

The background features abstract geometric shapes in shades of green and blue. A red plus sign is located to the left of the title. Green 'x' marks are scattered in the top-left and bottom-right corners. A red circle is in the bottom-right corner.

Analyse des vulnérabilités

a.BERBAR
2024-2025



01

Concept d'analyse de vulnérabilités

Définitions

- ❑ **Menace** - Un incident potentiellement dangereux (tsunami, tremblement de terre, virus, ...)
- ❑ **Vulnérabilité** - Une faiblesse qui peut permettre à la menace de faire du mal. Avoir un centre de données dans la zone inondée par le tsunami, ne pas résister aux tremblements de terre, ne pas appliquer de correctifs et d'antivirus,
- ❑ **Risque** = Menace x Vulnérabilité.
- ❑ **Impact** - Peut parfois être ajouté pour donner une image plus complète. Risque = Menace x Vulnérabilité x Impact (Quelle est la gravité ?).
- ❑ **Risque total** = Menace x Vulnérabilité x Valeur de l'actif.
- ❑ **Risque résiduel** = Risque total – Contre-mesures.

Recherche de vulnérabilités

- ❑ Le processus d'analyse des protocoles, des services et des configurations pour **découvrir les vulnérabilités et les défauts de conception** qui exposeront un système d'exploitation et ses applications à une exploitation, une attaque ou une utilisation abusive.
- ❑ Les vulnérabilités sont classées en fonction du **niveau de gravité** (faible, moyen ou élevé) et de la portée de l'exploitation (locale ou distante)

Recherche de vulnérabilités

- ❑ Un administrateur a besoin d'une recherche de vulnérabilité :
 - ❑ Recueillir des informations sur les tendances en matière de sécurité, les menaces, les surfaces d'attaque, les vecteurs et les techniques d'attaque
 - ❑ Pour découvrir les faiblesses du système d'exploitation et des applications, et alerter l'administrateur réseau avant une attaque réseau
 - ❑ Recueillir des informations pour aider à la prévention des problèmes de sécurité
 - ❑ Savoir comment se remettre d'une attaque réseau

Ressources pour recherche de vulnérabilités



Computerworld

<https://www.computerworld.com>



Microsoft Vulnerability Research (MSVR)

<https://www.microsoft.com>



PenTest Magazine

<https://pentestmag.com>



HackerStorm

<http://www.hackerstorm.co.uk>



Dark Reading

<https://www.darkreading.com>



SecurityTracker

<https://securitytracker.com>



SC Magazine

<https://www.scmagazine.com>



Trend Micro

<https://www.trendmicro.com>



SecurityFocus

<https://www.securityfocus.com>



Exploit Database

<https://www.exploit-db.com>



Help Net Security

<https://www.helpnetsecurity.com>



Security Magazine

<https://www.securitymagazine.com>

Évaluation des vulnérabilités

- ❑ L'évaluation de la vulnérabilité est un examen approfondi de la capacité d'un système ou d'une application, y compris les procédures et contrôles de sécurité actuels, à résister à l'exploitation.
- ❑ Identifie, mesure et classe les vulnérabilités de sécurité dans un système informatique, un réseau et des canaux de communication
- ❑ Une évaluation de la vulnérabilité peut être utilisée pour :
 - ❑ Identifier les faiblesses qui pourraient être exploitées
 - ❑ Prédire l'efficacité des mesures de sécurité supplémentaires pour protéger les ressources d'information contre les attaques
- ❑ Les informations obtenues à partir du scanner de vulnérabilité comprennent :
 - ❑ Vulnérabilités du réseau
 - ❑ Ports ouverts et services en cours d'exécution
 - ❑ Vulnérabilités des applications et des services
 - ❑ Erreurs de configuration des applications et des services

systemes et bases de données de notation des vulnérabilités

Système commun de notation des vulnérabilités (CVSS)

- CVSS fournit un cadre ouvert pour communiquer les caractéristiques et les impacts des vulnérabilités informatiques
- Son modèle quantitatif garantit une mesure précise et répétable, tout en permettant aux utilisateurs de visualiser les caractéristiques de vulnérabilité sous-jacentes utilisées pour générer les scores

CVSS v3.0 Ratings

Severity	Base Score Range
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

CVSS v2.0 Ratings

Severity	Base Score Range
Low	0.0-3.9
Medium	4.0-6.9
High	7.0-10

Common Vulnerability Scoring System Calculator Version 3 CVE-2017-0144

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.



Base Score Metrics

Exploitability Metrics

Attack Vector (AV)*

Network (N) | Adjacent Network (AN) | Local (L) | Physical (P)

Attack Complexity (AC)*

Low (LC) | High (HC)

Privileges Required (PR)*

None (N) | Low (L) | High (H)

User Interaction (UI)*

None (N) | Required (R)

Scope (S)*

Unchanged (U) | Changed (C)

Impact Metrics

Confidentiality Impact (CI)*

None (N) | Low (L) | High (H)

Integrity Impact (II)*

None (N) | Low (L) | High (H)

