UNIVERSITE UMET BURKINA

Titre de l'exposé : **Les Entreprises du Burkina Faso face aux Cybermenaces**

Professeur : M. Tapsoba Abram

Membre du groupe

L3 - Sécurité des systèmes informatiques et industriels

KABRE Gérald

Année académique : 2024 – 2025

Sommaire

Introduction

À l'heure où le Burkina Faso accélère sa transition numérique, ses entreprises se développent dans des secteurs stratégiques. Cette digitalisation, bien qu'indispensable à la modernisation, ouvre la porte à la cybercriminalité. Dans un contexte où les attaques informatiques deviennent de plus en plus sophistiquées et fréquentes, les entreprises burkinabè, peu préparées, se retrouvent exposées à des risques majeurs. Ce projet vise à dresser un état des lieux des défis de cybersécurité nationaux, identifier les failles exploitées par les hackers, proposer des solutions basées sur les systèmes de détection et de prévention d'intrusion (IDS/IPS), et explorer l'apport de l'intelligence artificielle (IA) dans la protection des systèmes d'information. L'objectif est d'offrir une démarche réaliste afin d'aider les entreprises à mieux se défendre.

I. Défis à relever

Les entreprises burkinabè, engagées dans une digitalisation accélérée, se heurtent à des obstacles multiples que l'on peut regrouper comme suit :

1. Infrastructures techniques obsolètes

De nombreuses structures utilisent encore des systèmes d'exploitation piratés non mis à jour, des routeurs sans correctifs récents, et des applications web mal codées, parfois dépourvues de certificat HTTPS. Beaucoup ne disposent ni de pare-feux performants, ni de centre de supervision de sécurité (SOC), exposant leur réseau aux intrusions.

Cas concret : En mai 2017, plusieurs sites web officiels du gouvernement burkinabè ont été compromis simultanément par des hackers étrangers. Les pirates ont infiltré un serveur commun, modifié les pages d'accueil afin d'afficher un message de prise de contrôle et rediriger vers leur page Facebook. Cette attaque a porté atteinte à la crédibilité des institutions et exposé des données sensibles.

2. Faible culture de cybersécurité et déficit de compétences humaines

La sensibilisation aux risques demeure insuffisante, avec des employés utilisant souvent des mots de passe faibles et ignorant les bonnes pratiques face aux cyberattaques. Par ailleurs, le Burkina Faso souffre d'une pénurie d'experts en cybersécurité, aggravée par un manque de formation locale et un exode des talents. En conséquence, les entreprises manquent de ressources pour auditer leurs systèmes et anticiper les menaces.

3. Contraintes budgétaires et environnement réglementaire en construction

La cybersécurité est souvent considérée comme un coût, ce qui limite les budgets alloués aux audits et à l'acquisition d'outils efficaces comme les antivirus professionnels, pare-feux

avancés ou solutions SIEM. Malgré l'existence d'une législation sur la protection des données, sa mise en œuvre est incomplète, les sanctions peu dissuasives, peu d'entreprises se confirment pleinement aux normes et la gouvernance numérique reste encore peu développée.

4. Vulnérabilités propres au contexte local

Le pays dépend fortement des technologies importées, souffre parfois d'instabilité dans les infrastructures télécoms, et évolue dans une région marquée par des tensions géopolitiques (cybercriminalité transfrontalière, désinformation, sabotage numérique).

II. Failles de sécurité exploitées

Les entreprises burkinabè, sont aujourd'hui confrontées à des failles de sécurité multiples rendant leurs systèmes d'information vulnérables. Ces failles peuvent être regroupées en plusieurs catégories :

1. Failles techniques

De nombreuses structures utilisent encore des systèmes obsolètes, privés de mises à jour et donc exposés à des failles connues. Ensuite, les mots de passe faibles sont monnaie courante et rarement modifiées. De plus, de nombreux équipements (serveurs, routeurs, caméras IP) conservent leurs configurations par défaut, facilitant leur compromission. Enfin, l'absence de chiffrement des données sensibles, qu'elles soient stockées ou transmises, expose gravement les informations confidentielles à tout incident de sécurité.

2. Failles humaines

Au Burkina Faso, le facteur humain constitue une faille majeure en cybersécurité. Les attaques par ingénierie sociale sont fréquentes : les cybercriminels manipulent les employés en profitant de leur manque de vigilance. Ce problème est accentué par l'absence de formation continue, car peu d'entreprises organisent des sessions de sensibilisation à la cybersécurité. Par ailleurs, la gestion des accès est souvent négligée : des stagiaires ou techniciens disposent parfois des mêmes privilèges que les administrateurs réseau, ce qui accroît considérablement les risques d'intrusion ou d'erreur interne.

3. Failles organisationnelles

La majorité des entreprises burkinabè ne disposent pas de supervision continue de leur système d'information. L'absence de centre opérationnel de sécurité (SOC) rend la détection d'intrusions extrêmement difficile, voire impossible en temps réel. De plus, l'absence de journalisation et d'audit des connexions empêche de retracer les actions

menées par les utilisateurs ou les attaquants, compliquant fortement toute tentative d'enquête après une attaque.

