Syn Flooding:
Detection:The generic symptom of SYN Flood attack to a web site visitor is that a site takes a long time to load, or loads some elements of a page but not others.
If you suspect a SYN Flood attack on a web server, you can use netstat command to check the web server connection requests that are in "SYN_RECEIVED" state.
netstat -tuna | grep :80 | grep SYN_RECV
If it shows numerous connections with this state, the server could be under SYN Flood attack.
Configure Firewall to prevent syn Flooding:iptables -A INPUT -p tcp --syn -m limit --limit 1/s --limit-burst 3 -j RETURN
–limit 1/s: Maximum average matching rate in seconds
–limit-burst 3: Maximum initial number of packets to match
Countermeasures:

Syncookies:
enable
2.configure terminal
3.parameter-maptypeinspect-zonezone-pmap-name
4.tcpsyn-floodrateper-destinationmaximum-rate
5.max-destinationlimit
6.exit
7.zonesecurityzone-name
8.protectionparameter-map-name
9.exit
10.showparameter-maptypeinspect-zonezone-pmap-name
11.showzonesecurity
12.showpolicy-firewallstatszonezone-name

Pour utiliser la commande ifconfig, il faut être root
Bloquer l'interface de boucle locale provoque des problèmes dans le réseau
Les configurations faites avec ifconfig ne sont pas permanentes.
Pour une configuration permanente, on utilise le fichier /etc/network/interfaces

Résolution de noms

M1 : Localement, on utilise le fichier /etc/hosts
M2 : On utilise un serveur DNS

Remarques:

La recherche de résolution se fait d'abord localement ensuite au serveur DNS.
Pour changer cet ordre, on utilise le fichier de configuration /etc/host.conf
Par défaut, les machines ne répondent aux pings sur broadcast.
--savoir si notre machine répond ou non aux pings sur broadcast :
$cat /proc/sys/net/ipv4/icmp_ignore_broadcast
Si le résultat de cette manipulation est 1, alors elle répond sinon elle ne répond pas
--faire en sorte que notre machine réponde aux pings sur broadcast (non permanente)
sudo echo 0> /proc/sys/net/ipv4/icmp_ignore_broadcast
----faire en sorte que notre machine réponde aux pings sur broadcast (permanente)
Fichier /etc/sysctl.conf
--écrire un script qui prend l'adresse d'un réseau en ligne de commande et ping tout un réseau
$nano pingBroadcast
--script

```
Set `echo $1|tr"."" " $2|tr"."" " $3|tr"."" "s`
for i in `seq 255`
        do
                if ping $1.$2.$3.$i &>dev/null
                        then echo 192.168.1.$1
                fi
        done
```

--exécuter le script
$chmod u+x pingBroadcast
$ ./pingBroadcast

Attaque TCP: SYN Flooding

•But :
–Attaque de déni de service
–Empêcher la machine d'accepter de nouvelles connexions
•Principe :
–Créer des connexions semi-ouvertes
–La machine cible doit attendre la fin du processus de connexion
–Elle maintient ses ressources à disposition (non libération)
–On sature la liste d'attente (waiting-list)
•Conséquences :
–Tous les services TCP deviennent indisponibles
•Caractéristiques :
–Les paquets TCP SYN ne sont pas forcement tracés
–Le réseau n'est pas saturé de trames ICMP facilement identifiables comme dans les attaques ECHO flooding ou ECHO smurfing

Firewall linux: netfilter (outil de gestion: iptables)

L'outils iptables contient trois tables : filter, nat et mangle.
1) La table filter : Elle est la table par défaut et contient les de règles de filtrage

- 3 chaines :
  INPUT : les entrants
  OUPUT : les sortants
  FORWARD : les passants
- 4 targets :
  ACCEPT : accepte les paquets
  REJECT : rejet avec retour à l'expéditeur
  DROP : refus brut des paquets sans retour
  DENY ... LOG : logger les paquets sur la sortie standard

2) La table nat : Elle permet la translation d'@IP et de port

- 2 chaines :
  PREROUTING : amont parefeu
  POSTROUTING : aval du parefeu
- 3 targets :
  DNAT : IP de destination
  SNAT : IP source
  MASQUERADE : simule une gateway

3) La table mangle : Elle permet la modification et le marquage des paquets

- 3 targets :
  TOS : type de service (type of service)
  TTL : durée de vie (time to live)
  MARK : marquer les paquets (taggage)
  SECMARK : marquage de sécurité (pour outils de sécurité type SE Linux)
  CONNSECMARK : copie d'un cas de sécurité

