11.7: ICMP echo request, id 2994, seq 1, length 64
09:49:38.112897 IP 92.242.140.21 > 192.168.11.8: ICMP echo request, id 2994, seq 1, length 64
09:49:38.113430 IP 92.242.140.21 > 192.168.11.9: ICMP echo request, id 2994, seq 1, length 64
09:49:38.113960 IP 92.242.140.21 > 192.168.11.10: ICMP echo request, id 2994, seq 1, length 64
```

درشکل بالا می بینید که یکسری بسته های ICMP دارد ارسال میشه اما هیچ replay دیده یا ثبت نشده

Three-Way Handshake
یا دست تکانی سه مرحله ای

- TCPکه یکی از پروتکل های مهم شبکه است، برای برقراری ارتباط بین دو دستگاه مانند کلاینت و سرور، از روشی به نام دست تکانی سه مرحله ای یا Three-Way Handshakeاستفاده می کند. مراحل این دست تکانی به شکل زیر است :

- **مرحله اول :** در این مرحله سیستم اول بسته ای را که فقط flag SYN در آن تنظیم شده است، به سیستم دوم ارسال می کند.(**درخواست برقراری ارتباط**)
- **مرحله دوم:** در این مرحله سیستم دوم بسته ای را که flagهای SYN و ACK در آن تنظیم شده است به سیستم اول پاسخ می دهد.(**آمادگی برای ارتباط**)

- **مرحله سوم:** در این مرحله سیستم اول پاسخی را به سیستم دوم ارسال می کند که فقط حاوی ACK flag درون بسته ارسالی می باشد.(**برقراری ارتباط**)

- اگر سه بدون هیچ مشکلی انجام شود، یک ارتباط TCP بین دو سیستم برقرار شده است.

```
┌──(root㉿kali)-[/home/hesam/Desktop/log]
└─# ping 192.168.100.60
PING 192.168.100.60 (192.168.100.60) 56(84) bytes of data.
64 bytes from 192.168.100.60: icmp_seq=1 ttl=128 time=0.489 ms
64 bytes from 192.168.100.60: icmp_seq=2 ttl=128 time=0.549 ms
64 bytes from 192.168.100.60: icmp_seq=3 ttl=128 time=0.625 ms
64 bytes from 192.168.100.60: icmp_seq=4 ttl=128 time=0.463 ms
64 bytes from 192.168.100.60: icmp_seq=5 ttl=128 time=0.565 ms
64 bytes from 192.168.100.60: icmp_seq=6 ttl=128 time=0.733 ms
64 bytes from 192.168.100.60: icmp_seq=7 ttl=128 time=0.677 ms
64 bytes from 192.168.100.60: icmp_seq=8 ttl=128 time=0.666 ms
64 bytes from 192.168.100.60: icmp_seq=9 ttl=128 time=0.765 ms
64 bytes from 192.168.100.60: icmp_seq=10 ttl=128 time=0.901 ms
^C
--- 192.168.100.60 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9040ms
rtt min/avg/max/mdev = 0.463/0.643/0.901/0.127 ms
```

- و اگردقت کنید درپینگ معمولی Seq Number تغییر می کند یعنی درواقع همان tree way handshak یا دست تکانی سه مرحله ای صورت می گیرد و یک عدد به seq اضافه می شود برای هر درخواست

درصورتی که در این گزارش seq ها ثابت هست

```
└─# tcpdump -r adversary.pcap 'host 92.242.140.21' -n
reading from file adversary.pcap, link-type EN10MB (Ethernet), snapshot length 65535
09:49:38.108457 IP 92.242.140.21 > 192.168.11.1: ICMP echo request, id 2994, seq 1, length 64
09:49:38.108945 IP 92.242.140.21 > 192.168.11.2: ICMP echo request, id 2994, seq 1, length 64
09:49:38.109423 IP 92.242.140.21 > 192.168.11.3: ICMP echo request, id 2994, seq 1, length 64
09:49:38.109903 IP 92.242.140.21 > 192.168.11.4: ICMP echo request, id 2994, seq 1, length 64
09:49:38.110401 IP 92.242.140.21 > 192.168.11.5: ICMP echo request, id 2994, seq 1, length 64
09:49:38.110877 IP 92.242.140.21 > 192.168.11.6: ICMP echo request, id 2994, seq 1, length 64
09:49:38.111356 IP 92.242.140.21 > 192.168.11.7: ICMP echo request, id 2994, seq 1, length 64
09:49:38.112897 IP 92.242.140.21 > 192.168.11.8: ICMP echo request, id 2994, seq 1, length 64
09:49:38.113430 IP 92.242.140.21 > 192.168.11.9: ICMP echo request, id 2994, seq 1, length 64
09:49:38.113960 IP 92.242.140.21 > 192.168.11.10: ICMP echo request, id 2994, seq 1, length 64
```

پس نشان دهنده این است که عملا مهاجم ازطریق ابزاردارد به سمت سرور ما حمله می کند

و حتی در این حالت علاوه بر **seq** که تغییر نکرده **Id** هم به ازا هر IP ثابت هست در صورتی که باید تغییر کند و این نشان دهنده این هست که حمله **ping Sweep** به سمت سرور ما از طریق یک ابزار درحال انجام شدن هست .

```
reading from file adversary.pcap, link-type EN10MB (Ethernet), snapshot length 65535
09:49:38.108457 IP 92.242.140.21 > 192.168.11.1: ICMP echo request, id 2994, seq 1, length 64
09:49:38.108945 IP 92.242.140.21 > 192.168.11.2: ICMP echo request, id 2994, seq 1, length 64
09:49:38.109423 IP 92.242.140.21 > 192.168.11.3: ICMP echo request, id 2994, seq 1, length 64
09:49:38.109903 IP 92.242.140.21 > 192.168.11.4: ICMP echo request, id 2994, seq 1, length 64
09:49:38.110401 IP 92.242.140.21 > 192.168.11.5: ICMP echo request, id 2994, seq 1, length 64
09:49:38.110877 IP 92.242.140.21 > 192.168.11.6: ICMP echo request, id 2994, seq 1, length 64
09:49:38.111356 IP 92.242.140.21 > 192.168.11.7: ICMP echo request, id 2994, seq 1, length 64
09:49:38.112897 IP 92.242.140.21 > 192.168.11.8: ICMP echo request, id 2994, seq 1, length 64
09:49:38.113430 IP 92.242.140.21 > 192.168.11.9: ICMP echo request, id 2994, seq 1, length 64
09:49:38.113960 IP 92.242.140.21 > 192.168.11.10: ICMP echo request, id 2994, seq 1, length 64
```

وقتی بسته ها را در Wiresharkاز نزدیک مشاهده می کنید، می بینید که در اینجا فقط بسته های ARPدر حین اسکن شبکه ارسال می شوند.

