Tempest

ACADEMY

Conference

O Bonito, O Feio e o Que Ninguém Fala pra Você.

Gestão de Vulnerabilidades

Dayvidson Bezerra
Terencio Amazonas

Classificação da Informação: PÚBLICA Autor da apresentação: Dayvidson, Terencio.

Tempest

ACADEMY

Conference

01 O Bonito

02 O Feio

03 O que ninguém fala para você

04 Panorama da gerência de vulnerabilidades

Classificação da Informação: PÚBLICA Autor da apresentação: Dayvidson, Terencio.

Tempest
ACADEMY
Conference

O Que é Gestão de Vulnerabilidades?

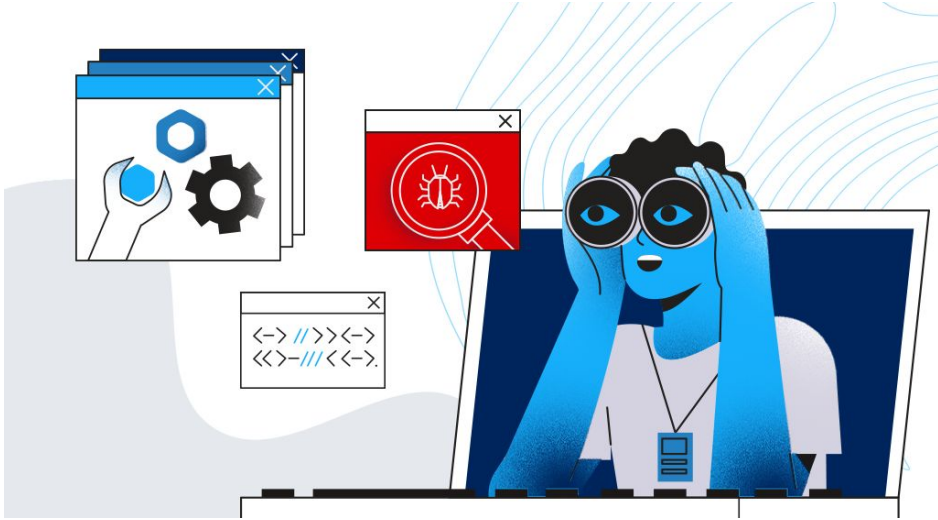
- **O objetivo principal:**
  - É reduzir a exposição geral da organização ao risco, mitigando o maior número possível de vulnerabilidades.
- **Abordagem Baseada em Riscos:**
  - Descobrir, priorizar, corrigir e reavaliar vulnerabilidades e erros de configuração no ambiente.
- **Processo Contínuo:**
  - Cíclico, proativo e muitas vezes automatizado que mantém seus sistemas “protegidos” contra ataques cibernéticos e violações de dados.

Tempest

ACADEMY

Conference

O Bonito



Tempest

[ACADEMY]

Conference

O Mundo das Ferramentas

- Ferramentas são legais;
- Funcionam;
- Geralmente tem uma taxa de detecção boa;
- Facilitam o dia-a-dia.

O que promete é bonito!

Tempest
:ACADEMY:
Conference

- Ser a maior base de Vulnerabilidades
- Entrega rápida de detecção
- Gestão da Ferramenta na Cloud
- Maior número de plugins de detecção
- Gráficos informacionais
- Inteligência sobre ameaças
- Resultado dos Scans
- Reports
- API e Integrações
- Facilidade na Gestão
- Priorização de correção
- Hardening

Classificação da Informação: PÚBLICA Autor da apresentação: Dayvidson, Terencio.

Tempest

ACADEMY

Conference

A Facilidade e a Otimização

- Sensação de confiabilidade para os clientes;
- Workflow da gestão de vulnerabilidades;
- Facilidade de uso;
- A ferramenta já vem pré-configurada;
- Qualquer time pilota a ferramenta.