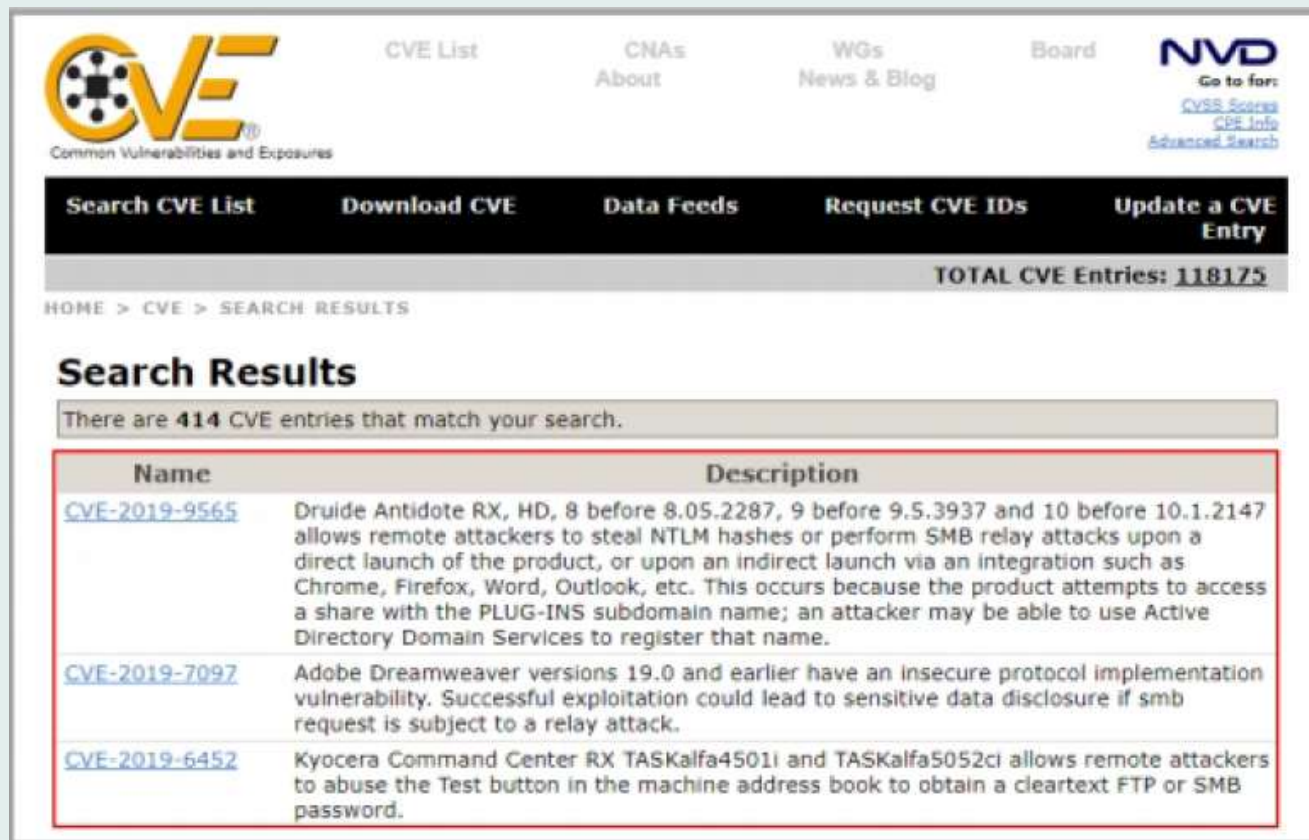
Availability Impact (A)*

None (N) | Low (L) | High (H)

* All base metrics are required to generate a base score.

systemes et bases de donnees de notation des vulnerabilites

- ❑ Vulnérabilités et expositions courantes (CVE)
- ❑ Une liste ou un dictionnaire accessible au public et gratuit d'identifiants normalisés pour les vulnérabilités et expositions logicielles courantes



The screenshot shows the CVE website interface. At the top, there is a navigation bar with links: CVE List, CNAs About, WG's News & Blog, Board, and NVD. The NVD section includes links for CVSS Scores, CVE Info, and Advanced Search. Below the navigation bar is a search bar with buttons: Search CVE List, Download CVE, Data Feeds, Request CVE IDs, and Update a CVE Entry. A status bar indicates 'TOTAL CVE Entries: 118175'. The main content area shows 'HOME > CVE > SEARCH RESULTS' and a 'Search Results' section. A message states 'There are 414 CVE entries that match your search.' Below this is a table with two columns: Name and Description.

Name	Description
CVE-2019-9565	Druid Antidote RX, HD, 8 before 8.05.2287, 9 before 9.5.3937 and 10 before 10.1.2147 allows remote attackers to steal NTLM hashes or perform SMB relay attacks upon a direct launch of the product, or upon an indirect launch via an integration such as Chrome, Firefox, Word, Outlook, etc. This occurs because the product attempts to access a share with the PLUG-INS subdomain name; an attacker may be able to use Active Directory Domain Services to register that name.
CVE-2019-7097	Adobe Dreamweaver versions 19.0 and earlier have an insecure protocol implementation vulnerability. Successful exploitation could lead to sensitive data disclosure if smb request is subject to a relay attack.
CVE-2019-6452	Kyocera Command Center RX TASKalfa4501i and TASKalfa5052ci allows remote attackers to abuse the Test button in the machine address book to obtain a cleartext FTP or SMB password.

systèmes et bases de données de notation des vulnérabilités

- ❑ Base de données nationale sur la vulnérabilité (NVD)
- ❑ Un référentiel du gouvernement américain de données de gestion des vulnérabilités basées sur des normes représentées à l'aide du protocole d'automatisation du contenu de sécurité (SCAP)
- ❑ Ces données permettent l'automatisation de la gestion des vulnérabilités, des mesures de sécurité et de la conformité
- ❑ Le NVD comprend des bases de données de références de listes de contrôle de sécurité, de failles logicielles liées à la sécurité, de mauvaises configurations, de noms de produits et de mesures d'impact

NIST
Information Technology Laboratory
NATIONAL VULNERABILITY DATABASE

VULNERABILITIES

Vulnerability Identifier
CVE-2019-6452 Detail

Vulnerability Published Date
06/04/2019

Current Description
Hypocore Command Center R4 TASKalfa503i and TASKalfa5052ci allows remote attackers to abuse the Test button in the machine address book to obtain a cleartext FTP or SMB password.