arp

No.	Time	Source	Destination	Protocol	Length	Info
64	0.550463087	TaicangT_69:a5…	Dell_71:c5:de	ARP	60	Who has 192.168.1.3? Tell 192.168.1.1
65	0.550463118	Dell_71:c5:de	TaicangT_69:a5:10	ARP	60	192.168.1.3 is at 8c:ec:4b:71:c5:de
209	1.589157998	TaicangT_69:a5…	VMware_b2:bb:77	ARP	60	Who has 192.168.1.9? Tell 192.168.1.1
210	1.589181561	VMware_b2:bb:77	TaicangT_69:a5:10	ARP	42	192.168.1.9 is at 00:0c:29:b2:bb:77
228	1.974212283	VMware_b2:bb:77	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.9
229	1.974288490	VMware_b2:bb:77	Broadcast	ARP	42	Who has 192.168.1.2? Tell 192.168.1.9
230	1.974336247	VMware_b2:bb:77	Broadcast	ARP	42	Who has 192.168.1.3? Tell 192.168.1.9
231	1.974396043	VMware_b2:bb:77	Broadcast	ARP	42	Who has 192.168.1.4? Tell 192.168.1.9
232	1.974433312	VMware_b2:bb:77	Broadcast	ARP	42	Who has 192.168.1.5? Tell 192.168.1.9
233	1.974456184	Dell_71:c5:de	VMware_b2:bb:77	ARP	60	192.168.1.3 is at 8c:ec:4b:71:c5:de
234	1.974463392	VMware_b2:bb:77	Broadcast	ARP	42	Who has 192.168.1.6? Tell 192.168.1.9
235	1.974494541	VMware_b2:bb:77	Broadcast	ARP	42	Who has 192.168.1.7? Tell 192.168.1.9
236	1.974541930	VMware_b2:bb:77	Broadcast	ARP	42	Who has 192.168.1.8? Tell 192.168.1.9
237	1.974575204	VMware_b2:bb:77	Broadcast	ARP	42	Who has 192.168.1.10? Tell 192.168.1.9
238	1.974604998	VMware_b2:bb:77	Broadcast	ARP	42	Who has 192.168.1.112 Tell 192.168.1.9

```
▸ Frame 64: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, id 0
▸ Ethernet II, Src: TaicangT_69:a5:10 (18:45:93:69:a5:10), Dst: Dell_71:c5:de (8c:ec:4b:71:c5:de)
▸ Address Resolution Protocol (request)
```

nmap -sn 192.168.1.0/24 --packet-trace

```
root@kali:~# nmap -sn 192.168.1.0/24 --packet-trace
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-20 05:48 EST
SENT (0.0687s) ARP who-has 192.168.1.1 tell 192.168.1.9
SENT (0.0688s) ARP who-has 192.168.1.2 tell 192.168.1.9
SENT (0.0689s) ARP who-has 192.168.1.3 tell 192.168.1.9
SENT (0.0690s) ARP who-has 192.168.1.4 tell 192.168.1.9
SENT (0.0691s) ARP who-has 192.168.1.5 tell 192.168.1.9
SENT (0.0692s) ARP who-has 192.168.1.6 tell 192.168.1.9
SENT (0.0692s) ARP who-has 192.168.1.7 tell 192.168.1.9
SENT (0.0693s) ARP who-has 192.168.1.8 tell 192.168.1.9
SENT (0.0694s) ARP who-has 192.168.1.10 tell 192.168.1.9
SENT (0.0695s) ARP who-has 192.168.1.11 tell 192.168.1.9
RCVD (0.0690s) ARP reply 192.168.1.3 is-at 8C:EC:4B:71:C5:DE
RCVD (0.0699s) ARP reply 192.168.1.1 is-at 18:45:93:69:A5:10
SENT (0.0730s) ARP who-has 192.168.1.14 tell 192.168.1.9
SENT (0.0731s) ARP who-has 192.168.1.15 tell 192.168.1.9
SENT (0.0731s) ARP who-has 192.168.1.16 tell 192.168.1.9
SENT (0.0732s) ARP who-has 192.168.1.17 tell 192.168.1.9
RCVD (0.0791s) ARP reply 192.168.1.4 is-at 2A:84:98:9F:E5:5E
RCVD (0.0796s) ARP reply 192.168.1.5 is-at 30:24:32:1F:89:AC
SENT (0.0820s) ARP who-has 192.168.1.20 tell 192.168.1.9
SENT (0.0822s) ARP who-has 192.168.1.21 tell 192.168.1.9
SENT (0.0823s) ARP who-has 192.168.1.22 tell 192.168.1.9
SENT (0.0824s) ARP who-has 192.168.1.23 tell 192.168.1.9
SENT (0.1699s) ARP who-has 192.168.1.26 tell 192.168.1.9
SENT (0.1703s) ARP who-has 192.168.1.27 tell 192.168.1.9
SENT (0.1705s) ARP who-has 192.168.1.28 tell 192.168.1.9
```

- **بررسی ترافیک شبکه (Packet Analysis)**
- با **Wireshark** یا **tcpdump** باید دید دستگاه چه ترافیکی تولید می‌کند.
- مثال‌ها:
- **برای کشف MITM**
- اگر در Wireshark ببینند:

- ARP Reply
- 192.168.1.1 is-at 8c:85:90:12:44:af

- در حالی که MAC روتر چیز دیگری است →
- دستگاه دارد **ARP Spoofing** انجام می‌دهد.
- نتیجه:

- Risk = **Man-in-the-Middle Attack**

- **برای کشف DHCP Rogue**
- در Wireshark فیلتر:

- dhcp

- **اگر ببینند:**

- DHCP Offer
- Server Identifier: 192.168.1.77

- در حالی که DHCP اصلی شبکه چیز دیگری است →
- این دستگاه **Rogue DHCP Server** است.

- **برای کشف Sniffing**
- Snifferها معمولاً:
- ترافیک زیادی دریافت می‌کنند
- ARP broadcast زیاد می‌فرستند
- یا کارت شبکه در **promiscuous mode** است

- **نشانه‌ها:**
- ARP traffic زیاد
- Packet capture activity
- Network scanning

Rogue Device

- در یک **سازمان واقعی** وقتی می‌گوییم **Rogue Device** منظور هر **دستگاه ناآشنا، غیرثبت‌شده یا غیرمجاز** است که بدون اجازه وارد شبکه شود.