Les principales options de iptables
-L : liste les règles (--line-numbers : numéros de règles)
-t : type (NAT...)
-nL : pas de résolution de nom pour éviter les problèmes DNS
-v : nombre et taille de paquets accepté/refusé

Actions sur les chaines
-A : ajout de règle à une chaine (-A INPUT)
-D : suppression de règle (-D INPUT 1 - numéro de la règle dans la chaine INPUT)
-R : remplace la règle (-R INPUT)
-I : insertion d'une règle (sans chiffre au début de la chaine (ex: INPUT 1)
-F : flush les règles pour une chaine (-F INPUT)
-N : création de chaîne
-X : drop de chaine personnelle
-P : définition de la policy d'une chaine (par défaut - ex: -P INPUT DROP)
Caractéristiques
-p : protocole (-p tcp)
-s : la source (ip, réseau)
-d : la destination (ip réseau)
-j : action à faire (DROP/ACCEPT)
-d : la destination (ip, réseau)
-i : interface d'entrée (eth0...)
-o : interface de sortie
--sport : port source
--dport : port de destination
-m multiport --sport 80,443 : plusieurs ports
-t : type (NAT...)
Filtrage par état de paquet
NEW : 1er paquet d'une connexion
ESTABLISHED : paquet à une connexion déjà établie
RELATED : paquet en relation avec une connexion déjà rétablie (FTP)
INVALID : paquet invalide soit pour la taille ou autre

--laisser passer la communication dans le sens retour si la communication a déjà état établie
$iptables -A INPUT -p tcp -m state - - state RELATED, ESTABLISHED -j ACCEPT

3/
iptables -A INPUT -m state –state RELATED,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -m state –state RELATED,ESTABLISHED -j ACCEPT

Exercices sur iptables

--afficher la liste des règles de la table filter
$iptables -L **ou** $iptables -t filter -L
--afficher la liste des règles accompagnée du numéro de l règle de la table filter
$iptables -L - -line-numbers **ou** $iptables -t filter -L - -line-numbers
--afficher la liste des règles de la table nat
$iptables -t nat -L
--afficher la liste des règles accompagnée du numéro de l règle de la table nat
$iptables -t nat -L - -line-numbers
--utiliser comme politique par défaut DROp pour les 3 chaines de la table filter
$iptables -P INPUT DROP
$iptables -P OUTPUT DROP
$iptables -P FORWARD DROP
--autoriser tous les paquets icmp en entrée
$iptables -I INPUT -p icmp -j ACCEPT
$iptables -I OUTPUT -p icmp -j ACCEPT
--accepter uniquement les pings du réseau 192.168.188.0/24
$iptables -I INPUT -p icmp -s 192.168.188.0/24 -j ACCEPT
--bloquer l'accès à facebook pendant entre 8h et 18h
1E: chercher l'@IP de facebook
Si facebook a une seule adresse IP : $dig www.facebook.com +short
Si facebook a plusieurs adresses IP : $whois @IP_facebook
2E: bloquer le trafic tcp de facebook
$iptables -I OUTPUT -p tcp -m iprange - - dest-range @debut-@fin -m time - -timestart 8:0 - - timestop 18:0 -j ACCEPT
--changer l'@IP des paquets qui vont sortir du firewall par l'interface eth1 en 10.10.10.1
$iptables -t nat -A PREROUTING -I eth1 -p tcp –dport 25 -j DNAT 10.10.10.1
--sauvegarde la configuration du firewall avec l'heure de sauvegarde:
$iptables-save > monFichier. `date+%F`
--restaurer le contenu
$iptables-restore <monFichier

Attaque IP : Source Routing

•La méthode de détournement initiale consistait à utiliser l'option source routing du protocole IP.

•Cette option permettait de spécifier le chemin à suivre pour les paquets IP, à l'aide d'une série d'adresses IP indiquant les routeurs à utiliser

•En exploitant cette option, le pirate peut indiquer un chemin de retour pour les paquets vers un routeur sous son contrôle.

•Solution: c'est simple !!!!