Source: MITRE
[View Analysis Description](#)

Impact

CVSS v3 Score
CVSS v3.0 Severity and Metrics:
Base Score: 8.8 HIGH
Vector: AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/AU:(V2 legend)
Impact Score: 5.9
Exploitability Score: 2.9

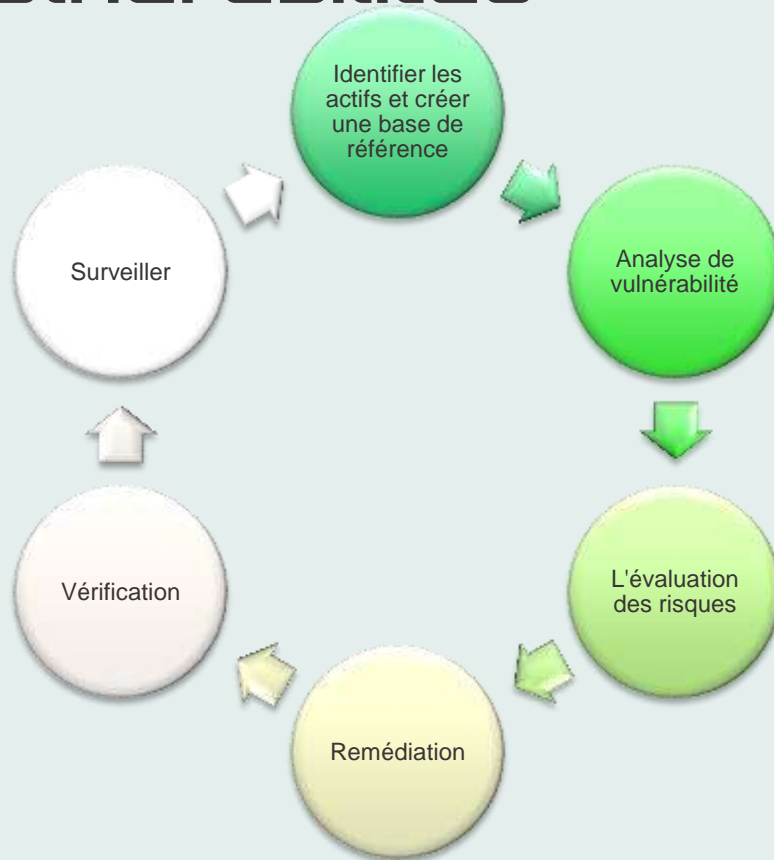
CVSS v2 Score
CVSS v2.0 Severity and Metrics:
Base Score: 4.0 MEDIUM
Vector: (AV:N/AC:L/Au:S/C:P/B:N/AU:N) (V2 legend)
Impact Subscore: 2.9
Exploitability Subscore: 1.1

QUICK INFO
CVE Dictionary Entry:
CVE-2019-6452
NVD Published Date:
06/04/2019
NVD Last Modified:
06/11/2019

Attack Vector (AV): Network
Attack Complexity (AC): Low
Privileges Required (PR): Low
User Interaction (UI): None

Access Vector (AV): Network
Access Complexity (AC): Low
Authentication (AU): Single
Confidentiality (C): Partial
Integrity (I): None

Cycle de vie de la gestion des vulnérabilités



Phase de pré-évaluation

- ❑ **modifier les actifs et créer une base de référence**
- ❑ Identifier et comprendre les processus métiers
- ❑ Identifier les applications, les données et les services qui prennent en charge les processus métier et effectuer des revues de code
- ❑ Identifier les logiciels approuvés, les pilotes et la configuration de base de chaque système
- ❑ Créez un inventaire de tous les actifs et hiérarchisez/classez les actifs critiques
- ❑ Comprendre l'architecture du réseau et cartographier l'infrastructure du réseau
- ❑ Identifier les contrôles déjà en place
- ❑ Comprendre la mise en œuvre des politiques et la conformité aux normes
- ❑ Définir la portée de l'évaluation
- ❑ Créer des procédures de protection des informations pour soutenir une planification, une programmation, une coordination et une logistique efficaces

Phase d'évaluation de la vulnérabilité

- ❑ Examiner et évaluer la sécurité physique
- ❑ Vérifiez les erreurs de configuration et les erreurs humaines
- ❑ Exécuter des analyses de vulnérabilité
- ❑ Sélectionnez le type d'analyse en fonction des exigences de l'organisation ou de la conformité
- ❑ Identifier et hiérarchiser les vulnérabilités
- ❑ Identifier les faux positifs et les faux négatifs
- ❑ Appliquer le contexte commercial et technologique aux résultats du scanner
- ❑ Effectuer la collecte d'informations OSINT pour valider les vulnérabilités
- ❑ Créer un rapport d'analyse des vulnérabilités