- این دستگاه *لزومی ندارد بدخواه باشد*؛ فقط چون ناشناس است، **ریسک ایجاد می‌کند.**

- **رایج‌ترین حالت.**
- **مثال:**
- یک کارمند لپ‌تاپ شخصی خود را به پورت LAN وصل کند.
- پیمانکار یا مهمان بدون هماهنگی وارد شبکه شود.

- **ریسک:**
- سیستم Patch نشده
- آنتی‌ویروس ندارد
- ممکن است Malware داشته باشد

- **این روزها بسیار رایج است:**
- **مثال:**
- دوربین IP
- پرینتر شبکه‌ای
- Smart TV
- دستگاه کارت‌خوان
- دستگاه سانترال VoIP

- **ریسک:**
- پورت‌های باز زیاد
- Patch نشدن
- امکان استراق سمع ترافیک

- در تحلیل **Data Exfiltration** ، **host** یعنی **همان دستگاهی که می‌خواهی رفتار آن را مانیتور کنی**؛ یعنی **Rogue Device**.

- در سناریوی **Data Exfiltration** هدف این نیست که رفتار شبکه را ببینی
- بلکه رفتار **یک دستگاه مشکوک** را بررسی کنی.

بررسی Data Exfiltration

- باید دید آیا دستگاه داده به بیرون می‌فرستد یا نه.
- **نشانه‌ها:**
- ارتباط زیاد با IP خارجی
- DNS request غیرعادی
- ارسال حجم زیاد داده

سناریوی پروژه سازمان

- **Kali =** سیستم مانیتورینگ

Rogue Device = ۱۹۲.۱۶۸.۱.۷۷

- 192.168.1.1 = **Router**
- 192.168.1.10 = **Domain DNS Server**

شناسایی ارتباطات خارجی (Baseline)

- **دیدن ارتباطات فعال دستگاه**
- **روی سیستم مانیتورینگ**
- tcpdump -i eth0 host 192.168.1.77 and not net 192.168.1.0/24
- اگر خروجی داشت یعنی دستگاه با **IPخارجی** صحبت می‌کند.
- **نمونه خروجی مشکوک:**
- 192.168.1.77.49832 > 45.67.89.10.443
- 192.168.1.77.49833 > 185.212.44.21.443

تحلیل حجم داده خروجی (Critical)

- **محاسبه حجم دیتای خروجی**
- tcpdump -i eth0 host 192.168.1.77 -w exfil.pcap
- **بعد از چند دقیقه:**
- capinfos exfil.pcap
- **نمونه خروجی :**
- **Data size: 580 MB**
- **Duration: 5 minutes**
- **تحلیل:**
- حجم بالا در زمان کوتاه
- غیرطبیعی برای یک دستگاه ناشناس

تشخیص روش‌های خاص Exfiltration

- **ICMP Exfiltration**
- tcpdump -i eth0 icmp and host 192.168.1.77
- **اگر ببینید:**
- **ICMP echo request (payload size: 1400 bytes)**

- **تحلیل:**
- Payload بزرگ
- تکرار بالا

- روی **Kali:**
- tcpdump -i eth0 port 53 and host 192.168.1.77
- **این یعنی:**
- همه DNS Query و Response که **Rogue Device (۱۹۲.۱۶۸.۱.۷۷)** می‌فرستد یا دریافت می‌کند را capture کن.

هدف Tiering Model چیست؟

- **هدف این مدل:**
- جلوگیری از **Lateral Movement**
- قطع کردن مسیرهای **Privilege Escalation**
- محدود کردن **دسترسی‌های Admin**
- جداسازی کامل سطوح **حیاتی، مهم و کاربری**

- **به زبان ساده:**
- هر کسی فقط باید روی **Tier خودش** مدیریت کند و نه روی **Tier** دیگر.

- **Tier0 (هسته امنیت و هویت)**
- **حیاتی‌ترین سطح امنیتی سازمان**
- **شامل چه چیزهایی؟**

- Domain Controllers
- Active Directory Forest/Domain
- PKI (Certificate Authority)
- ADFS / Azure AD Connect
- Identity Providers
- MFA servers
- Privileged Access Workstations (PAW)
- Root-level Security Services
- Backup servers

- **چه کسانی در این سطح فعالیت می‌کنند؟**

- Domain Admins
- Enterprise Admins
- PKI Admins
- Cybersecurity Root Admins

- **دسترسی این گروه چگونه باید باشد؟**
- فقط از طریق **سیستم‌های امن (PAW)**
- عدم استفاده برای کارهای روزمره
- بدون اتصال به اینترنت
- بدون دسترسی به Email
- MFA اجباری
- Session Recording فعال

- **Tier1 (سیستم‌های حیاتی ولی غیر هویتی)**
- سیستم‌هایی که سرویس‌های مهم را ارائه می‌کنند ولی جزو هسته AD نیستند.
- **شامل چه چیزهایی؟**

- Application Servers
- Database Servers
- Web Servers
- File Servers
- Hypervisors (VMware/Hyper-V)
- Monitoring Servers (اگر دسترسی دامین ادمین را ندارند)
- Network Attached Storage

- **چه کسانی در این سطح کار می‌کنند؟**

- Server Admins
- App Admins
- DB Admins
- Virtualization Admins

- **محدودیت‌ها**
- Adminهای 1Tier **نباید وارد 0Tier شوند**
- نباید بتوانند DC را مدیریت کنند
- نباید روی Domain Admin تاثیر بگذارند
- **مثال تخلف مهم**
- اگر Admin یک Web Server بتواند از طریق Credential Dumping به Domain Admin برسد → Tiering Model شکست خورده.

- **Tier 2 (Clients & User Environment)**

- **پایین‌ترین سطح امنیتی**

- **شامل چه چیزهایی؟**

- User Workstations
- Laptops
- VDI
- Printers
- User Accounts
- Helpdesk Operations

- **چه کسانی این سطح را مدیریت می‌کنند؟**

- Helpdesk
- Desktop Support
- IT Support Level 1 & 2

- **محدودیت‌ها**

- Local Admin بودن روی کلاینت‌ها **نباید** امکان Escalation بدهد
- باید ابزارهای محدودتر و اکانت‌های محدودتر استفاده کنند

قوانین طلایی Tiering Model (بسیار مهم)

- **قانون ۱: یک ادمین فقط می‌تواند روی Tier خودش مدیریت کند**
- Tier0 Admin فقط مدیریت → Tier0
- Tier1 Admin فقط مدیریت → Tier1
- Tier2 Admin فقط مدیریت → Tier2
- ✕ Domain Admin نباید برای نصب نرم‌افزار روی یک Client وارد شود
- ✕ Server Admin نباید وارد DC شود
- ✕ Helpdesk نباید دسترسی به Server داشته باشد

- **قانون ۲: دستگاهی که به Tier پایین‌تر آلوده شود، حق اتصال به Tier بالاتر ندارد**
- یعنی اگر یک Admin در Tire1روی Workstation ناامن لاگین کند، نباید بتواند به Tire0وصل شود.

