Aula 24 — Hardening, Atualizações e Proteção de Recursos

UC01 • Instalação de redes locais | Aula 24 de 27 | 3h30 | Turma TR5 | Professor: Msc Arlindo Batista Xavier Filho

Objetivos de aprendizagem

- Reconhecer hardening como redução sistemática da superfície de ataque mantendo a função do serviço.
- Inspecionar configurações de proteção, atualizações, usuários e serviços em Windows e Debian.
- Separar evidências observadas, hipótese de risco, ação autorizada e resultado de reteste.
- Priorizar achados e elaborar um plano de correção seguro, documentado e reversível.

1. Situação-problema — entregar a rede não significa terminar a segurança

Depois de implementar DHCP, DNS e compartilhamentos, a Escola Horizonte identificou três questões: uma estação pode estar com atualizações pendentes; o servidor de arquivos mantém serviços cuja necessidade não foi comprovada; e parte dos usuários utiliza contas com privilégios acima do necessário. Antes da entrega do projeto, a equipe deverá realizar uma verificação básica de configuração de segurança. Os achados usados na oficina são simulados e não representam o ambiente real do Senac.



Figura 24.1 — Ativos fictícios que serão analisados na oficina da Escola Horizonte.

2. O que avaliar no hardening

Dimensão	Pergunta técnica / evidência
Inventário e suporte	Qual é o SO, a versão e o responsável pelo ativo? Há suporte?
Atualizações	Existe política de patches? Qual a última atualização comprovada?
Proteção do host	Firewall e antimalware estão ativos, quando aplicável?
Serviços e portas	Quais serviços estão escutando e quais são necessários?
Identidades e acesso	Existem acessos excessivos ou contas sem justificativa?
Dados e continuidade	O compartilhamento possui permissões, cópias de segurança e plano de recuperação?

Uma porta aberta não é automaticamente uma vulnerabilidade: é necessário considerar a finalidade, origem permitida, autenticação, exposição, versão e controles compensatórios. Similarmente, uma atualização “pendente” exige confirmar sua aplicabilidade, janela de manutenção e possibilidade de recuperação.

3. Ferramentas de inspeção — somente leitura

Windows: PowerShell ou prompt autorizado

```
hostname
Get-ComputerInfo | Select-Object CsName, WindowsProductName, OsVersion
Get-NetFirewallProfile | Select-Object Name, Enabled, DefaultInboundAction
Get-MpComputerStatus | Select-Object AMRunningMode, AntivirusEnabled, RealTimeProtectionEnabled
Get-Service | Where-Object Status -eq 'Running' | Select-Object -First 12 Name, DisplayName
Get-NetTCPConnection -State Listen -ErrorAction SilentlyContinue |
  Select-Object -First 12 LocalAddress, LocalPort, State
Get-HotFix | Sort-Object InstalledOn -Descending | Select-Object -First 5
```

Get-MpComputerStatus pode não estar disponível quando outro produto de segurança estiver instalado ou quando o módulo não estiver presente; registre “não verificável” em vez de assumir proteção desligada. Get-HotFix não é inventário completo de todas as atualizações do Windows: complemente com o histórico oficial de atualizações e ferramenta de gestão aplicável.

Debian: terminal da VM isolada

```
hostnamectl
cat /etc/os-release
id
ss -lnt
systemctl --type=service --state=running --no-pager
apt list --upgradable 2>/dev/null
systemctl is-enabled unattended-upgrades.service 2>/dev/null
sudo nft list ruleset        # apenas VM autorizada; leitura
```

O resultado de apt list --upgradable depende da atualização prévia dos índices de pacotes: índices desatualizados podem omitir atualizações. Não execute apt upgrade, desative serviços nem altere firewall em equipamentos institucionais durante a inspeção.