Phase de poste évaluation

❑ Évaluation des risques

- ❑ Effectuer une catégorisation des risques
- ❑ Évaluer le niveau d'impact
- ❑ Identifier la menace et le niveau de risque

❑ Remédiation

- ❑ Prioriser les mesures correctives en fonction du classement des risques
- ❑ Élaborer un plan d'action pour mettre en œuvre la recommandation/mesure corrective
- ❑ Effectuer une analyse des causes profondes
- ❑ Appliquer des correctifs/correctifs
- ❑ Capturer les leçons apprises
- ❑ Réaliser des formations de sensibilisation
- ❑ Sélectionnez le type d'analyse en fonction des exigences de l'organisation ou de la conformité

Phase de poste évaluation

❑ Vérification

- ❑ Rescanner le système pour vérifier si les correctifs appliqués ont corrigé les vulnérabilités
- ❑ Effectuer une analyse dynamique
- ❑ Examen de la surface d'attaque

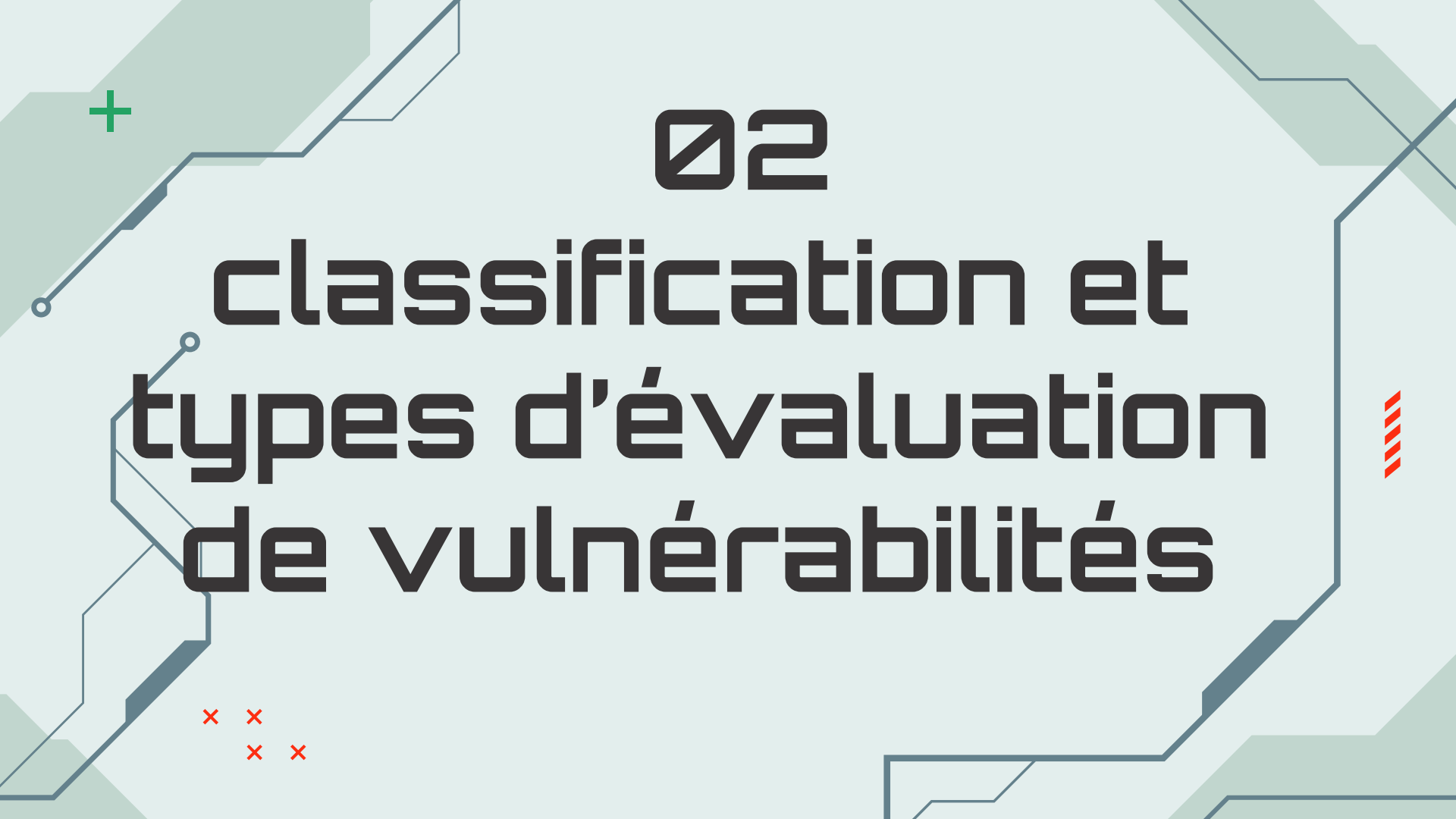
❑ Monitoring

- ❑ Scan et Évaluation périodique des vulnérabilités
- ❑ Correction rapide des vulnérabilités identifiées
- ❑ Journaux de détection et de prévention des intrusions
- ❑ Mise en œuvre de politiques, de procédures et de contrôles



02

classification et types d'évaluation de vulnérabilités



Classification de vulnérabilités

Misconfiguration



Default Passwords



Buffer Overflows



**Operating System
Flaws**



Application Flaws



Unpatched Servers



Design Flaws



Default Installations



Open Services



Types d'évaluations de vulnérabilités

Évaluation active

Utilise un scanner réseau pour trouver des hôtes, des services et des vulnérabilités