- **قانون 3: دستگاه‌های Tier0 باید از سایر Tierها جدا شوند**
- **جداسازی از طریق:**

- VLAN
- Firewall ACL
- Jump Servers
- PAW
- RDP Restriction
- Credential Guard

پروفایل‌های پیکربندی امن سرور به صورت زیرتعریف می‌گردد:

- Level1 – Domain Controller
  - موارد موجود در این پروفایل به دامین کنترلر اعمال می‌شوند.

- Level1 – Member Server
  - موارد موجود در این پروفایل به Member Serverها اعمال می‌شوند.

- مواردی که در این پروفایل به Member Serverهایی که Roleهای زیر بر روی آن‌ها فعال هست نیز اعمال می‌گردد:

- AD Certificate Services
- DHCP Server
- DNS Server
- File Server
- Hyper-V
- Network Policy and Access Services
- Print Server
- Remote Access Services
- Remote Desktop Services
- Web Server

- اطمینان از تنظیم Enforce password historyبه تعداد ۲۴ یا بیشتر
- پروفایل قابل اجرا:

- Level 1 – Domain Controller
- Level 1 – Member Server

- این Policyمربوط به تنظیم تعداد کلمات عبور منحصر به فردی و جدیدی است که کاربر می تواند برای خود انتخاب نماید. هنگامی که کلمه عبور کاربر منقضی می گردد، وی باید اقدام به تغییر کلمه عبور خود نماید و تعداد مشخص شده در این Policy، تعیین می کند که چه تعداد از کلمات عبور انتخاب شده توسط کاربر در سرور ذخیره شده و دیگر نمی تواند از این کلمات عبور استفاده نماید.

- مقداری که شما باید برای Enforce password historyتعریف نمایید، بین صفر تا ۲۴ می باشد. به عنوان مثال، برای یک دامین کنترلر تعداد ۲۴ کلمه عبور است.

Local Group Policy Editor