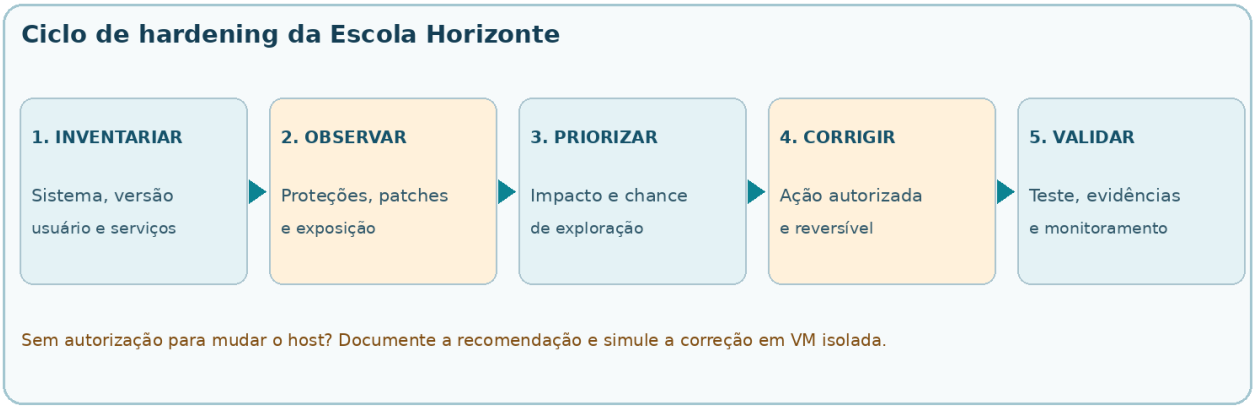


Figura 24.2 — Ciclo de proteção: observar, justificar, corrigir somente com autorização e validar.

4. Oficina prática — Auditoria de configuração da Escola Horizonte

1. Organize uma equipe e receba o inventário dos três ativos fictícios (Windows, Debian e servidor de arquivos).
2. Colete evidências de consulta em uma estação ou VM autorizada, usando comandos compatíveis com o sistema disponível.
3. Classifique cinco cartões de achados: W1 firewall do perfil público desativado; W2 atualizações sem comprovação; L1 serviço de teste em escuta sem necessidade documentada; S1 visitantes com permissão de edição em pasta; S2 backup sem teste de restauração.
4. Em cada achado, registre: evidência, impacto provável, chance estimada (baixa, média, alta), prioridade e ação recomendada.
5. Selecione dois achados prioritários e descreva o procedimento de correção, autorização necessária, teste de aceite e reversão.

6. Execute somente ações explicitamente autorizadas em VM isolada ou simulação. Em ambiente institucional, encerre a atividade com relatório e recomendação, sem aplicar alterações.
7. Revise a proposta com outra equipe e exporte o relatório de evidências para anexar ao Teams.

5. Critério simples de priorização — proposta didática

Impacto × probabilidade	Baixa	Média	Alta
Impacto baixo	Baixa	Baixa	Média
Impacto médio	Baixa	Média	Alta
Impacto alto	Média	Alta	Alta

Essa matriz é uma ferramenta pedagógica simplificada. Não é um escore CVSS nem uma avaliação formal de risco. A equipe deve justificar seus critérios com base nas consequências para o serviço, exposição e evidências disponíveis.

6. Entrega no Teams

- Ficha de inspeção com pelo menos cinco achados e suas evidências ou cartões simulados.
- Plano de tratamento de dois riscos priorizados (responsável, medida, pré-requisito, verificação e reversão).
- Um registro de “antes e depois” realizado em VM ou descrição do teste quando não houver permissão para mudar a configuração.
- Conclusão: quais riscos permanecem, o que precisa de aprovação e qual é o próximo passo do projeto da Escola Horizonte.

Referências e aprofundamento

CIS. CIS Critical Security Controls v8.1. Disponível em: https://www.cisecurity.org/controls/cis-controls-list. Acesso em: 31 out. 2026.

MICROSOFT. Get-NetFirewallProfile — NetSecurity. Disponível em: https://learn.microsoft.com/en-us/powershell/module/netsecurity/get-netfirewallprofile. Acesso em: 31 out. 2026.

MICROSOFT. Get-MpComputerStatus — Defender. Disponível em: https://learn.microsoft.com/pt-br/powershell/module/defender/get-mpcomputerstatus. Acesso em: 31 out. 2026.

DEBIAN. Security Information. Disponível em: https://www.debian.org/security/. Acesso em: 31 out. 2026.

DEBIAN. PeriodicUpdates. Disponível em: https://wiki.debian.org/PeriodicUpdates. Acesso em: 31 out. 2026.

DEBIAN. nftables. Disponível em: https://wiki.debian.org/nftables. Acesso em: 31 out. 2026.