Évaluation externe

Évalue le réseau du point de vue d'un pirate informatique pour découvrir les exploits et les vulnérabilités accessibles au monde extérieur

Évaluation basée sur l'hôte

Effectue une vérification au niveau de la configuration pour identifier les configurations système, les répertoires utilisateur, les systèmes de fichiers, les paramètres de registre, etc., afin d'évaluer la possibilité de compromission

Évaluation des candidatures

Teste et analyse tous les éléments de l'infrastructure Web pour détecter toute **mauvaise configuration, tout contenu obsolète ou toute vulnérabilité connue**

Évaluation passive

Utilisé pour renifler le trafic réseau afin de découvrir les systèmes actifs présents, les services réseau, les applications et les vulnérabilités présentes

Évaluation interne

Analyse l'infrastructure interne pour découvrir les exploits et les vulnérabilités

Évaluation basée sur le réseau

Détermine les éventuelles attaques de sécurité du réseau qui peuvent survenir sur le système de l'organisation

Évaluation de la base de données

Se concentre sur les tests de bases de données, telles que MYSQL, MSSQL, ORACLE, POSTGRESQL, etc., pour détecter la présence de vulnérabilités de type exposition ou injection de données

Types d'évaluations de vulnérabilités

Évaluation du réseau sans fil

Détermine les vulnérabilités des réseaux sans fil de l'organisation

Évaluation distribuée

Évalue simultanément les actifs de l'organisation distribuée, tels que les applications client et serveur, grâce à des techniques de synchronisation appropriées

Évaluation accréditée

Évalue le réseau en obtenant les informations d'identification de toutes les machines présentes sur le réseau

Évaluation non accréditée

Évalue le réseau sans acquérir aucune information d'identification des actifs présents dans le réseau de l'entreprise

Évaluation manuelle

Dans ce type d'évaluation, le hacker éthique évalue manuellement les vulnérabilités, le classement des vulnérabilités, le score de vulnérabilité, etc.

Évaluation automatisée

Dans ce type d'évaluation, le hacker éthique utilise divers outils d'évaluation de la vulnérabilité, tels que Nessus, Qualys, GFI LanGuard, etc.



02

Solutions et outils d'évaluation de la vulnérabilité

Comparaison des approches d'évaluation de la vulnérabilité

Solutions d'évaluation basées sur les produits ou sur les services

Solutions basées sur les produits

- Installé dans le réseau interne de l'organisation
- Installé dans un espace privé ou non routable ou dans la partie adressable sur Internet du réseau d'une organisation
- S'il est installé sur le réseau privé ou, en d'autres termes, derrière le pare-feu, il ne peut pas toujours détecter les attaques extérieures



Solutions basées sur les services

- Proposés par des tiers, tels que des sociétés d'audit ou de conseil en sécurité
- Certaines solutions sont hébergées à l'intérieur du réseau, tandis que d'autres sont hébergées à l'extérieur du réseau
- Un inconvénient de cette solution est que les attaquants peuvent auditer le réseau depuis l'extérieur.



Comparaison des approches d'évaluation de la vulnérabilité

Évaluation basée sur l'arbre ou sur l'inférence

Évaluation basée sur les arbres

- L'auditeur sélectionne des stratégies différentes pour chaque machine ou composant du système d'information
- Par exemple, l'administrateur sélectionne un scanner pour les serveurs exécutant Windows, les bases de données et les services Web, et utilise un autre scanner pour les serveurs Linux
- Cette approche repose sur le fait que l'administrateur fournit une première vue d'ensemble des renseignements, puis effectue une analyse continue sans intégrer aucune information trouvée au moment de l'analyse.