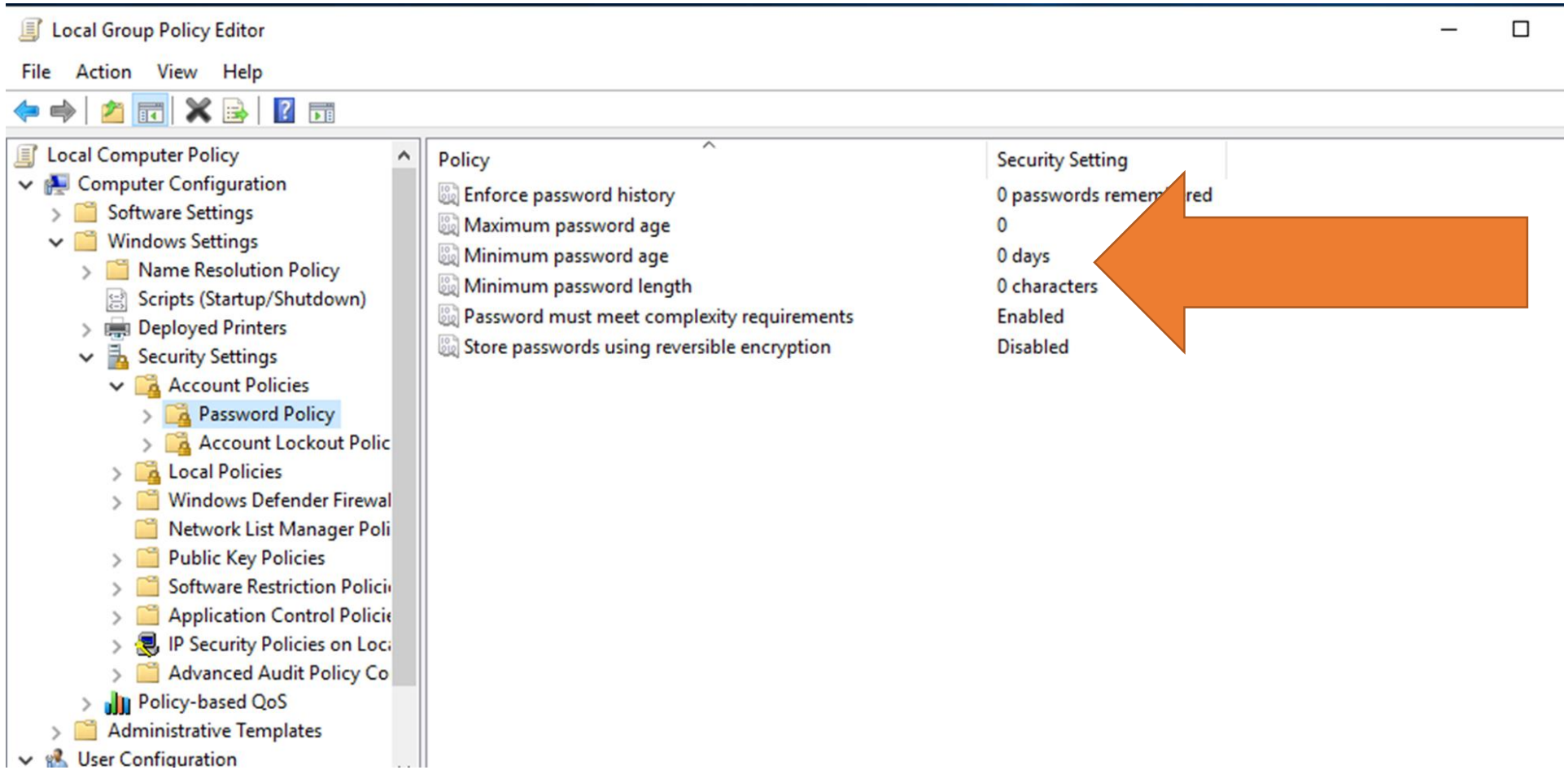
File Action View Help

- Local Computer Policy
  - Computer Configuration
    - Software Settings
    - Windows Settings
      - Name Resolution Policy
      - Scripts (Startup/Shutdown)
      - Deployed Printers
      - Security Settings
        - Account Policies
          - Password Policy
          - Account Lockout Polic
        - Local Policies
        - Windows Defender Firewal
        - Network List Manager Poli
        - Public Key Policies
        - Software Restriction Polici
        - Application Control Policie
        - IP Security Policies on Loc
        - Advanced Audit Policy Co
      - Policy-based QoS
    - Administrative Templates
  - User Configuration

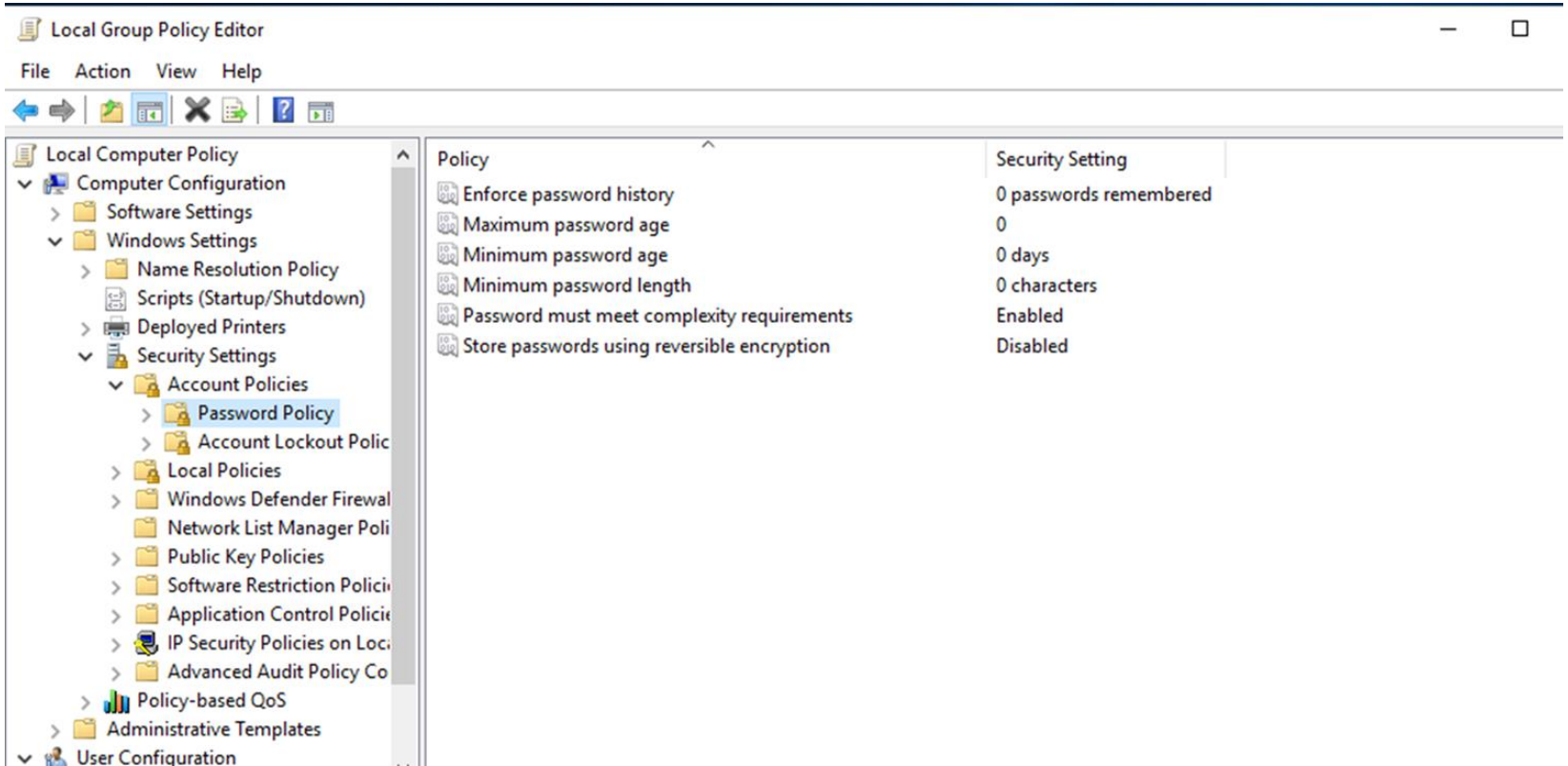
Policy	Security Setting
Enforce password history	0 passwords remembered
Maximum password age	0
Minimum password age	0 days
Minimum password length	0 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

- برای حفظ اثربخشی این Policy، از تنظیمات مربوط به Minimum Password Age استفاده کنید تا از تغییر مکرر رمز عبور کاربران جلوگیری به عمل آید.

- حالت پیشنهادی برای این Policy مقدار ۲۴ یا بیشتر می باشد.

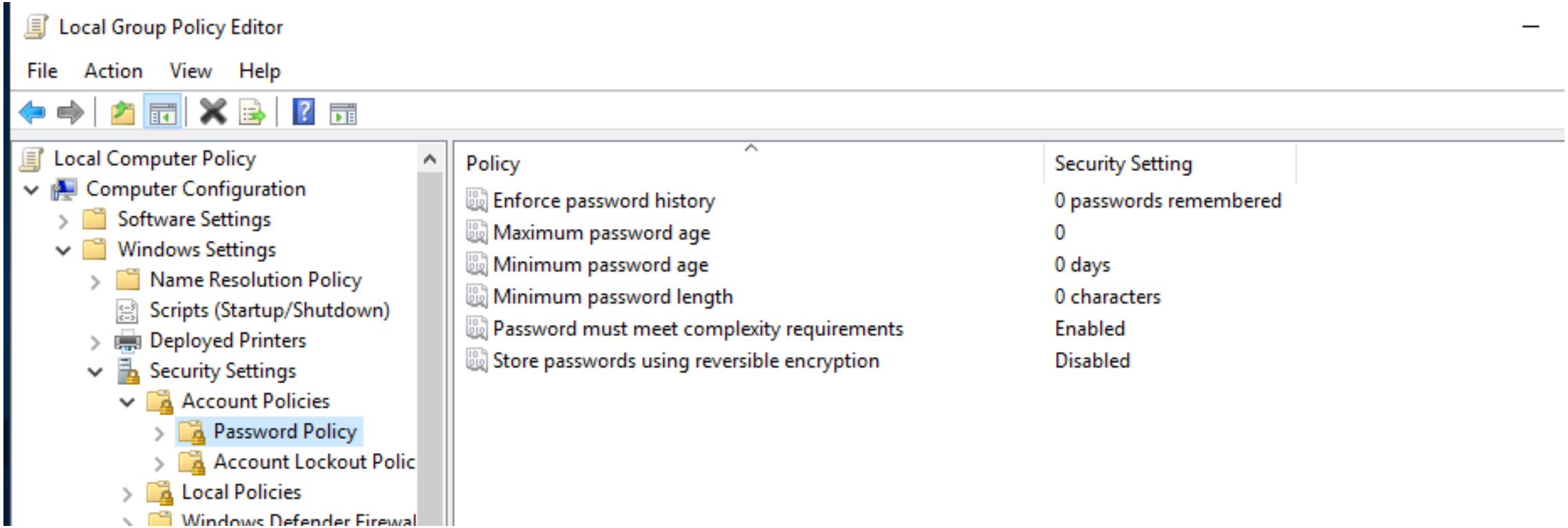


- Rationale
- **در صورتی که یک رمز عبور به مدت زیادی تغییر نکرده** باشد، احتمال موفقیت آمیز بودن حملات Brute Forceعلیه آن توسط نفوذگران که دانش اولیه ای در مورد کاربران دارند، افزایش می یابد.
