Parc d'Activités Schweitzer
26 rue du Bois Fossé
85300 CHALLANS
Tél. 02 51 49 31 31

espace technologie

FICHE CONSEILS

AUDIT CYBER SECURITE

POURQUOI UN AUDIT CYBERSECURITE EST INDISPENSABLE

Introduction - Ne pas confondre sécurité informatique et cybersécurité

Votre système informatique est installé par des techniciens et ingénieurs système et réseau. Ils sont formés par des écoles spécialisées et bénéficient de formation continue durant toute leur carrière. Ils possèdent de fortes compétences dans le domaine de la sécurité. Cependant, ils ne sont pas formés aux techniques utilisées par les Cybercriminels pour pénétrer et accéder aux données de votre système d'informations.

Exemple

Notre expert en CyberSécurité a découvert une faille de sécurité majeure sur un système informatique hautement sécurisé pourtant vérifié et contrôlé par plusieurs ingénieurs réseau.

La faille provenait d'un téléviseur de grande marque qui embarquait un logiciel (espion d'origine). Le pirate connaissait cette faille, il a pénétré le réseau par le logiciel du téléviseur, installé un logiciel d'enregistrement de frappe, repéré le serveur et récupéré le login et mot de passe administrateur.

A partir de ce moment, le pirate pouvait accéder ou (détruire, copier) toutes les données de l'entreprise, y compris les sauvegardes.

Seul un Expert en CyberSécurité formé aux techniques de cybercriminalité peut anticiper et découvrir ce type de failles de sécurité.

ESPACE TECHNOLOGIE COMPTE DESORMAIS DANS SON EFFECTIF UN SPECIALISTE EN CYBERSECURITE

❖ Profil de notre Responsable sécurité des systèmes d'informations

Doublement diplômé en Cyber sécurité

- **Mastère spécialisé cyber sécurité à Centrale Supélec**
  - L'école Française la plus reconnue en Cyber Sécurité
    - Ce mastère spécialisé a été classé 1er dans la catégorie « Télécoms, réseaux et sécurité des systèmes » du classement SMBG 2019
    - Label "Cyber Excellence" par le ministère de la défense
- **Mastère spécialisé cyber sécurité à IMT Atlantique**
- Préparation Norme ISO 27001
- Ingénieur Système et réseau

Parcours professionnel

Ingénieur système spécialisé dans les systèmes Windows/Linux et réseau(Firewall).

Passionné de cyber sécurité et formé aux dernières générations d'attaques cyber criminelles.

- **Depuis 2019:** Responsable Sécurité et cyber surveillance chez Espace Technologie
- **De 2015 à 2019** Espace Technologie en qualité d'ingénieur système et réseau.
- **De 2013 à 2015 :** Administrateur Système Linux chez un fournisseur d'accès Internet.

POURQUOI ESPACE TECHNOLOGIE A DECIDE DE CREER CE POSTE AU SEIN DE SON EQUIPE ?

Nous sommes très peu d'entreprises informatiques en France, (encore moins dans l'ouest) à posséder ce type de compétence, car la grande majorité des diplômés rejoignent les équipes de cyber Défense de l'armée.

Et pourtant :
Plus de 7 PME sur 10 ont ou vont subir une cyber attaque plus ou moins destructrice.

❖ Quelques Chiffres pour les entreprises de moins de 100 salariés

44% des entreprises de 9 à 49 salariés ont déjà subi une ou plusieurs **attaques ou tentatives** d'attaques informatiques.

On estime que ce chiffre passera à 77% en 2020.

En moyenne, il faut **6 mois** à une entreprise pour détecter une violation de ses données.

800 millions d'adresses email accompagnées de mots de passe circulent sur le Dark Web

Prévision : Une entreprise sera victime d'une attaque par un rançongiciel **toutes les 14 secondes** cette année

Le Groupe d' Assurance Hiscox déclare que 81 % des entreprises Françaises ont la plus mauvaise note Européenne en protection contre les risques Cybercriminels.

DESORMAIS NOUS SOMMES EN MESURE D'AUDITER VOTRE SYSTEME D'INFORMATION ET D'IDENTIFIER LES FAILLES UTILISEES PAR LES HACKERS POUR PENETRER VOTRE RESEAU.

Notre prestation consiste à simuler une cyber attaque et vous présenter le rapport complet.

Ce type de compétences très spécifique vient compléter notre gamme de service pour protéger le patrimoine informationnel des entreprises.

