چک لیست پروژه محور Hardening VMware ESXi

- **تنظیم Syslog**
- **هدف**
- ارسال لاگ‌ها به Syslogمرکزی برای حفظ رویدادها و امکان تحلیل امنیتی.
- **تهدید**
- اگر لاگ‌ها فقط روی خود ESXiذخیره شوند، در صورت خرابی Hostیا دستکاری توسط مهاجم، شواهد از بین می‌روند.

- Host
- ↓
- Manage
- ↓
- System
- ↓
- Advanced Settings

- جستجو کنید
- Syslog.global.logHost
- مقدار را وارد کنید.
- مثلاً

- udp://192.168.10.50:514
- tcp://192.168.10.50:514

- سپس
- Host
- ↓
- Actions
- ↓
- Refresh System Configuration

- **فعال‌سازی CHAP دوطرفه برای iSCSI**
- **کنترل:** آیا احراز هویت بین Target iSCSI و Host iSCSI به صورت CHAP دوطرفه فعال شده است؟
- **مسیر گرافیکی**

1.وارد **Host Client** شوید

2.بروید به:**Host**

3.سپس:**Manage**

4.بعد:**Storage**

5.وارد:**Storage Adapters**

6.آداپتور iSCSI را انتخاب کنیدمثلا:

- iSCSI Software Adapter

- روی **Edit Settings** یا **Properties** کلیک کنید
- در بخش **Authentication** یا **CHAP:**
- **CHAP** را فعال کنید
- در صورت نیاز **Bidirectional CHAP** را نیز فعال کنید
- Username / Secret را تنظیم کنید

- **مسیر معمول در vCenter**
- اگر با **vCenter** کار می‌کنی:

1. **Hosts and Clusters**
2. انتخاب Host
3. تب **Configure**
4. بخش **Storage**
5. **Storage Adapters**
6. انتخاب iSCSI Adapter
7. **Edit**
8. قسمت **CHAP Authentication**

- **نکات هاردنینگ**
- Secret باید قوی و غیرتکراری باشد
- در صورت عدم نیاز، iSCSI را غیرفعال نگه دارید
- فقط Targetهای مجاز به Host معرفی شوند

تعیین Timeout برای SSH و Shell بیکار

کنترل :آیا برای خاتمه دادن ارتباط بیکار SSH و Shell زمان تعیین شده است؟

- **مقدار پیش‌فرض:** ۰
- **مقدار پیشنهادی:** ۹۰۰

یعنی اگر ۱۵ دقیقه فعالیتی نباشد، سشن بسته شود.

مسیر درHost Client

1.وارد **ESXi Host Client** شوید

2.بروید به:**Host**

3.سپس:**Manage**

4.بعد:**System**

5.وارد:**Advanced Settings**

جستجوی پارامتر

در قسمتSearch ، این کلید را پیدا کنید:

- UserVars.ESXiShellInteractiveTimeOut

مقداردهی

مقدار را روی:

- 900

قرار دهید.

- **تنظیمات فایروال ESXi**
- **مسیر گرافیکی**

1.وارد **Host Client** شوید

2.بروید به:**Host**

3.سپس:**Manage**

4.بعد:**Networking**

5.وارد:**Firewall rules**یا**Firewall**

6.Ruleهای مورد نیاز را بررسی کنید

7.فقط سرویس‌های لازم را **Enable** نگه دارید

8.برای سرویس‌های مدیریتی، در صورت وجود، **Allowed IPs** را محدود کنید

- **اصول هاردنینگ**
- فقط پورت‌های ضروری باز باشند
- SSH، CIM، vSphere Web Access و سرویس‌های مشابه فقط در صورت نیاز فعال شوند
- IP Management Console محدود شود
- Ruleهای غیرضروری Disable شوند

Account Lock Failures

- Host Client
- → Manage
- → System
- → Advanced Settings
- → Security.AccountLockFailures
- مقدار
- 5

Password History

- Host Client
- → Manage
- → System
- → Advanced Settings
- → Security.PasswordHistory

- Target : 5

آیا پالیسی برای پیچیدگی رمز عبور کاربر تعیین شده است؟

- استفاده از Policy Passwordاز جمله استفاده از کلمات عبور با طول زیاد و استفاده از کاراکترهای ویژه جهت افزایش امنیت رمز عبور ضروری است .

- همچنین توصیه میشود از کلمه عبور rootاستفاده نشود

- Host Client
- → Manage
- → System
- → Advanced Settings
- → Security.PasswordQualityControl

DCUI Timeout

- Host Client
- → Manage
- → System
- → Advanced Settings
- → UserVars.DcuiTimeOut

- 600 seconds

آیا احراز هویت کاربران اکتیودایرکتوری از طریق Proxy Authenticationفعال شده است؟

- چنانچه سرور ESXi به اکتیو دایرکتوری جوین شود، نام کاربری و رمز عبور کاربران در قسمت Profile Host سرور ESXiذخیره می گردد.