- در صورتی که مقدار تنظیم شده در در این بخش برابر با صفر باشد، کاربران دیگر نیازی به تغییر کلمات عبور خود نخواهند داشت و این یک ریسک امنیتی مهم می باشد.
- بدین صورت اگر رمز عبور یکی از کاربران به خطر بیافتد، دسترسی کاربر مخرب به این حساب تا زمانی که کلمه عبور آن تغییر نکند، امکان پذیر خواهد بود.



- Remediation
- برای انجام پیکربندی توصیه شده به مسیر زیر از طریق Group Policyرفته و مقدار 60 یا کمتر (صفر نباشد)را برای آن تنظیم نمایید:

- Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Maximum password age



- Impact

- اگر مقدار Maximum Password Age خیلی کم باشد، کاربران لازم است تا در بازه های زمانی کوتاه کلمات عبور خود را تغییر دهند. چنین کاری می تواند امنیت سازمان را کاهش دهد، زیرا کاربران ممکن است کلمات عبور خود را در یک مکان نام یاد داشت نموده و یا آن را گم کنند.

- همچنین اگر مقدار این تنظیم شده در این Policy خیلی زیاد باشد، باز هم منجر به کاهش سطح امنیتی سازمان خواهد شد، زیرا به نفوذگران بالقوه این اجازه را می دهد تا زمان بیشتری را برای شکستن کلمات عبور در اختیار داشته باشند.

اطمینان از تنظیم Minimum password age به عدد یک یا بیشتر

- پروفایل قابل اجرا:

- Level 1 – Domain Controller
- Level 1 – Member Server

- توضیحات:
- تنظیمات این Policy تعریف می کند که کاربران، پس از حداقل چند روز می توانند کلمه عبور خود را تغییر دهند. بازه ای که می توانید در این Policy تنظیم نمایید بین یک تا ۹۹۹ روز می باشد. (شما ممکن است مقدار صفر را برای این Policy تنظیم کرده باشید تا کاربران بلافاصله بتوانند رمز عبور خود را تغییر دهند.) مقدار پیش فرض برای این Policy برابر با صفر می باشد.

- مقداری که برای این Policy توصیه می گردد، عدد ۱ یا بیشتر می باشد.

Local Group Policy Editor

File Action View Help

- Local Computer Policy
  - Computer Configuration
    - Software Settings
    - Windows Settings
      - Name Resolution Policy
      - Scripts (Startup/Shutdown)
      - Deployed Printers
      - Security Settings
        - Account Policies
          - Password Policy
          - Account Lockout Polic
        - Local Policies
        - Windows Defender Firewal

Policy	Security Setting
Enforce password history	0 passwords remembered
Maximum password age	0
Minimum password age	0 days
Minimum password length	0 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

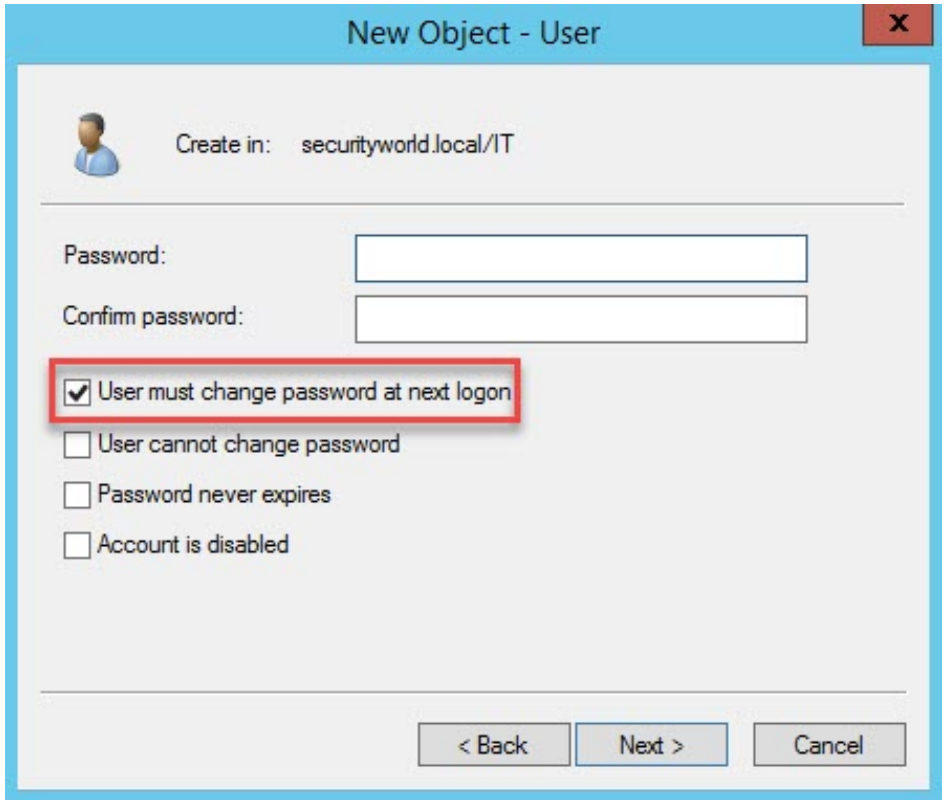
- استفاده از Policyمربوط به Enforce Password History، از انتخاب کلمه عبور قدیمی که توسط کاربر استفاده شده است، جلوگیری به عمل می آورد. البته در تنظیم این Policyباید دقت نمایید.

