#DETECTION PING

alert icmp any any -> any any (msg:"Ping détecté"; sid:1000001; rev:1;)

#DETECTION SCAN DE PORTS

alert tcp any any -> $HOME_NET any (msg:"Possible TCP Port Scan"; flags:S; sid:1000002; rev:1;)

alert udp any any -> $HOME_NET any (msg:"Possible UDP Port Scan"; sid:1000003; rev:1;)

#DETECTION DDos

alert udp any any -> $HOME_NET any (msg:"POTENTIEL UDP DDos UDP - Flood"; threshold: type both, track by_dst, count 100, seconds 1; sid:1000004; rev:1;)

alert tcp any any -> $HOME_NET any (msg:"POTENTIEL TCP DDos UDP - SYN Flood"; flow:to_server; flags:S; threshold: type both, track by_dst, count 50, seconds 1; sid:1000005; rev:1;)

#DETECTION EXFILTRATION DE DONNEES

#Règle FTP

alert tcp $HOME_NET any -> any any (msg:"EXFIL FTP - Gros volume"; flow:to_server,established; byte_test:4,>,1000000,0,relative; classtype:attempted-recon; sid:1000006; rev:1;)

#Règle SMB

alert tcp $HOME_NET any -> any any (msg:"EXFIL SMB - Gros volume"; flow:to_server,established; byte_test:4,>,1000000,0,relative; classtype:attempted-recon; sid:1000007; rev:1;)

#DETECTION DE CONNEXION RDP ET SSH

#Règle RDP

alert tcp any any -> any 3389 (msg:"Tentative de connexion RDP détectée"; sid:1000008; rev:1;)

#Règle SSH

alert tcp any any -> any 22 (msg:"Tentaive de connexion SSH détectée"; sid:1000009; rev:1;)

#DETECTION DE MALWARES

#Téléchargement de fichiers .exe

alert http any any -> any any (msg:"Téléchargement fichier EXE détecté -Possible Malware"; content:".exe"; http_uri; nocase; threshold: type threshold, track by_src, count 1, seconds 10; sid:1000010; rev:1;)

#Téléchargement de fichiers .zip

alert http any any -> any any (msg:"Téléchargement fichier ZIP détecté"; content:".zip"; http_uri; nocase; threshold: type threshold, track by_src, count 1, seconds 10; sid:1000011; rev:1;)

#Téléchargement de fichiers .rar

alert http any any -> any any (msg:"Téléchargement fichier RAR détecté"; content:".rar"; http_uri; nocase; threshold: type threshold, track by_src, count 1, seconds 10; sid:1000012; rev:1;)

#Téléchargement de fichiers .dll

alert http any any -> any any (msg:"Téléchargement fichier DLL détecté"; content:".dll"; http_uri; nocase; threshold: type threshold, track by_src, count 1, seconds 10; sid:1000013; rev:1;)

#DETECTION DE PHISHING

alert http any any -> any any (msg:"Phishing détecté"; flow:to_client,established; content:"Connexion"; nocase; content:"Mot de passe"; sid:1000014; rev:1;)

#DETECTION INJECTION SQL

#SQLi - tautlology OR 1=1

alert http any any -> any any (msg:"SQLi attempt - tautology OR 1=1"; flow:to_server,established; http.uri; content:" OR 1=1"; nocase; classtype:web-application-attack; sid:1000015; rev:1;)

#SQLi - UNION SELECT

alert http any any -> any any (msg:"SQLi attempt - UNION SELECT"; flow:to_server,established; http.uri; pcre:"/union\s+select/i"; classtype:web-application-attack; sid:1000016; rev:1;)

#SQLi - quote and comment

alert http any any -> any any (msg:"SQLi attempt - SQL comment or quote"; flow:to_server,established; http.uri; pcre:"/('|%27|--|%23)/Ui"; classtype:web-application-attack; sid:1000017; rev:1;)

#DETECTION XSS

alert http any any -> any any (msg:"BANKING - XSS attempt detected"; flow:to_server,established; http.uri; pcre:"/<script>/Ui"; classtype:web-application-attack; sid:1000018; rev:1;)

#DETECTION C&C DNS

alert dns any any -> any any (msg:"Possible C&C DNS request"; dns.query; content:".maliciousdomain.com"; classtype:trojan-activity; sid:1000019; rev:1;)a