Cas concret – Campagne d'escroquerie par SMS (Phishing) au Burkina Faso : Actuellement, une vague de SMS frauduleux cible la population burkinabè. Ces messages annoncent de fausses bonnes nouvelles comme : "Vous avez gagné 500 000 FCFA à un tirage Orange Money", ou encore "Félicitations, vous avez trouvé un emploi ! Cliquez ici pour confirmer : [URL]". En réalité, le lien redirige vers un site web contrefait (imitation d'Orange, …) qui demande à la victime ses informations personnelles. Une fois ces données saisies, les cybercriminels les utilisent pour vider les comptes de la victime, voler son identité ou envoyer le lien à d'autres contacts, propageant ainsi la campagne à grande échelle.

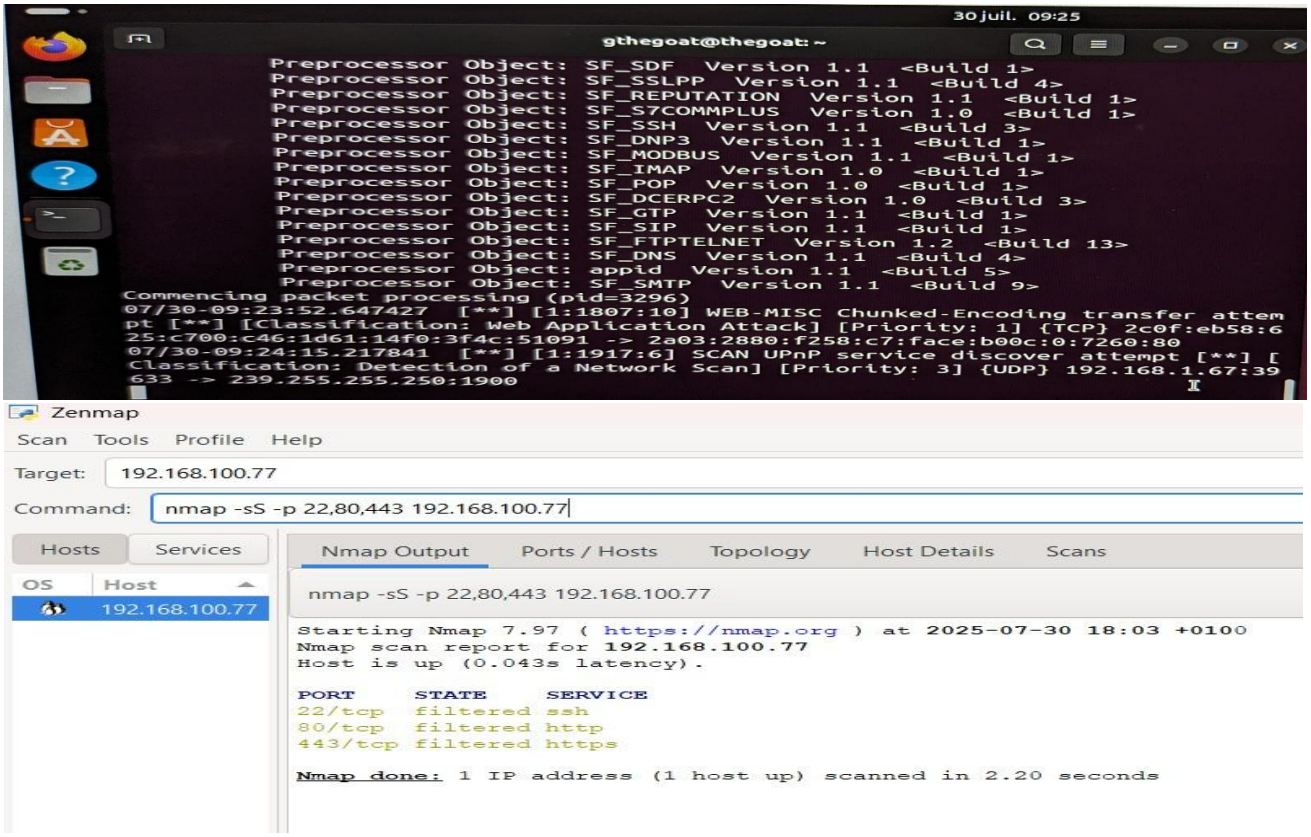
Failles exploitées dans ce cas : De prime abord, nous avons le manque de sensibilisation des utilisateurs, qui ne sont pas formés à identifier les tentatives d'arnaque. Les protections sur les smartphones restent faibles, avec peu ou pas d'antivirus, des navigateurs non sécurisés, et une absence d'alerte lors du clic sur des liens suspects. De plus, les opérateurs ne filtrent pas les numéros ou URLs frauduleux en amont, et aucun système IDS/IPS mobile n'est en place pour surveiller et bloquer les connexions vers des sites malveillants.