- به عنوان مثال اگر مقدار Policyمربوط به Enforce Password Historyرا برابر **۱۲** قرار داده باشید، تا اطمینان حاصل نمایید که کاربران نمی توانند از ۱۲ رمز عبور آخر خود استفاده نمایند، کاربر می تواند در عرض چند دقیقه ۱۳ بار رمز عبور خود را تغییر داده و رمز عبوری که پیش از این استفاده می کرده است را مجدداً انتخاب نماید.

- البته این موضوع در صورتی عملی خواهد بود که شما مقدار Policyمربوط به Minimum Password Ageرا برابر با صفر تنظیم کرده باشید که به صورت پیش فرض نیز، تنظیمات این Policyهمین عدد می باشد.

- به منظور پیشگیری از چنین مشکلی و تاثیر Policyمربوط به Enforce Password History، می بایست مقدار Minimum Password Ageرا به عدد یک یا بیشتر از آن تغییر دهید.

- در صورتی که ادمین، یک رمز عبور را برای کاربری تنظیم نموده باشد و قصد داشته باشد تا کاربر پس از اولین ورود، رمز عبور خود را تغییر دهد، باید گزینه User must change password at next logonرا هنگام تعریف رمز عبور کاربر، انتخاب نماید.
- بدین شکل کاربر، پس از تغییر رمز عبور خود، در صورتی که عدد یک برای Policyمربوط به Minimum Password Age، تنظیم شده باشد، امکان تغییر رمز عبور خود تا روز بعد را نخواهد داشت.



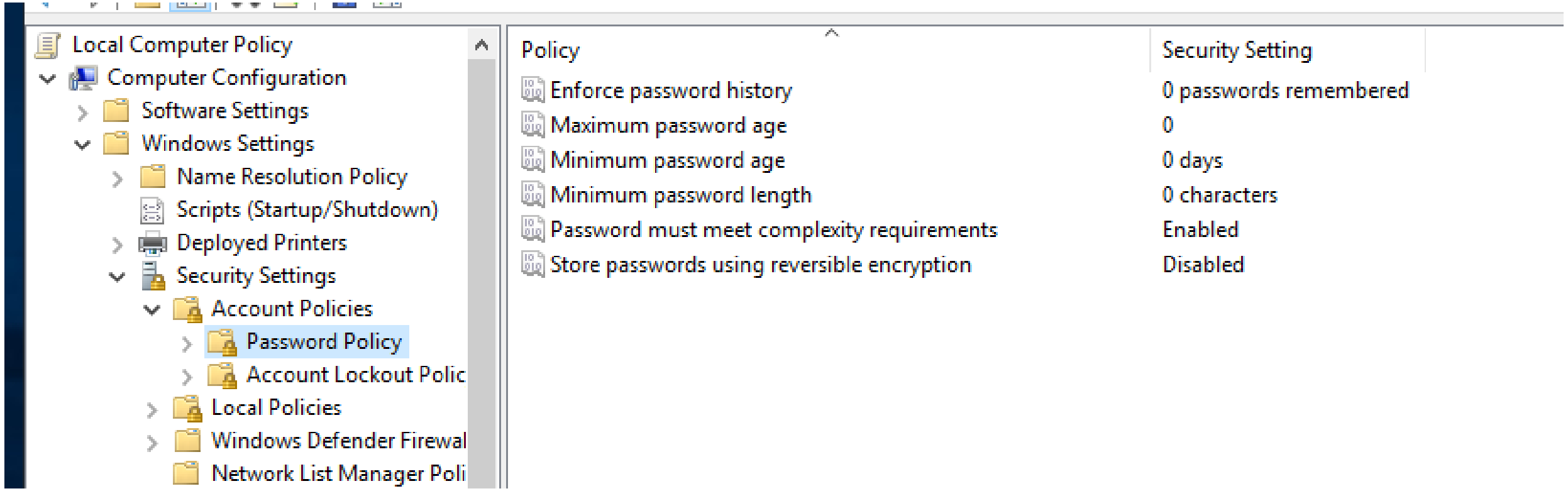
اطمینان از تنظیم Minimum password length به عدد 14 یا بیشتر

- پروفایل قابل اجرا:

- Level 1 – Domain Controller
- Level 1 – Member Server

- توضیحات:
- تنظیمات Policy مربوط به Minimum password length تعریف می کند که حداقل تعداد کاراکترهایی که کاربران می توانند برای رمز عبور خود انتخاب نمایند، چه تعداد است. تئوری های مختلف و زیادی در مورد چگونگی تعیین مناسب ترین طول کاراکتر برای یک سازمان وجود دارد.

- در محیط های سازمانی، مقدار ایده آل برای Policyمربوط به Minimum password length، مقدار ۱۴ کاراکتر می باشد، با این حال شما باید این مقدار را متناسب با محیط کسب و کار یا سازمان خود تنظیم نمایید.
- مقداری که برای این Policyتوصیه می گردد، عدد ۱۴ یا بیشتر می باشد.



اطمینان از فعال بودن مقدار
Password must meet complexity requirements – Scored

- تنظیمات این Policyکنترل می کند که کلیه کلمات عبور جدیدی که تنظیم می شوند، دارای پیچیدگی لازم باشند. در صورتی که این Policyفعال باشد، کلمه عبور انتخابی کاربر باید حداقل شرایط لازم را دارا باشد که این شرایط شامل موارد زیر می باشند:

- نباید شامل نام کاربری یا بخشی از نام کاربر (Full Name)که دو کاراکتر آن پشت سر هم باشد.
- حداقل دارای ۶ کاراکتر باشد.

- اضافه نمودن هر کاراکتر به رمز عبور، میزان پیچیدگی آن را به صورت تصاعدی افزایش می دهد. به عنوان مثال کلمه عبوری با هفت کاراکتر که در آن از حروف کوچک استفاده شده است، حدود ۸ میلیارد کلمه عبور مختلف را شامل می شود.

- علاوه بر این، استفاده از ترکیب کلید ALTبا اعداد نیز می تواند پیچیدگی یک رمز عبور را تا حد زیادی بالا ببرد.
- با این وجود، چنین الزامات سخت گیرانه ای می تواند منجر به نارضایتی کاربران شده و افزایش حجم کار بخش پشتیبانی را نیز به همراه داشته باشد.

- از سویی دیگر، سازمان شما می تواند، استفاده از علامت های تولید شده توسط نگه داشتن کلید ALTو فشردن اعداد ۰۱۲۸ تا ۰۱۵۹ را برای کلمات عبور تمامی Administratorها الزامی نماید.