Yann BELZ dirigeant d'espace Technologie déclare :
« J'ai été impressionné des vulnérabilités que notre expert m'a montré sur différents systèmes d'informations, ce sont des failles connues uniquement des hackers et, bien sûr, non documentées.
Les meilleurs ingénieurs systèmes ne sont pas formés sur ces menaces et je suis fier que désormais nous fassions partie des rares sociétés informatiques Françaises capables d'apporter ce niveau de services.
C'est très important pour nos clients car, on ne peut protéger que ce que l'on connait»

COMMENT SE PASSE UN AUDIT CYBER SECURITE

Une fois notre spécialiste missionné, il travaillera à distance ou dans vos locaux. Il ne disposera d'aucune information concernant votre système d'informations. Un rapport vous sera remis après la prestation.

- **Le rapport répondra aux questions suivantes :**

- **Chapitre 1 - Les Fichiers**
  - Auriez-vous pu consulter les documents de l'entreprise ?
    - □ Oui □ Non
  - Auriez vous pu modifier les documents de l'entreprise ?
    - □ Oui □ Non
  - Auriez vous pu subtiliser des documents de l'entreprise ?
    - □ Oui □ Non
  - Auriez vous pu détruire des documents de l'entreprise ?
    - □ Oui □ Non

- **Chapitre 2 - Les Emails**
  - Auriez-vous pu consulter des emails de l'entreprise ?
    - □ Oui □ Non
  - Auriez-vous pu subtiliser des emails de l'entreprise ?
    - □ Oui □ Non
  - Auriez-vous pu détruire des emails de l'entreprise ?
    - □ Oui □ Non

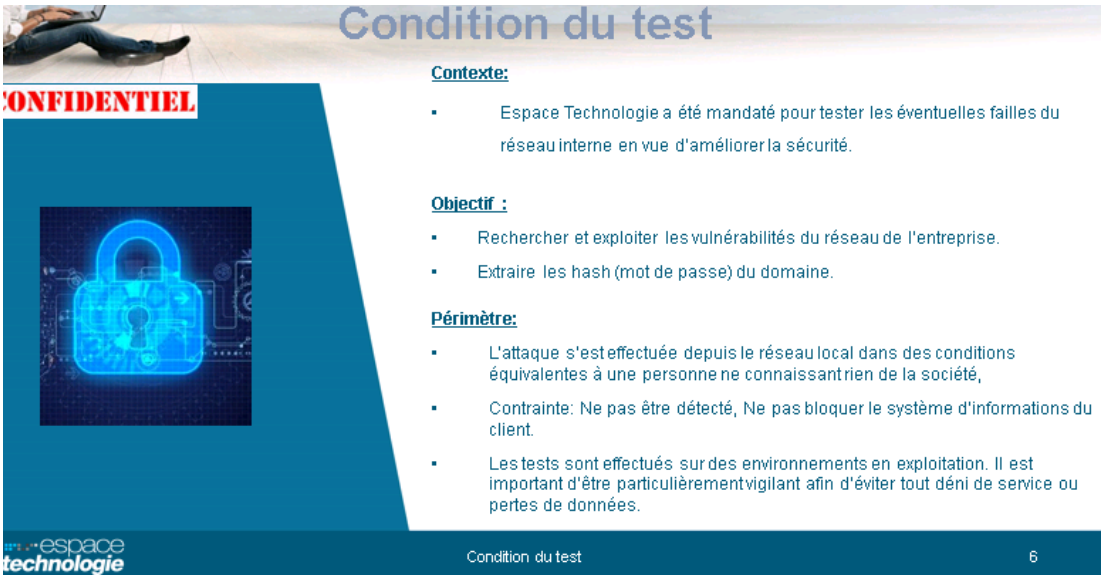
- **Chapitre 3 - Les logiciels métiers (ERP-CRM-PRODUCTION-PAYE)**
  - Auriez-vous pu accéder aux logiciels de l'entreprise ?
    - □ Oui □ Non
  - Auriez-vous pu modifier des données dans les logiciels de l'entreprise ?
    - □ Oui □ Non
  - Auriez-vous pu subtiliser des données des logiciels de l'entreprise ?
    - □ Oui □ Non
  - Auriez-vous pu détruire des données des logiciels de l'entreprise ?
    - □ Oui □ Non