Tempest

[ACADEMY]

Conference

O Feio

Tempest
[ACADEMY]
Conference

Deploy da Ferramenta

- Dificuldades em processos de instalação dos componentes; *(sincronização ativos);*
- Dificuldades no processo de instalação dos agentes;
- Manutenção do ambiente (monitoramento);
- Atualizações da ferramenta, componentes, agentes;
- Diferentes arquiteturas (*Agentless*, *Agent Based*, *Network Scanner Auth/NoAuth*).

Case: Falha conectividade Proxy

Case: Falha auto-update Agent

Classificação da Informação: PÚBLICA Autor da apresentação: Dayvidson, Terencio.

Tempest
ACADEMY
Conference

Nível de acesso e Superfície de Ataque

- Alto nível de acesso para realização de scan autenticado, permissão de administrador/root.
- Se possui agente por qual motivo ter scan via rede autenticado? *(Agent, Auth/NoAuth)*
- Gerenciamento dessas credenciais e privilégios que as ferramentas solicitam *(como administrar)?*
- Necessidade que serviços sejam habilitados para acesso remoto, como pré-requisitos.

Case: Ambiente híbrido

Classificação da Informação: PÚBLICA Autor da apresentação: Dayvidson, Terencio.

Tempest
[ACADEMY]
Conference

O Que Não é Falado Sobre as Ferramentas?

- Bugs (Features/Detecção);
- Limitações da ferramenta;
  - Ciclo de vida do Risco Aceito
- Cobertura da ferramenta;
  - GAP de Vulnerabilidades e Dispositivos.
- Falso Positivos;
- Falso Negativos;
- Conhecimentos que a equipe técnica precisa:
  - CVE;
  - CPE;
  - Banner ou Tipo da Exploração.

Tempest
[ACADEMY]
Conference

Quais Vulnerabilidades são Detectadas Primeiro?

- Vulnerabilidades críticas e conhecidas;
  - Força tarefa, rapidez;
- Vulnerabilidades de software que é usado em um grande número de clientes;
  - Impacto em larga escala;
- Vulnerabilidades de patches lançadas por fabricantes;
- Vulnerabilidades baseadas em boletins de segurança.

Tempest
ACADEMY
Conference

Bug Report - 01

Ativos com o Openssl nas versões 1.1.1f e 1.1.1l não estavam tendo suas vulnerabilidades detectadas;

- ➔ Foi verificado pela equipe que o plugin disponibilizado pelo fabricante não estava detectando a vulnerabilidade corretamente;
- ➔ Sem o conhecimento sobre a vulnerabilidade e conhecimento do ambiente não é possível detectar essas falhas;
- ➔ Caso não seja detectado o ambiente estará vulnerável e a operação com a sensação de segurança.

Tempest
ACADEMY
Conference

Bug Report - 02

Funcionalidade de proxy do agente não funcionava

- ➔ Detectado pela equipe da Tempest;
- ➔ Documentação do fabricante apontava como funcional;
- ➔ Afetava diretamente a arquitetura de segurança/comunicação com ambiente externo do cliente;
- ➔ Atraso no processo de deploy dos agentes e scans das vulnerabilidades.