- (کاراکترهای خارج از این محدود مربوط به حروف الفبای استاندارد بوده و باعث پیچیدگی در کلمات عبور نخواهند شد.)

اطمینان از تنظیم Account lockout duration به ۱۵ دقیقه یا بیشتر

- پروفایل قابل اجرا:

- Level 1 – Domain Controller
- Level 1 – Member Server

- تنظیمات Policy مربوط Account lockout duration به مدت زمانی که باید از مسدود شدن حساب کاربری بگذرد تا این حساب مجدد فعال شود را تعیین می کند.
- مقدار تعیین شده برای این Policy بر اساس دقیقه می باشد. در صورتی که شما مقدار صفر را برای این Policy تنظیم نمایید، حساب کاربری تا زمانی که مدیر شبکه به صورت دستی آن را فعال ننماید، مسدود خواهد بود.

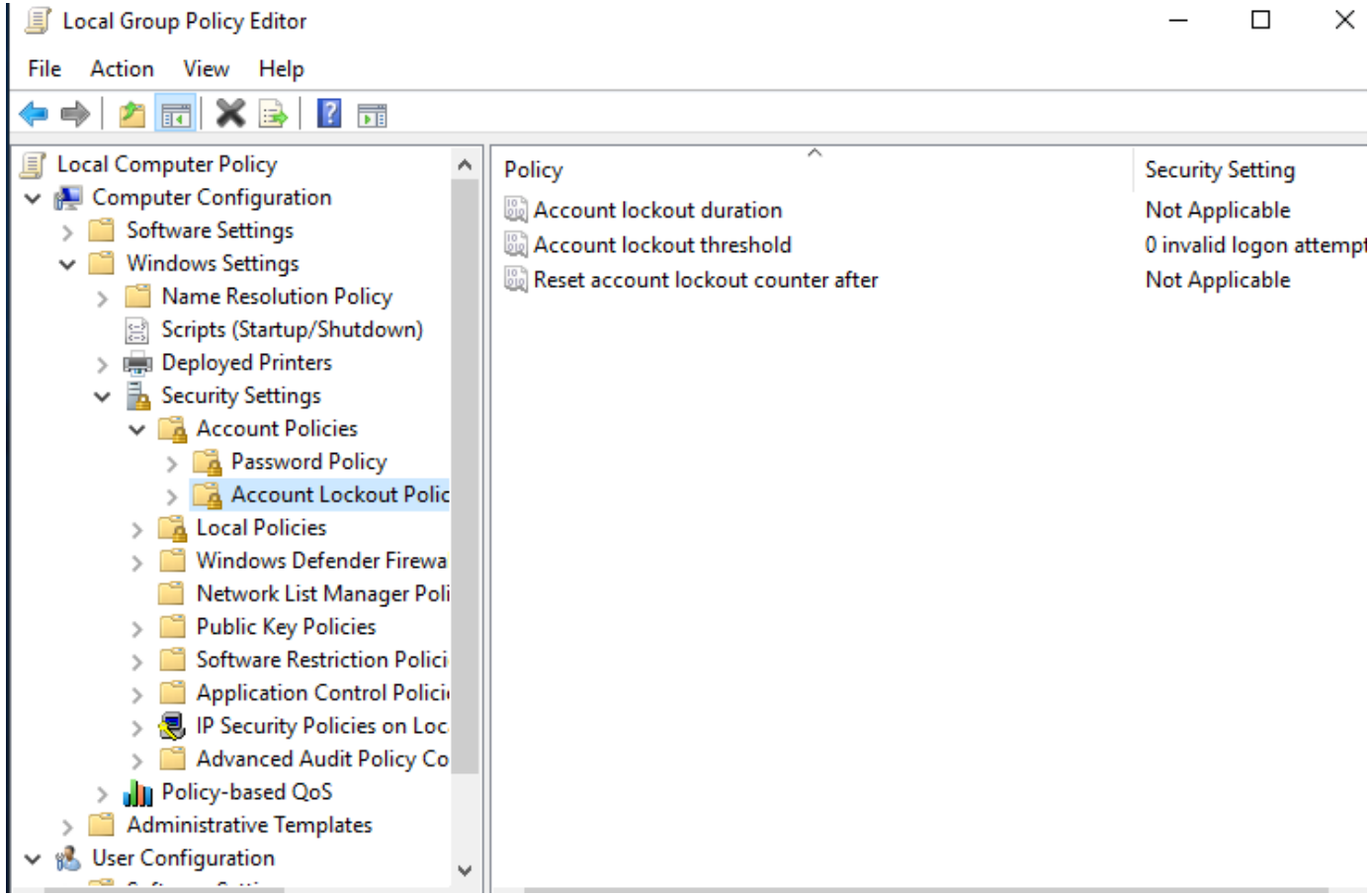
- اگر چه ممکن است پیکربندی این Policy ایده خوبی به نظر برسد، به هر ترتیب، تنظیم آن، به احتمال زیاد تماس با بخش Help Desk را افزایش خواهد داد.
- کاربران باید از مدت زمانی که حساب کاربری آن ها در صورت ورود کلمات عبور نادرست مسدود می ماند، اطلاع داشته باشند تا در صورت نیاز به دسترسی سریع به حساب کاربری خود، به بخش Help Desk تماس حاصل نمایند.

Local Group Policy Editor

File Action View Help

- Local Computer Policy
  - Computer Configuration
    - Software Settings
    - Windows Settings
      - Name Resolution Policy
      - Scripts (Startup/Shutdown)
      - Deployed Printers
      - Security Settings
        - Account Policies
          - Password Policy
          - Account Lockout Polic
        - Local Policies
        - Windows Defender Firewa
        - Network List Manager Poli
        - Public Key Policies
        - Software Restriction Polici
        - Application Control Polici
        - IP Security Policies on Loc
        - Advanced Audit Policy Co
      - Policy-based QoS
    - Administrative Templates
  - User Configuration

Policy	Security Setting
Account lockout duration	Not Applicable
Account lockout threshold	0 invalid logon attempts
Reset account lockout counter after	Not Applicable

- یک مهاجم می تواند با سوء استفاده از آستانه بسته شدن حساب کاربری، اقدام به تلاش برای ورود به یک حساب کاربری خاص با کلمات عبور نادرست نماید. این امر در واقع منجر به یک حمله انکار سرویس یا DoSمی شود.

- تنظیم این Policyوابسته به تنظیم Policyمربوط به Account Lockout Thresholdمی باشد، در صورتی که مقدار این Policyرا برابر با صفر قرار دهید، حساب کابری تا زمانی که مدیر شبکه به صورت دستی آن را فعال ننماید، مسدود خواهد بود.