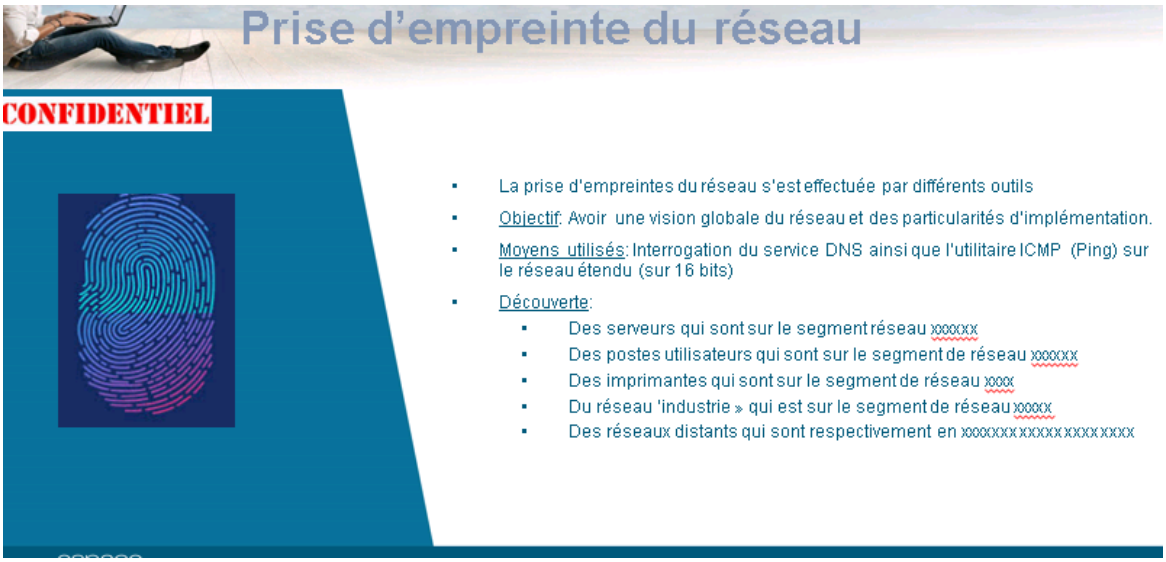
- **DESTRUCTION**

- Auriez-vous pu détruire toutes les données de l'entreprise ?
  - □ Oui □ Non
- Auriez-vous pu détruire les sauvegardes de l'entreprise ?
  - □ Oui □ Non

RAPPORT

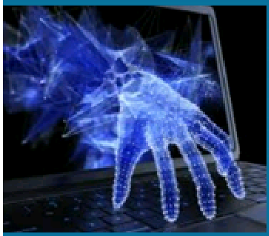
Quelques exemples de pages





Intrusion silencieuse

CONFIDENTIEL



- 1[er] objectif: Prendre le contrôle du contrôleur de domaine en étant le plus indétectable possible.

- L'attaque c'est déroulée en 3 points:

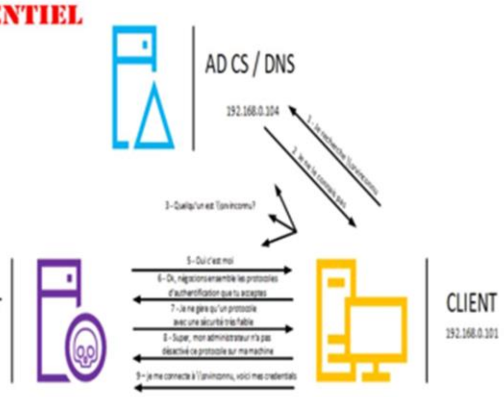
  - 1, Découverte d'une faille réseau/système
  - 2. Collecte des hash
  - 3. Déchiffrements des hash

Une fois en possession d'un compte Admin du domaine:

- Collecte de l'intégralité des comptes présents dans la base LDAP
- Lancement d'un déchiffrement global de tous les comptes.

Failles réseau

NTIEL



- Lorsqu'il s'agit de résoudre un nom en une IP sur un réseau Active Directory, trois protocoles sont utilisés : DNS, LLMNR et NBT-NS.

- LLMNR et NTB-NS sont deux protocoles utilisés afin de résoudre un nom en une adresse IP sur un réseau Active Directory.