- جهت جلوگیری از دخیره سازی نام کاربری و رمز عبور می توان از قابلیت Proxy Authenticationاستفاده کرد

- **Host → Manage → System → Advanced Settings**
- در قسمت Search، عبارت مربوط به **Proxy Authentication / Authentication Proxy** را جست‌وجو کنید.
- اگر تنظیم مربوطه فعال باشد، وضعیت آن باید در Advanced Settings مشخص شود.

در Search این عبارت‌ها را بررسی کنید:

- Config.HostAgent.plugins.hostsvc.esxAdminsGroup
- Config.HostAgent.plugins.hostsvc.esxAdminsGroupAutoAdd

- تنظیمات مرتبط با Authentication / Proxy

- اما برای احراز هویت واقعی AD، مسیر اصلی این است:
- **Host Client → Manage → Security & Users → Authentication**
- در این قسمت باید وضعیت **Active Directory**را ببینید.

- اگر به صورت :
- Domain: - Status: Not Joined
- باشد، احراز هویت مستقیم کاربران ADبرای ESXiبرقرار نیست.

- گروه ESXi Admins
- در Active Directoryاستفاده شود و دسترسی مدیریتی ESXiبه آن گروه اختصاص پیدا کند.

آیا سرور ESXIبه دامین جوین شده است ؟

- با جوین کردن سرور ESXiبه اکتیو دایرکتوری میتوان اطمینان داشت که یکسری پالیسی ها از جمله Policy Passwordاز سمت اکتیودایرکتوری الزامی است.

- پیشنهاد میشود یک گروه به نام Admins ESXدر اکتیودایرکتوری ایجاد و مجوز مدیریت ESXiبه این گروه اعطا گردد

آیا ویژگی MOB غیرفعال شده است ؟ MOB (Managed Object Browser)

- MOB یک اپلیکیشن تحت وب است که از طریق ESXi و vcenter قابل دسترس است و یکسری اطالعات اضافی و جزییات روی VMها و Datastore و Pool Resourceها را ارایه می دهد.

- **چرا مهم است؟**
- MOBیک رابط مدیریتی برای مشاهده و تعامل با **Managed Objects** مربوط به Host/VMwareاست.

- فعال بودن آن، سطح دسترسی و سطح حمله Management Interface را افزایش می‌دهد؛ بنابراین در یک پروژه Hardeningمعمولاً در صورت عدم نیاز باید غیرفعال باشد.

- Host → Manage
- System → Advanced Settings

در قسمت Search عبارت زیر را جستجو کنید:

Config.HostAgent.plugins.solo.enableMob

اگر مقدار فعلی **True** است:

روی Setting کلیک کنید → Edit → مقدار را False قرار دهیدSave → Verify

بعد از Save مجدداً همان Setting را باز کنید و مطمئن شوید:

Config.HostAgent.plugins.solo.enableMob = False

آیا سرویس SLPغیرفعال شده است ؟
SLP (Service Location Protocol)

- سرویس SLPترافیک ورودی شبکه را بدون احراز هویت و با دسترسی Rootبررسی و مورد تجزیه و تحلیل قرار میدهد که باعث می شود هدف مناسبی برای سو استفاده و حمله باشد و بایستی غیرفعال گردد

- Host → Manage → System → Services

- Slpd
- SLP / Service Location Protocol

- **اگر سرویس فعال باشد**
- اگر وضعیت آن مثلاً:
- **Running**
- باشد:

1.سرویس **slpd**را انتخاب کنید.

2.روی **Actions**کلیک کنید.

3. Stopرا بزنید.

4.سپس **Edit startup policy**را باز کنید.

5. Startup Policyرا روی:

- **Start and stop manually**
- قرار دهید.

آیا پروتکل SNMP غیر فعال شده است ؟

- پروتکل SNMP بمنظور مانیتورینگ منابع سرور مورد استفاده قرار میگیرد که اگر استفاده نمیشود بایستی غیرفعال گردد.

سپس:

Host → Manage → System → Services

در لیست سرویس‌ها دنبال:

snmpd

بگردید.

