چک لیست پروژه محور Hardening VMware ESXi

چرا امن‌سازی VMware ESXi اهمیت حیاتی دارد؟

- در سال‌های اخیر، مجازی‌سازی به ستون فقرات زیرساخت فناوری اطلاعات سازمان‌ها تبدیل شده است. امروزه ده‌ها یا حتی صدها سرور فیزیکی در قالب ماشین‌های مجازی روی یک یا چند میزبان **VMware ESXi** اجرا می‌شوند.

- این معماری اگرچه باعث کاهش هزینه، افزایش بهره‌وری و ساده‌سازی مدیریت زیرساخت شده است، اما در صورت عدم رعایت اصول امنیتی، یک نقطه شکست بحرانی (Single Point of Failure) ایجاد می‌کند.

- برخلاف یک سرور معمولی، نفوذ به یک Host ESXi می‌تواند به معنای دسترسی مهاجم به تمام ماشین‌های مجازی، سرویس‌های حیاتی، پایگاه‌های داده، فایل‌های سازمانی و حتی سامانه‌های پشتیبان باشد. به همین دلیل، ESXi یکی از جذاب‌ترین اهداف مهاجمان سایبری، گروه‌های باج‌افزاری و تهدیدهای پیشرفته (APT) است.

- امن‌سازی (Hardening) سرور ESXi، مجموعه‌ای از اقدامات فنی و مدیریتی است که با کاهش سطح حمله (Attack Surface)، محدودسازی دسترسی‌ها، حذف سرویس‌های غیرضروری و اعمال تنظیمات امنیتی استاندارد، احتمال موفقیت حملات را به حداقل می‌رساند.

مهم‌ترین تهدیدات علیه سرورهای VMware ESXi

- حملات باج‌افزاری (Ransomware)
- مهم‌ترین تهدید علیه ESXi، باج‌افزارها هستند. برخلاف حمله به یک سرور ویندوز، مهاجم پس از نفوذ به ESXiمی‌تواند تنها در چند دقیقه فایل‌های ماشین‌های مجازی (VMDK)، فایل‌های پیکربندی (VMX)و Snapshotها را رمزگذاری کند و هم‌زمان ده‌ها سرویس سازمان را از دسترس خارج سازد.
- **پیامدها:**
- توقف کامل سرویس‌های سازمان
- از دسترس خارج شدن دیتابیس‌ها
- از بین رفتن Snapshotها
- خسارت مالی و اعتباری

- **نمونه‌های شناخته‌شده:**
- ESXiArgs
- LockBit
- BlackCat (ALPHV)
- Akira
- Babuk
- HelloKitty

- **سرقت اطلاعات مدیریتی (Credential Theft)**
- مهاجمان معمولاً با روش‌هایی مانند Phishing، Keyloggerیا Password Spraying، اطلاعات ورود مدیران VMwareرا سرقت می‌کنند.

- **پس از ورود به vCenterیا ESXi، می‌توانند:**
- ماشین‌های مجازی را خاموش کنند.
- Snapshotتهیه کنند.
- فایل‌های VMDKرا کپی کنند.
- دسترسی‌های جدید ایجاد کنند.
- تنظیمات امنیتی را تغییر دهند.

- **حملات Brute Forceو Password Spraying**
- اگر SSH، ESXi Shellیا رابط مدیریتی بدون محدودیت در دسترس باشند، مهاجم می‌تواند با هزاران تلاش ورود، رمز عبور حساب‌های مدیریتی را حدس بزند.

- **راهکارهای :Hardening**
- استفاده از رمزهای عبور پیچیده
- قفل شدن حساب پس از چند تلاش ناموفق
- احراز هویت چندمرحله‌ای (MFA)
- محدود کردن دسترسی مدیریتی

- سوءاستفاده از سرویس‌های مدیریتی
- فعال بودن سرویس‌هایی مانند:
- SSH
- ESXi Shell
- DCUI
- Web Management
- سطح حمله را افزایش می‌دهد. این سرویس‌ها باید فقط در زمان نیاز فعال باشند.

- **حملات VM Escape**
- یکی از خطرناک‌ترین سناریوها، فرار از ماشین مجازی (VM Escape) است.

- در این حمله، مهاجم از داخل یک ماشین مجازی، با سوءاستفاده از آسیب‌پذیری‌های Hypervisor، به خود ESXi دسترسی پیدا می‌کند و سپس سایر ماشین‌های مجازی را نیز در اختیار می‌گیرد.

- اگرچه این حملات نادر هستند، اما به دلیل پیامدهای بسیار شدید، به‌روزرسانی منظم ESXi و نصب وصله‌های امنیتی اهمیت زیادی دارد.

- **حملات داخلی (Insider Threat)**
- همه تهدیدها از بیرون سازمان نیستند. کاربران یا مدیران دارای دسترسی نیز می‌توانند:
- ماشین‌های مجازی را حذف کنند.
- Snapshotها را پاک کنند.
- فایل‌های VMDKرا کپی کنند.
- تنظیمات شبکه را تغییر دهند.
- Logها را حذف کنند.
- برای کاهش این ریسک باید از اصل **حداقل سطح دسترسی (Least Privilege)**، ثبت کامل رویدادها و تفکیک وظایف استفاده شود.

حملات به Datastore

- Datastoreمحل ذخیره مهم‌ترین دارایی‌های مجازی است، از جمله:
- فایل‌های VMDK
- فایل‌های VMX
- Snapshotها
- ISOها
- Templateها
- دسترسی غیرمجاز به Datastoreمی‌تواند منجر به سرقت یا تخریب گسترده داده‌ها شود.