Tempest

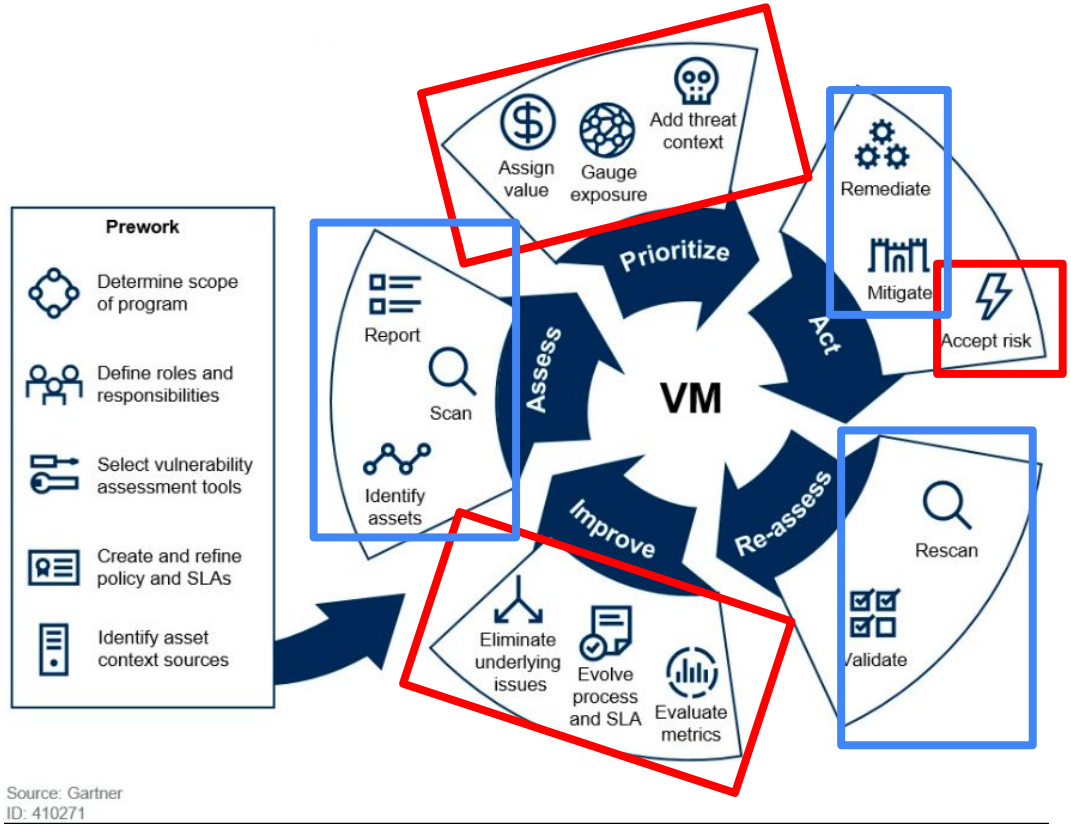
[ACADEMY]

Conference

O Que Ninguém Fala pra Você

Ciclo de Gestão de Vulnerabilidades

Tempest
ACADEMY
Conference



Source: Gartner
ID: 410271

O que fazer para ficar Bonito?

Tempest
ACADEMY
Conference

Gestão Centralizada das Vulnerabilidades:

- ➔ Políticas;
- ➔ Quando foi descoberta?
- ➔ Quando foi corrigida?
- ➔ Qual equipe? Quem corrigiu?
- ➔ Porque foi reaberta?
- ➔ SLA de correção;
- ➔ Aceite de risco;
- ➔ Mitigação de risco;

3E - Eficiência, Eficácia e Efetividade

Tempest
[ACADEMY]
Conference

Princípios:

- Ter Eficiência em gestão de vulnerabilidades;
  - Fazer o que foi proposto de maneira rápida e em menor tempo;
- Ter Eficácia em gestão de vulnerabilidades;
  - Entregou o que era para ser entregue;
  - As ferramentas de scans de vulnerabilidades se encontram aqui;
- Ter Efetividade em gestão de vulnerabilidades;
  - De forma definitiva, corrigiu de maneira efetiva e o problema não vai aparecer novamente.

Blindspot nas Ferramentas de Scans de Vulnerabilidades

Tempest ACADEMY Conference

CISA Known Exploited

08.02.2022!

VulnKBdiff

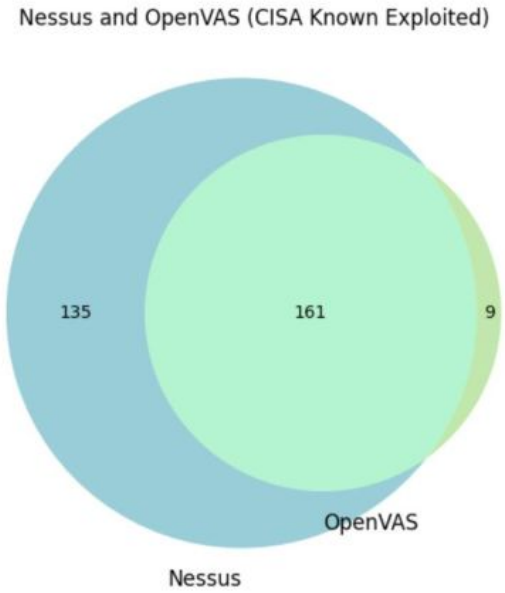
Profile: CISA Known Exploited

Filtered CVEs: 352

OpenVAS CVEs: 170

Nessus CVEs: 296

NVD CVEs: 350



Fonte: https://avleonov.com/2022/02/18/vmconf-22-blindspots-in-the-knowledge-bases-of-vulnerability-scanners/