- Dans ces conditions, un attaquant tentera de répondre à toutes les requêtes LLMNR/NBT-NS émises afin de rediriger un utilisateur vers un faux service (SMB par exemple) et ainsi récupérer le hash Net-NTLMv2 du compte associé. Ensuite l'attaquant tentera soit de casser le hash Net-NTLMv2 pour en extraire le mot de passe en clair ou bien rejouer le hash pour se connecter à un équipement (attaque PTH).

Déchiffrement des hash

CONFIDENTIEL

- Une fois le hash d'un probable administrateur récupéré, la nuit est mise à profit pour lancer le cassage de ce mot de passe:

Sur 331 comptes déclarés dans l'active Directory, 189 sont désormais déchiffrés.

[redacted]--ntds
[redacted]i1404ee:3eb3c3a555804f0042797302d
3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

Dont des comptes très important tel que:

NOM	PASSWORD
Administrator	[redacted]T

Désactiver LLMNR :	Désactivation NBT-NS :	Se proteger de WAPD
Ouvrez l'éditeur de stratégie de groupe locale: gpedit.msc	Il est possible de désactiver de manière plus globale ce paramètre via DHCP en utilisant	La méthode radicale consiste à **créer une entrée wpad dans host local**

La faille Bluekeep est une nouvelle vulnérabilité publiée cet été.
Actuellement un attaquant peut provoquer un crash de la machine a distance.
Certains groupes de hackeurs ont déjà développé un RCE (remote code exécution) afin de prendre la main sur la machine.

Dans peu de temps ce code sera public et les risques d'exploitation de cette vulnérabilité seront extrêmement élevé. (cf WANNACRY avec la faille EthernalBlue)

osoft Windows Remote Desktop Services 'CVE-2019-0708' Remote Code Execution Vulnerability (BlueKeep) - (Remote Active)		10.0 (High)	99%	3389/tcp
osoft Windows Remote Desktop Services 'CVE-2019-0708' Remote Code Execution Vulnerability (BlueKeep) - (Remote Active)		10.0 (High)	99%	3389/tcp

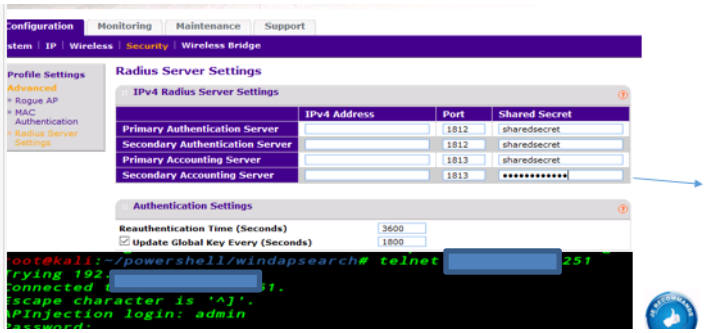
- ***Recommandations:***

Appliquer les dernières mises a jour de sécurité de Microsoft
Néanmoins actuellement les mises a jours proposées par Microsoft semblent ne pas corriger entièrement le problème

nerability		Severity	QoD	Host
osoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)		9.3 (High)	95%	[redacted]

Cette machine est vulnérable à la faille EthernalBlue, publiée en 2017
Un attaquant peut prendre le contrôle de la machine et ensuite procéder à une escalade de privilège afin de compromettre l'ensemble du domaine.
De plus, cette faille est largement utilisée dans le déploiement de ransomwares.

- ***Recommandations:***



Serveur

- Cette machine possède les comptes par défaut comme authentification.
- Une fois connecté, il est aisé pour un hacker d'afficher les mots de passes « secrets » cachés derrière les ronds noires.
- Cela m'a permis d'activer le service Telnet* et ainsi me connecter à cette machine.

Serveur

- La faille la plus importante sur ce serveur est la possibilité d'uploader ce que l'on souhaite.
- On peut notamment envoyer un code d'exécution pour prendre la main à distance.
- Heureusement le [redacted] est là pour empêcher l'exécution de code.
- Néanmoins un attaquant pourrait détruire le serveur en inversant les commandes « put » par delete

UN AUDIT CYBER SECURITE EST INDISPENSABLE AU MOINS UNE FOIS DANS LA VIE DE VOTRE ENTREPRISE

Plus d'informations sur nos prestations contactez-nous :

ESPACE TECHNOLOGIE
Parc d'Activités Schweitzer
26 rue du Bois Fossé - BP 147
85301 CHALLANS Cedex

Tél. 02 51 49 31 31

www.espace-technologie.com
contact@espace-technologie.com