–Désactiver la fonction de "source-routing" sur les paquets IP

•Sur toutes les machines, sur tous les routeurs

•Option devenue quasi-inutile et dangereuse

•Malheureusement, ce n'est pas toujours le réglage par défaut

Attaque TCP: SYN Flooding

Cas linux : contrer l'attaque

- echo 1 > /proc/sys/net/ipv4/tcp_syncookies
  – La machine ne garde pas en mémoire les demandes de connexion semi-ouverte tant qu'elle n'a pas reçu la confirmation ACK
- Echo 1024 > /proc/sys/net/ipv4/tcp_max_syn_backlog
  – On positionne à 1024 le nombre maximum de SYN_WAIT
- echo 1 > /proc/sys/net/ipv4/conf/all/rp_filter
  – Enfin, la variable rp_filter permet de vérifier qu'un paquet arrive bien par l'interface sur laquelle il devrait arriver (éviter l'IP spoofing)

Attaque TCP: SYN Flooding

- La machine A envoie une demande de connexion TCP à la machine B
  – paquet SYN
  – La trame TCP est encapsulé dans un paquet IP avec une fausse adresse
- La machine B répond à la demande
  – Paquet SYN/ACK
  – Attend une confirmation d'ouverture qui n'arrivera jamais
- La connexion reste semi-ouverte pour un temps limité mais très grand devant la capacité des réseaux
- La machine A recommence avec
  – un grand nombre de demandes fabriquées
  – de fausses adresses (sources variées)

4/
Iptables –t filter –A INPUT –p TCP –dport 22 –j ACCEPT
Iptables –t filter –A INPUT –p TCP –dport 53 –j ACCEPT
OU
Iptables –t filter –A INPUT –p TCP –dport 22,53 –j ACCEPT

5/
iptables -A INPUT -p tcp --syn -m limit --limit 1/s --limit-burst 3 –j ACCEPT

–limit 1/s: Maximum average matching rate in seconds
–limit-burst 3: Maximum initial number of packets to match

