Rapport d'Énumération et Analyse de Services Réseau

Ce rapport présente l'analyse et l'énumération de trois services réseau couramment rencontrés lors d'un audit de sécurité : SMTP, SNMP et RPC. Pour chaque service, nous décrivons son rôle, les commandes à utiliser pour l'énumération, des exemples de résultats et une évaluation de l’impact potentiel en termes de sécurité.

1. SMTP (Simple Mail Transfer Protocol)

• Port : 25/TCP • Fonction : Permet l’envoi d’emails entre serveurs de messagerie. ### Commandes utilisées : nmap -p 25 --script=smtp-commands,smtp-enum-users,smtp-open-relay telnet 25 ### Exemple de résultats : 220 mail.local ESMTP Postfix VRFY admin → User exists EXPN → Liste des membres d’un alias ### Impact : Un serveur SMTP mal configuré peut permettre : - L’énumération d’utilisateurs valides (brute force facilité). - Le relais de mails non autorisés (SPAM, phishing).

2. SNMP (Simple Network Management Protocol)

• Port : 161/UDP • Fonction : Utilisé pour la supervision réseau et la gestion des périphériques. ### Commandes utilisées : nmap -sU -p 161 --script=snmp-info,snmp-brute,snmp-processes snmpwalk -v2c -c public ### Exemple de résultats : SNMPv2-MIB::sysName.0 = STRING: server01 SNMPv2-MIB::hrSystemUptime.0 = Timeticks: (1234567) 2 days, 8:34:56 ### Impact : - Si la communauté par défaut (public/private) est active, il est possible de récupérer : • Liste des utilisateurs • Processus en cours • Interfaces réseau - Peut faciliter une attaque plus poussée (pivot, bruteforce, etc.).

3. RPC (Remote Procedure Call)

• Ports : 135/TCP (Windows), 111/TCP-UDP (Linux/Unix) • Fonction : Permet à un programme d’exécuter une procédure sur une machine distante. ### Commandes utilisées : nmap -p 135 --script=msrpc-enum (Windows) nmap -p 111 --script=rpcinfo (Linux) rpcinfo -p ### Exemple de résultats : program 100000 version 2 ready and waiting MSRPC: Host is running Windows RPC service ### Impact : - Fuite d’informations sensibles : services disponibles, utilisateurs, partages. - Exploits connus (exemple : EternalBlue via MSRPC sur Windows).

Conclusion : L’énumération de ces services (SMTP, SNMP, RPC) révèle souvent des informations critiques si les configurations ne sont pas sécurisées. Une attention particulière doit être portée sur la désactivation des fonctionnalités non utilisées, le changement des identifiants par défaut et la mise à jour régulière des systèmes.