اگر وضعیت سرویس:

Running

است:

1. snmpdرا انتخاب کنید .
2. **Actions**
3. **Stop**

سپس Startup Policy را بررسی کنید:

Actions → Edit startup policy

و آن را طوری تنظیم کنید که SNMP هنگام راه‌اندازی Host به‌صورت خودکار اجرا نشود؛

Off / Disabled

⚠نکته مهم پروژه

قبل از Stop کردن snmpd حتماً بررسی کنید آیا **vCenter** ، **Zabbix**، **PRTG**، **SolarWinds** یا **NMS سازمان** از SNMP برای مانیتورینگ ESXi استفاده می‌کند یا خیر.

اگر SNMP واقعاً استفاده نمی‌شود:

PASS → SNMP Disabled

لیست کاربرانی که می توانند در حالت Down Lockبه ESXiمتصل شوند خالی است ؟

- لیست کاربران جهت دسترسی به mode down Lockedبایستی خالی باشد. کاربر Rootرا نمیتوان از این لیست حذف کرد

- Host → Manage → Security & Users
- سپس بخش مربوط به:
- **Lockdown Mode / Users / Exception Users**
- را بررسی کنید.

- در ESXi 7 ممکن است این بخش را از مسیر:
- **Host → Manage → Security & Users → Lockdown Mode**
- ببینید.

- **چه چیزی باید بررسی شود؟**
- در حالت **Normal Lockdown Mode**، کاربران موجود در **Exception Users** می‌توانند در شرایط خاص مستقیماً به ESXi Host دسترسی داشته باشند.
- بنابراین برای کنترل چک‌لیست:
- **Exception Users / Users allowed to access the host directly**
- باید:
- **خالی باشد** ✅

- **چرا مهم است؟**
- هدف Lockdown Mode این است که مدیریت ESXiتا حد امکان از طریق **vCenter**انجام شود و کاربر نتواند کنترل‌های vCenterرا با اتصال مستقیم به Hostدور بزند.

- ⚠ **اما یک نکته بسیار مهم**
- **قبل از فعال کردن Lockdown Mode، این لیست را خالی نکنید.**
- ابتدا باید مطمئن شوید:
- vCenterبه Hostدسترسی دارد.
- حساب مدیریتی vCenterسالم است.
- دسترسی اضطراری/ DCUIبررسی شده.
- هیچ ابزار Backup/Monitoring/Managementبه حساب مستقیم ESXiوابسته نیست.

- **در غیر این صورت ممکن است بعد از فعال‌کردن Lockdown، دسترسی مدیریتی خودتان به Hostرا از دست بدهید.**

- **آیا محل ذخیره سازی الگها در یک حافظه دایمی پیکربندی شده است ؟**

- به طور پیش فرض ، ESXi لاگها را در حافظه نگهداری می کند که با ریبوت کردن سرور، لاگ ها حذف خواهد شد. توصیه می شود محل ذخیره سازی الگ ها به یک حافظه دایمی تغییر نماید

- با ارسال لاگ ها به یک لاگ سرور متمرکز ، امکان تجمیع و پیداکردن وابستگی بین لاگ ها وجود دارد و در صورت وقوع رخدادهای مشکوک و یا حمله ، امکان کشف و تشخیص آن وجود دارد

- آیا نسخه **ESXI** به روز میباشد؟
- به منظور رفع آسیب پذیری ها، توصیه اکید می شود آخرین وصله های امنیتی روی سرور ESXI نصب گردد .

- آیا قابلیت TPS محدود شده است ؟
- TPS (Transparent Page Sharing)

- TPS مکانیزمی است که توسط VMkernel بمنظور استفاده بهینه از حافظه رم بکار گرفته می شود که در آن Pageهای یکسان بین VMها فقط یکبار ذخیره میشوند.

- ولی به دلایلی امنیتی توصیه میشود جهت جلوگیری از دسترسی VMها به اطالعات همدیگر این قابلیت بر روی VMها محدود گردد

- در **ESXi Host Client** وارد شوید:
- **Host → Manage → System → Advanced Settings**
- در قسمت Search عبارت زیر را جستجو کنید:
- Mem.ShareForceSalting

مقدار مطلوب

برای: Hardening

Mem.ShareForceSalting = 2

اگر مقدار فعلی 2 باشد:

PASS — TPS ✅محدود شده است

اگر مقدار 0 یا مقدار دیگری باشد:

FAIL / ⚠نیازمند بررسی و اصلاح

نحوه تغییر

اگر مقدار 2 نیست:

Advanced Settings → Mem.ShareForceSalting → Edit

سپس:

Value: 2

↓

Save

مفهوم امنیتی

هدف این تنظیم این است که اشتراک‌گذاری صفحات حافظه (TPS) بین VMها محدود شود تا یک VM نتواند از طریق رفتارهای مربوط به اشتراک حافظه، اطلاعاتی درباره VM دیگر به‌دست آورد.