	EXPLICATION	MEASURES DE SECURITY	Outils
ARP POISONING	Créer de fausses entrées dans les caches ARP. 1E: faire croire à A que je suis B : ârpspoof -t machineA machineB 2E: résoudre le problème de la couche 2 : $iptables -t nat -A PREROUTING -p tcp –dport 22 -j DNAT –to @IP_pirate	-installer arpwatch -utiliser des @mac statiques -DAI -DHCP snooping. - Nids	Ettercap: $ettercap -G
MAC flooding	Envoyer des @MAC aléatoires pour saturer la table CAMdu switch. Ceci le force à se comporter comme un hub $macof -i eth0	Utiliser le port-security -limiter le nombre d'@mac par port -si dépassement, spécifier l'action à faire	Ettercap: $ettercap -G
switch spoofing	Utiliser le protocole DTP pour transmettre un port en mode trunk. Ceci permet au pirate de récupérer tous les paquets VLAN	Configurer les ports d'accès aux machinesen mode access	Yersinia
Double etiquettage	Utilizer deux étiquettes pour accéder à d'autres hôtes	Obliger l'étiquetatage de tous les paquets Changer le VLAN par défaut	Scapy
Cisco Discovery Protocole CDP	CDP permet à un équipement CISCO d'avoir des infos sur les autres équipements CISCO directement connectés	Désactiver le protocole CDP sur tous les équipements #no cdp run	
DHCP	Envoyer plusieurs DHCPDiscovery pour : -Épuiser des @IP (stanvation) -Faux serveur DHCP(rogne)	DHCP spoofing Se baser sur le nombre de requêtes Eviter les faux serveurs DHCP	serinia
STP spoofing	Transformer son proper switch en switch root en lui donnant une priorité minimale	Si le BPDUgward est activé sur un port Il faut activer gward root si pour un port gward root est activé	
Attaque VLAN Hopping basique	l'envoi d'une trame forgée avec un tague 802.1Q. L'intérêt est de pouvoir discuter avec des cibles membres d'un VLAN déférent du siens	ne pas utiliser des protocoles comme DTP	
PING DE LA MORT	-Il s'agit d'un paquet de taille supérieure à la longueur maximum (65536) d'un paquet IP. -Lorsqu'un paquet IP est trop long pour pouvoir passer, celui-ci est segmenté en fragments. Dans certaines piles IP, une fois réassemblé la partie en trop peut déborder de l'espace mémoire prévu et corrompre ainsi le code du noyau, provoquant une instabilité du système.	- Les dernières versions des noyaux Linux sont immunisées. - Il est conseillé de réassembler les fragments de paquets au niveau du firewall.	
TEARDROP	-Cette attaque est assez similaire à celle du Ping de la mort. -Les paquets fragmentés se chevauchent au lieu de se réassembler bout-à-bout.	//	
ICMP Sweep	l'envoi d'une série de paquets ICMP request à un ensemble de machines pour découvrir les machines actives		Nmap –Zenmap –Fping –Netcat –Superscan
ICMP FLOODING	– La machine cible passe tout son temps à répondre à des requêtes ICMP. *But du ICMP Flooding :* – Rendre un ou plusieurs services inaccessibles ; – Rendre un réseau totalement inaccessible .	- Désactiver le forward ICMP_ECHO sur les routeurs. - Utiliser des contrôles de débit • Ex : 3 ICMP_ECHO / REPLY par second • Liste noire dynamique (interdiction pendant "x" minutes)	
SOURCE ROUTING	--Cette option permettait de spécifier le chemin à suivre pour les paquets IP, à l'aide d'une série d'adresses IP indiquant les routeurs à utiliser. --En exploitant cette option, le pirate peut indiquer un chemin de retour pour les paquets vers un routeur sous son contrôle.	– Désactiver la fonction de "source-routing" sur les paquets IP	
EPUI RESS DHCP	• Si un pirate a réussi à saturer un serveur DHCP par épuisement de ressources, il peut très bien en activer un autre à la place. □ il pourra ainsi contrôler tout le trafic réseau.	• Chaque fois que c'est possible, il faut limiter le service DHCP à une liste « fermée » de correspondances d'adresses MAC et IP. • S'il est impossible d'établir une liste « fermée », segmentez votre réseau en sous-réseaux et attribuez-leur chacun un serveur DHCP. □ Ces serveurs seront indépendants les uns des autres.	
DNS CACHE POISONING	• Le principe de cette attaque est très similaire à celui de l'ARP-Poisoining. • L'objectif du pirate est d'empoisonner ce cache avec de fausses informations. – il doit avoir sous contrôle un nom de domaine et son serveur DNS.	• Configurez votre serveur DNS pour qu'il ne résolve directement que les noms de machine du réseau sur lequel il a autorité. • Autorisez seulement des machines internes à demander la résolution de noms de domaines distants.	
XSS	Le cross-site scripting (abrégé XSS), est un type de faille de sécurité des sites web permettant d'injecter du contenu dans une page, permettant ainsi de provoquer des actions sur les navigateurs web visitant la page.	• Chaque élément de l'URL subissant un Traitement doit obligatoirement être filtré afin d'ôter toutes les balises HTML. • Une simple transformation peut suffire pour les rendre inexécutables.	
INJECTION SQL	• L'attaque par SQL-Injection consiste à injecter des caractères spéciaux ou des chaînes de caractères particulières dans les requêtes SQL du client	• Pour bien sécuriser votre serveur SQL, vérifiez que tous les comptes possèdent un mot de passe	

Vocabulaire :

• Attaque par eMail :
– ***Hoax*** : fausse information, rumeur destiné à saturer la messagerie ;
– ***Mail bombing*** : Attaque consistant à générer beaucoup de mail pour saturer un serveur de mail ;
– ***Spamming*** : Envoie de courriers non sollicités à but commercial ;
– ***Phishing*** : Envoie de courriers permettant le détournement d'informat
• Attaque Réseau TCP/IP :
– ***Spoofing*** : Forger un message réseau faux et/ou malformé
– ***Flooding*** : Inondation en vue de saturer une machine
– ***Smurfing*** : Équivalent du flooding mais sur tout un réseau
– ***Hijacking*** : Détournement d'une connexion
– ***Sniffing*** : Écoute des communications en vue d'obtenir des informatic
– ***Replay*** : Le rejeu
– ***Denial Of Service*** : Déni de service
– ***DDoS*** : Déni de service distribué
• ***Buffer Overflow*** : Attaque par débordement ;
• ***Service poisoning*** : Corruption d'un service (détournement de son con
• ***Backdoor*** : Logiciel de prise de contrôle à distance ;
• ***Keystroke*** : Enregistrement des touches tapés par les utilisateurs ;
• ***Trapdoor*** : Logiciel permettant d'obtenir des droits privilégiés suite à une action particulière ;
• ***Rootkit*** : outil de dissimulation d'activité ;
• ***Spyware*** : Logiciel d'espionnage de la machine ;
• ***virus*** : programme qui se duplique sur d'autres machines ;
• ***ver*** : programme qui se duplique lui-même par le réseau ;
• ***cheval de Troie*** (Trojan) : logiciel nuisible déguisé en programme légitime ;
• ***exploit*** : permet d'exploiter une faille de sécurité pour obtenir une élévation des privilèges .