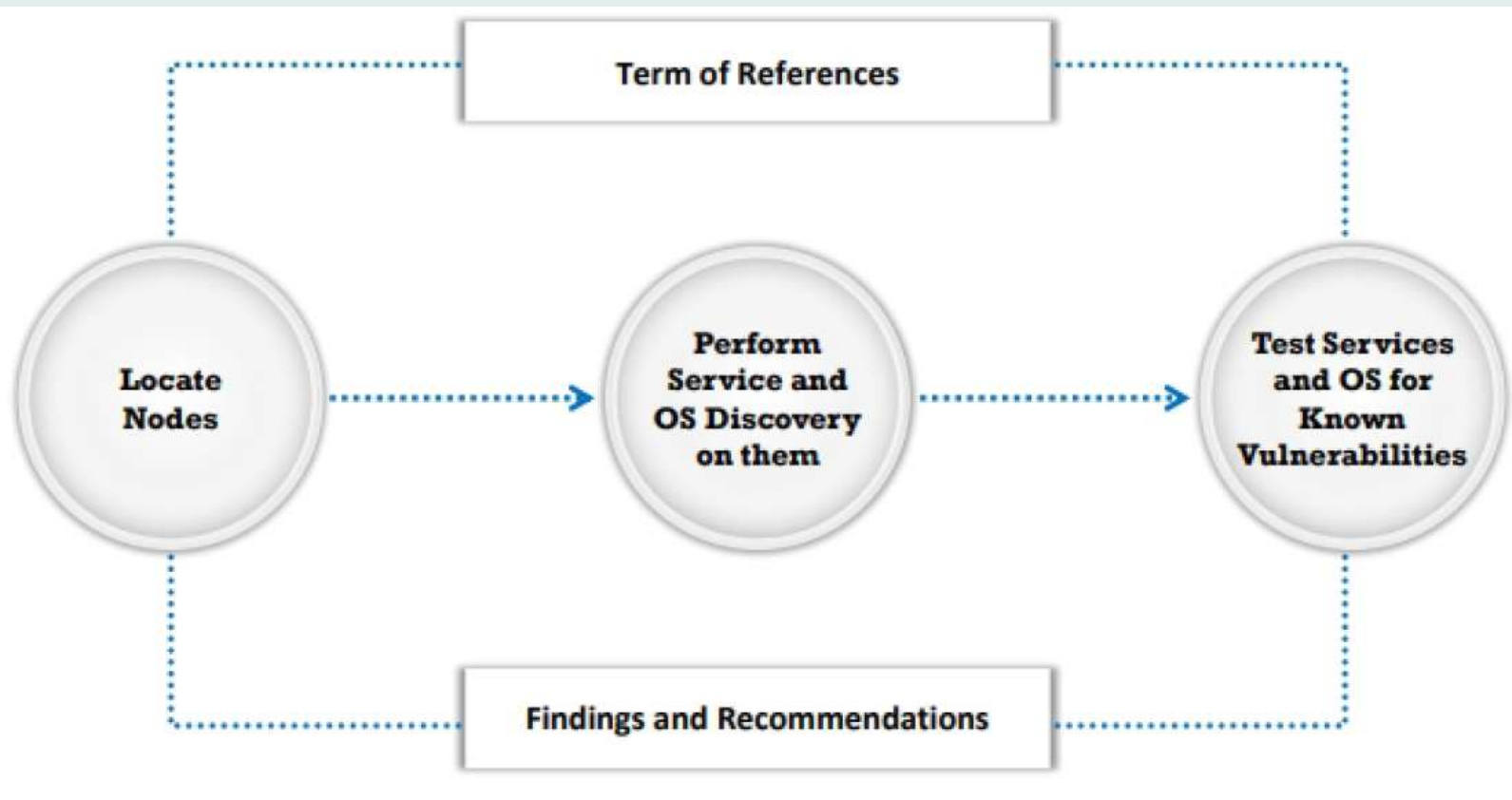
Évaluation basée sur l'inférence

- L'analyse commence par la création d'un inventaire des protocoles trouvés sur la machine
- Après avoir trouvé un protocole, le processus d'analyse détecte les ports connectés à des services, tels qu'un serveur de messagerie, un serveur Web ou un serveur de base de données.
- Après avoir trouvé les services, le processus sélectionne les vulnérabilités sur chaque machine et commence à exécuter uniquement les tests pertinents

caractéristiques d'une bonne solution d'évaluation de la vulnérabilité

- ❑ Assure des résultats corrects en testant le réseau, les ressources réseau, les ports, les protocoles et les systèmes d'exploitation
- ❑ Utilise une approche bien organisée basée sur l'inférence pour les tests
- ❑ Analyse automatiquement les bases de données continuellement mises à jour
- ❑ Crée des rapports brefs, exploitables et personnalisables, y compris les vulnérabilités, par niveau de gravité et une analyse des tendances
- ❑ Prend en charge plusieurs réseaux
- ❑ Suggère des remèdes et des solutions de contournement appropriés pour corriger les vulnérabilités
- ❑ Imiter la vue extérieure des attaquants

Fonctionnement d'une solution de scan de vulnérabilités



types d'outils d'évaluation de la vulnérabilité

Outils d'évaluation de la vulnérabilité basés sur l'hôte

- Recherche et identifie le système d'exploitation exécuté sur un ordinateur hôte particulier et le teste pour détecter les déficiences connues
- Recherches d'applications et de services courants



Outils d'évaluation en profondeur

- Trouve et identifie les vulnérabilités jusqu'à-là inconnues dans un système
- Ces types d'outils incluent les « fuzzers »



Outils d'évaluation de la vulnérabilité de la couche applicative

- Dirigé vers des serveurs Web ou des bases de données



Outils d'évaluation de la portée

- Assure la sécurité du système informatique en testant les vulnérabilités des applications et du système d'exploitation



Outils actifs et passifs

- Les scanners actifs effectuent des contrôles de vulnérabilité sur le réseau qui consomment des ressources sur le réseau
- Les scanners passifs n'affectent pas considérablement les ressources du système ; ils observent uniquement les données du système et effectuent le traitement des données sur une machine d'analyse distincte

Outils d'examen de localisation et de données

- Scanner basé sur le réseau
- Scanner basé sur un agent
- Scanner de proxy
- Scanner de cluster



choisir un outil d'évaluation de la vulnérabilité

- ❑ Les outils d'évaluation des vulnérabilités sont utilisés pour tester les vulnérabilités d'un hôte ou d'une application.
 - ❑ Choisissez les outils qui répondent le mieux aux exigences suivantes :
 - ❑ Peut tester de dizaines à 30 000 vulnérabilités différentes, selon le produit
 - ❑ Contient plusieurs centaines de signatures d'attaques différentes
 - ❑ Adapté à votre environnement et à votre expertise
 - ❑ Dispose d'un réseau précis, d'une cartographie des applications et de tests de pénétration
 - ❑ Dispose d'un certain nombre de scripts de vulnérabilité régulièrement mis à jour pour les plates-formes que vous analysez
 - ❑ Génère des rapports
 - ❑ Vérifie différents niveaux de pénétration afin d'éviter les blocages

Qualis vulnerability management

- Un service basé sur le cloud qui offre une visibilité immédiate et globale sur les parties du système informatique pouvant être vulnérables aux dernières menaces sur Internet, ainsi que sur les moyens de les protéger.