III. Solutions IDS/IPS

Pour protéger les réseaux burkinabè contre les cyberattaques, il est indispensable d'utiliser des systèmes de détection et de prévention d'intrusion (IDS, IPS). IDS (Intrusion Detection System) : système de détection qui analyse le trafic réseau pour identifier des activités suspectes. Il ne bloque pas l'attaque mais alerte l'administrateur. IPS (Intrusion Prevention System) : système de prévention qui va bloquer automatiquement les menaces en temps réel. Il agit comme un pare-feu intelligent, capable d'interrompre les connexions malveillantes. Comme exemples d'IDS/IPS nous avons : snort, suricata.

Cas pratique de mise en œuvre IDS/IPS avec Snort sur Ubuntu : Dans le cadre d'une simulation d'attaque réseau, nous avons mis en place un environnement de test en virtualisant une machine sous Ubuntu. Nous y avons installé Snort.

Étape 1 – Mode IDS (Intrusion Detection System) :
Nous avons d'abord configuré Snort en mode IDS, afin de surveiller le trafic sans le bloquer. Ensuite, nous avons simulé une attaque en lançant un scan réseau Nmap depuis une autre machine. Résultat : Snort a détecté le scan et a généré une alerte, ce qui prouve que le système identifie les comportements suspects en temps réel.



Étape 2 – Passage en mode IPS (Intrusion Prevention System) :
Par la suite, nous avons relancé Snort en mode IPS, ce qui lui permet non seulement de détecter les attaques, mais aussi de les bloquer automatiquement. Nous avons relancé le scan Nmap. Résultat : Snort a cette fois bloqué le scan en temps réel, empêchant l'attaquant d'obtenir des informations sur le réseau.

Exemple concret applicable au Burkina Faso

Prenons l'exemple d'une mairie locale ou d'un hôpital public au Burkina Faso disposant d'un réseau interne mal sécurisé. Ces institutions manipulent des données sensibles (état civil, informations médicales, données financières), souvent sans supervision de sécurité réseau.

Solution : nous recommandons de déployer des solutions IDS/IPS telles que Snort ou Suricata sur un serveur dédié. Ces outils permettent de détecter diverses activités suspectes, notamment les scans de ports, les connexions vers des IP malveillantes… Lorsqu'une tentative de compromission est détectée, comme un phishing, malware ou accès non autorisé, l'IPS bloque automatiquement la connexion, limitant les risques d'intrusion. Ces solutions sont peu coûteuses, compatibles avec le matériel existant, personnalisables selon les besoins, et peuvent être administrées par des techniciens locaux, facilitant ainsi leur maintenance et adaptation aux menaces.

IV. Automatisation IA dans les systèmes d'information

L'intégration de l'IA dans les systèmes d'information offre de nombreuses opportunités d'automatisation en cybersécurité. L'IA permet une sécurité proactive grâce à la détection d'anomalies comportementales, la prédiction des tentatives d'intrusion, et la classification automatique des menaces. Elle optimise également la gestion des incidents en automatisant le triage des alertes, la réponse d'urgence et l'investigation forensique assistée. Sur le plan opérationnel, l'IA facilite la gestion automatique des vulnérabilités, l'orchestration des mises à jour sécuritaires, et l'optimisation des politiques de sécurité.

Exemple concret : Détection d'attaque interne chez Capital One (États-Unis, 2019) Capital One, une grande banque américaine, a été victime d'une attaque interne majeure où un individu a exploité une vulnérabilité pour accéder illégalement à plus de 100 millions de dossiers clients. Suite à cet incident, Capital One a renforcé sa sécurité en intégrant des solutions d'IA dans son SOC (Security Operations Center). Un système basé sur le machine learning analyse en continu les logs réseau et les comportements des utilisateurs pour détecter des anomalies, comme des accès inhabituels à des heures décalées, des transferts massifs de données ou des requêtes suspectes sur les bases de données. Par exemple, l'algorithme a pu identifier rapidement qu'un compte utilisateur faisait des requêtes répétées et volumineuses vers des serveurs sensibles à une heure tardive, un comportement déviant par rapport à la normale. Le système a automatiquement isolé le compte, bloqué les requêtes, et envoyé une alerte immédiate aux analystes de sécurité. Cette automatisation a permis de réduire le temps de détection et de réponse de plusieurs heures à quelques minutes, limitant ainsi l'impact de l'attaque.

Conclusion

La montée en puissance de la digitalisation au Burkina Faso expose les entreprises à des cybermenaces toujours plus sophistiquées, amplifiées par des infrastructures insuffisantes, un manque de ressources humaines qualifiées et une sensibilisation limitée. Face à ces défis, il est crucial d'adopter une approche intégrée combinant déploiement de solutions IDS/IPS, et l'exploitation des capacités de l'IA pour automatiser la détection, la prévention et la réponse aux attaques. En renforçant les compétences locales, en améliorant la gouvernance numérique, et en sensibilisant l'ensemble des acteurs, le Burkina Faso pourra non seulement mieux protéger ses systèmes d'information, mais aussi soutenir sa transformation numérique de manière sécurisée et durable. Ce projet met ainsi en lumière les leviers essentiels pour bâtir une cybersécurité robuste, adaptée au contexte national, et garante de la confiance dans l'économie numérique émergente.