- **حملات شبکه‌ای علیه Hypervisor**
- Hypervisorمستقیماً به شبکه مدیریتی، شبکه ذخیره‌سازی و شبکه ماشین‌های مجازی متصل است. مهاجمان ممکن است از تکنیک‌هایی مانند:
- ARP Spoofing
- MAC Flooding
- VLAN Hopping
- Packet Sniffing
- Man-in-the-Middle (MITM)
- برای شنود یا دستکاری ترافیک استفاده کنند.

- **حذف یا دستکاری لاگ‌ها**
- یکی از اولین اقدامات مهاجم پس از نفوذ، حذف یا تغییر لاگ‌های امنیتی است تا آثار حمله پنهان بماند.
- به همین دلیل، ارسال لاگ‌ها به یک **Syslog Server**یا **SIEM**مستقل مانند Splunk یا Wazuh از مهم‌ترین اقدامات Hardeningمحسوب می‌شود.

- **چرا Hardeningسرور ESXiضروری است؟**
- اجرای Hardeningباعث می‌شود:
- کاهش سطح حمله Attack Surface
- محدود شدن دسترسی مهاجمان
- جلوگیری از سوءاستفاده از سرویس‌های غیرضروری
- افزایش امنیت حساب‌های مدیریتی
- محافظت از ماشین‌های مجازی و Datastore
- بهبود قابلیت کشف و پاسخ به رخدادها از طریق ثبت لاگ مناسب
- هم‌راستایی با استانداردهایی مانند **CIS Benchmark**، **NIST SP 800-53**، **DISA STIG**و **ISO/IEC 27001**

- **تأثیر Hardening بر دسترسی مدیریتی ESXi**
- **هدف سناریو**
- مشاهده تفاوت وضعیت سرور قبل و بعد از اعمال تنظیمات Hardening بر روی سرویس‌های مدیریتی.

- **وضعیت اولیه (Baseline)**
- در این مرحله، تنها وضعیت امنیتی میزبان را مستند می‌کنیم:
- SSH فعال است.
- ESXi Shell فعال است.
- Lockdown Mode غیرفعال است.
- Syslog محلی است.
- NTP تنظیم نشده است.
- حساب‌های مدیریتی بررسی نشده‌اند.

- **اجرای Hardening**
- کنترل‌های CISرا اعمال کنید، مانند:
- غیرفعال کردن SSH
- غیرفعال کردن ESXi Shell
- فعال کردن Lockdown Mode
- تنظیم Syslogروی سرور مرکزی
- پیکربندی NTP
- محدودسازی دسترسی مدیریتی
- حذف حساب‌های غیرضروری

- **تهدید**
- فعال بودن ESXi Shell باعث می‌شود مهاجم در صورت به‌دست آوردن نام کاربری و رمز عبور، مستقیماً به Hypervisor دسترسی پیدا کند.
- نمونه حملات:
- اجرای Backdoor
- نصب Rootkit
- حذف Logها
- تغییر تنظیمات امنیتی
- نصب VIBهای مخرب
- استخراج اطلاعات ماشین‌های مجازی

- **سناریوی واقعی حمله**
- فرض کنید مهاجم از طریق حمله Phishing رمز عبور ادمین vCenter را به دست آورده است.
- اگر ESXi Shell فعال باشد:

1. ورود به Host
2. اجرای Shell
3. خاموش کردن Logging
4. نصب Backdoor
5. دسترسی دائمی به Host

- در نتیجه مهاجم می‌تواند کنترل کامل Hypervisor را در اختیار بگیرد.

- **غیرفعال کردن ESXi Shell**
- **هدف**
- جلوگیری از دسترسی مستقیم به سیستم عامل ESXi

- Host
- ↓
- Configure
- ↓
- System
- ↓
- Services

- در ادامه سرویس TSM را پیدا کرده و STOP نمایید

- و Startup Policy را روی قراردهیم
- Start and stop manually
- **نحوه تست**
- از قسمت
- وضعیت باید Stopped باشد

- **نکات پروژه‌ای**
- در پروژه‌های Production بهتر است Shell فقط هنگام عیب‌یابی فعال شود.

- **Lockdown Mode**
- کنسول وب

- Host
- ↓
- Configure
- ↓
- Security Profile
- ↓
- Lockdown Mode
- ↓
- Edit

- انتخاب گزینه Normal یا Strict

- **Password Policy**
- کنسول وب

- Host
- ↓
- Configure
- ↓
- System
- ↓
- Advanced System Settings
- ↓
- Security.PasswordQualityControl

Disable SSH Service

- کاهش سطح حمله (Attack Surface)
- **اهمیت**
- Critical
- **تهدید**
- فعال بودن SSH باعث می‌شود مهاجم بعد از سرقت Credential مستقیماً وارد Hypervisor شود.

- حملات قابل جلوگیری
- Brute Force
- Credential Stuffing
- Password Spraying
- Lateral Movement
- Persistence
- Malware Installation

- **سناریوی واقعی**
- مهاجم با VPN وارد شبکه می‌شود.
- Credential مدیر را پیدا می‌کند.
- SSH فعال است.
- مستقیماً وارد ESXi می‌شود.
- Logها را حذف می‌کند.
- Backdoor نصب می‌کند.

مسیر پیاده سازی

- Host
- ↓
- Configure
- ↓
- Services
- ↓
- TSM-SSH
- ↓
- Stop

- **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