- Il aide à l'identification continue des menaces et à la surveillance des changements inattendus dans un réseau avant qu'ils ne deviennent des failles de sécurité.



Nessus professional

- ❑ Solution professionnelle d'évaluation pour l'identification des vulnérabilités, des problèmes de configuration et des malwares

The screenshot shows the Nessus Professional web interface. The browser address bar indicates the URL: <https://localhost:8834/#/scans/reports/6/hosts/2/vulnerabilities/group...>. The page title is 'Local Network / 10.10.1.22 / SSL (Multiple Issues)'. The left sidebar contains navigation links: 'My Scans', 'All Scans', 'Trash', 'Policies', 'Plugin Rules', and 'TerraScan'. The main content area displays a table of vulnerabilities. A red box highlights the first six rows of the table. To the right of the table, there are sections for 'Scan Details' and a 'Vulnerabilities' donut chart.

Sev	Score	Name	Family	Count
HIGH	7.5	SSL Medium ...	General	2
MEDIUM	6.5	SSL Certificat...	General	2
MEDIUM	6.4 *	SSL Self-Sign...	General	1
MEDIUM	5.3	SSL Certificat...	General	1
INFO		SSL Certificat...	General	2
INFO		SSL Cipher Bl...	General	2
INFO		SSL Cipher S...	General	2
INFO		SSL Perfect F...	General	2
INFO		SSL Certificat...	General	1

Scan Details

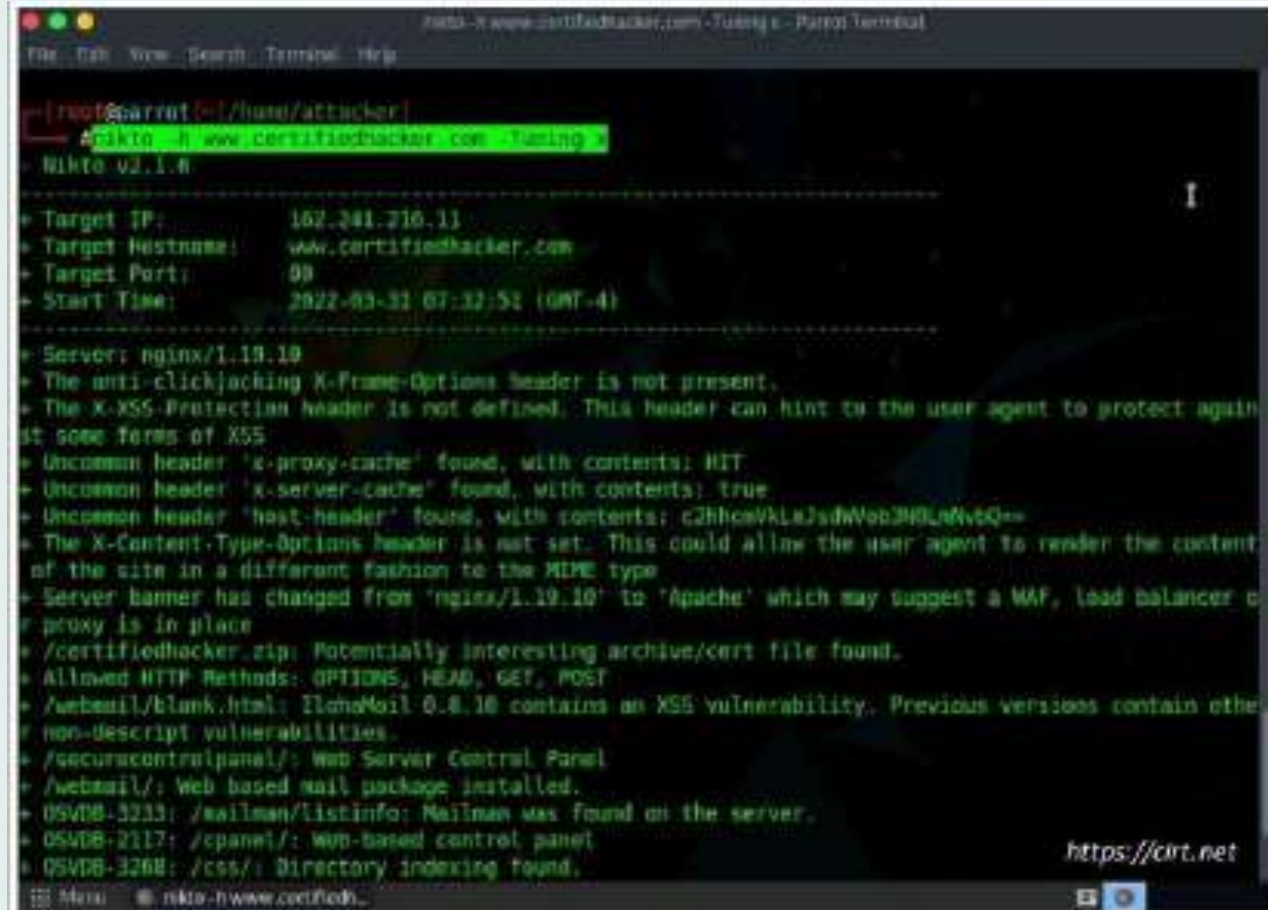
- Policy: NetworkScan_Pt
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: Today at 11:09 P
- End: Today at 11:27 P
- Elapsed: 17 minutes