Blindspot nas Ferramentas de Scans de Vulnerabilidades

Tempest ACADEMY Conference

CISA Known Exploited

VulnKBdiff

Profile: CISA Known Exploited

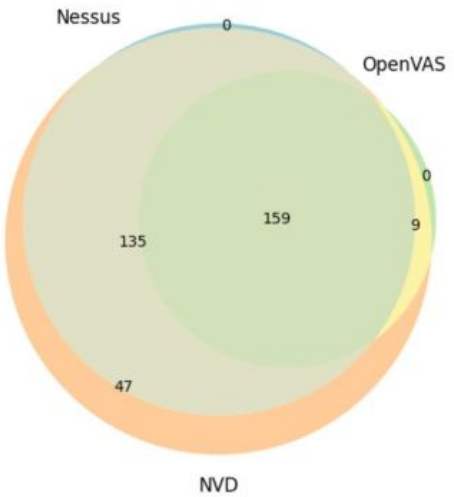
Filtered CVEs: 352

OpenVAS CVEs: 170

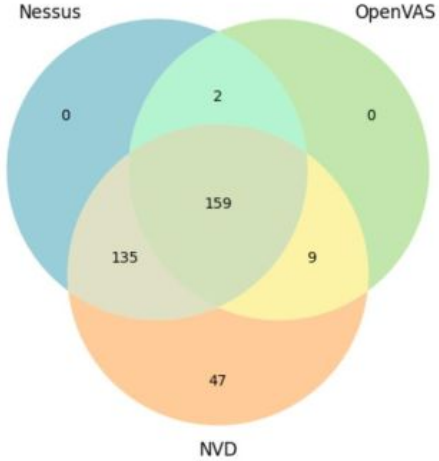
Nessus CVEs: 296

NVD CVEs: 350

Nessus, OpenVAS and NVD (CISA Known Exploited), weighted



Nessus, OpenVAS and NVD (CISA Known Exploited), unweighted



Fonte: https://avleonov.com/2022/02/18/vmconf-22-blindspots-in-the-knowledge-bases-of-vulnerability-scanners/

Tempest

:ACADEMY:

Conference

Panorama da Gerência de Vulnerabilidades

Cyber Threat Intelligence

Tempest
:ACADEMY:
Conference

- **Reports Situacionais**
  - Visão gerencial do que está ocorrendo;
- **Notícias sobre ataques/explorações que estão ocorrendo**
  - Como isso interfere no dia-a-dia.

- **Feeds de IOCs**
  - As vezes eu não posso corrigir a exploração, mas é possível detectar o atacante;
- **Monitoração de vulnerabilidades de plataformas**;
  - As ferramentas não vão encontrar tudo, portanto é importante ter outras fontes de alerta.

Conclusão

Tempest
ACADEMY
Conference

- Gerência de vulnerabilidade é uma disciplina muito madura;
- Muitas empresas executam apenas parte do processo (enumeração, discovery) - ferramentas;
- Processos e procedimentos fazem a diferença para gerenciar de maneira eficaz o que é importante;
- Não é opcional não agregar inteligência ao processo de gerenciamento de vulnerabilidades.

Agradecimentos

Tempest
[ACADEMY]
Conference

Obrigado !!

Dayvidson Bezerra

Terencio Amazonas

Tempest
ACADEMY
Conference

Ask The Experts !!

Tire suas dúvidas

Tempest
ACADEMY
Conference

Classificação da Informação: PÚBLICA Autor da apresentação:Dayvidson, Terencio