Vulnerabilities

- Cri
- Hig
- Mit
- Lo
- Inf

Nikto

- ❑ Outil d'évaluation des serveurs web qui permet d'examiner les serveurs web afin de découvrir des problèmes potentiels et des vulnérabilités de sécurité



```
nikto -h www.certifiedhacker.com -Timing - Parrot Terminal
File Edit View Search Terminal Help

root@parrot:~/home/attacker#
nikto -h www.certifiedhacker.com -Timing
Nikto v2.1.6

+ Target IP: 162.241.216.11
+ Target Hostname: www.certifiedhacker.com
+ Target Port: 80
+ Start Time: 2022-03-31 07:32:52 (GMT-4)

+ Server: nginx/1.19.10
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS.
+ Uncommon header 'x-proxy-cache' found, with contents: HIT
+ Uncommon header 'x-server-cache' found, with contents: true
+ Uncommon header 'host-header' found, with contents: c3hHceVhLajsdWeb3N0LnVvcQ==
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Server banner has changed from 'nginx/1.19.10' to 'Apache' which may suggest a WAF, load balancer or proxy is in place
+ /certifiedhacker.zip: Potentially interesting archive/cert file found.
+ Allowed HTTP Methods: OPTIONS, HEAD, GET, POST
+ /webmail/blank.html: ELMail 0.8.10 contains an XSS vulnerability. Previous versions contain other non-descript vulnerabilities.
+ /securitecontrolpanel/: Web Server Control Panel
+ /webmail/: Web based mail package installed.
+ OSVDB-3233: /mailman/listinfo: Mailman was found on the server.
+ OSVDB-2117: /cpanel/: Web-based control panel
+ OSVDB-3268: /css/: Directory indexing found.

https://cirt.net
Nikto © nikto -h www.certifiedhacker.com
```

Autres outils d'évaluation de la sécurité



Qualys FreeScan

<https://www.qualys.com>



Acunetix Web Vulnerability Scanner

<https://www.acunetix.com>



Nexpose

<https://www.rapid7.com>



Network Security Scanner

<https://www.beyondtrust.com>



SAINT

<https://www.carson-saint.com>



beSECURE (AVDS)

<https://www.beyondsecurity.com>



Core Impact Pro

<https://www.coresecurity.com>



N-Stalker Web Application Security Scanner

<https://www.nstalker.com>



ManageEngine Vulnerability Manager Plus

<https://www.manageengine.com>



Nipper Studio

<https://www.titania.com>



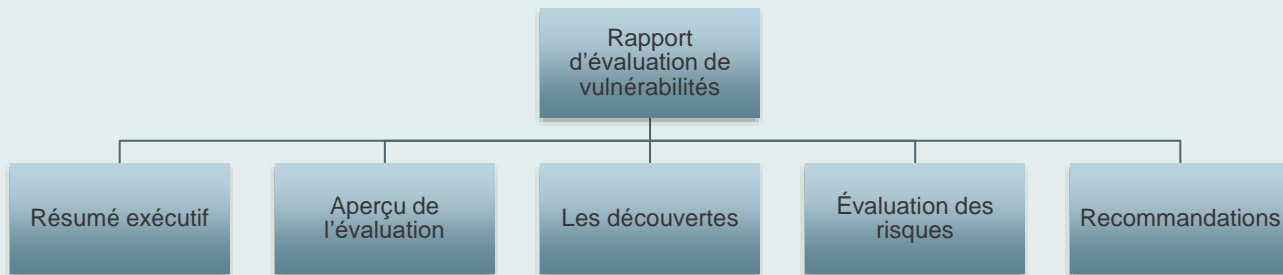
03

Rapport d'évaluation de vulnérabilités



Rapport d'évaluation de vulnérabilités

- ❑ Le rapport d'évaluation des vulnérabilités révèle les risques détectés après l'analyse d'un réseau.
- ❑ Il alerte l'organisation sur les attaques potentielles et propose des contre-mesures.
- ❑ Les informations disponibles dans le rapport sont utilisées pour corriger les failles de sécurité.



Contenu du Rapport

Résumé exécutif

Portée et objectifs de l'évaluation
Récit de test
Résumé des découvertes
Résumé de la remédiation

Les découvertes

Les hôtes scannés
Types de vulnérabilités identifiées
Informations détaillées sur les vuln
identifiées
Notes décrivant des détails
supplémentaires sur le résultat des
scans

Recommandations

Priorisation des mesures
correctives en fonction du
classement des risques
Plan d'action pour implémenter les
recommandations pour chaque
vulnérabilité identifiée
L'analyse des causes racines
Application de patche/ correctifs
Leçons retenues
Formations de sensibilisation
Implémentation d'analyse de
vulnérabilité périodique
Implémentation de politiques,
procédures et contrôles

Aperçu des évaluations

Méthodologie d'évaluation
Informations de scan
Informations sur la cible

Évaluation des risques

Classification des vuln basée sur le
niveau de risque
Les vulnérabilités potentielles
pouvant compromettre le système
ou les applications
Hôtes critiques avec vulnérabilités
sévère



THANKS!

Do you have any questions?

M1SSI@outlook.com

<https://master-ssi.jimdofree.com/>