Tunnel ICMP

- La transmission tunnel ICMP est le fait d'envelopper des données réelles dans un en-tête ICMP.
- De nombreux routeur et firewall qui autorisent aveuglément le passage de paquets ICMP ECHO, ICMP ECHO REPLY et UDP sont vulnérables à cette attaque.
- Outil : loki, ptunnel
- Exemple :

Serveur :
```
ptunnel –c interface
Service ssh start
– On interdit en entrée tout sauf le trafic icmp
Iptables –P INPUT DROP
Iptables –A INPUT –p icmp –j ACCEPT
Iptables –A INPUT –i lo –j ACCEPT
```
Client :
```
ptunnel –p serveur –lp port_local –dp port_distant –da localhost
ssh –p port_local localhost
```

Traceroute

•Quand un routeur intermédiaire reçoit un paquet, il décrémente son TTL avant de le transmettre au routeur suivant.
•Si le TTL atteint zéro, un message ICMP " temps dépassé » est envoyé à l'hôte d'origine.
•Traceroute envoi le premier paquet avec un TTL = 1
•Le premier routeur dans le chemin du paquet retournera un message ICMP " temps dépassé "
–Ceci permet à l'attaquant de connaître l'adresse IP du premier routeur.
•Les paquets suivants sont envoyés en augmentant chaque fois le TTL de 1,
–Ainsi l'attaquant sera en mesure de connaître tous les routeurs entre lui et la cible .
•L'attaquant pourrait tracer le chemin emprunté par un paquet, et avoir des informations sur la topologie du réseau cible .
–hping3 - -traceroute -V -1 @cible
•cheops permet de cartographier un réseau en utilisant ping et traceroute

Firewalk

•But : identifier les ports filtrés derrière un pare-feu.
•Le Firewalking est généralement fait en 2 phases:
–la phase 1 consiste à faire un traceroute à la cible pour déterminer le nombre n de sauts pour atteindre le pare-feu.
–Pendant la phase de balayage, la valeur TTL du paquet est réglée à n+1 et envoyer à un hôte connu derrière le pare-feu.
–Si un ICMP "temps dépassé " est reçu, cela voudrait dire que le paquet a atteint la machine mais avec un TTL = 0
•provoquant ainsi le message ICMP
–sinon on peut en déduire qu'il existe une règle de filtrage du pare-feu qui arrête ce trafic.
Outils : firewalk, nmap

Nmap firewalking
nmap --script=firewalk --traceroute <host>
•nmap --script=firewalk --traceroute --script-args=arg=val <host>
•Arguments
–firewalk.max-retries : le nombre maximum de retransmission.
–firewalk.recv-timeout : la durée en millisecondes de la boucle de capture de paquets.
–firewalk.probe-timeout : période de validité en millisecondes
–firewalk.max-active-probes : maximum number of parallel active probes.
–firewalk.max-probed-ports : maximum number of ports to probe per protocol. Set to -1 to scan every filtered port.

Attaque TCP: SYN Flooding

- La machine A envoie une demande de connexion TCP à la machine B
  - paquet SYN
  - La trame TCP est encapsulé dans un paquet IP avec une fausse adresse
- La machine B répond à la demande
  - Paquet SYN/ACK
  - Attend une confirmation d'ouverture qui n'arrivera jamais
- La connexion reste semi-ouverte pour un temps limité mais très grand devant la capacité des réseaux
- La machine A recommence avec
  - un grand nombre de demandes fabriquées
  - de fausses adresses (sources variées)

Attaque Session Flood

- La méthode générale de cette attaque consiste à saturer un service distant en montant un plus grand nombres de connexions TCP que peut en supporter la cible.
- Cela ressemble beaucoup à l'attaque SynFlood excepté le fait qu'elle se base sur le montage complet d'une session TCP (SYN - SYN/ACK - ACK).
- La conséquence pour la cible est de ne plus pouvoir accepter aucune session TCP supplémentaire.
- Cette attaque à l'avantage d'être très simple à mettre en oeuvre, mais la faiblesse d'être très rapidement repéré.
- Du côté cible, les préconisations afin de tenter de l'éviter sont :
  - Augmenter le nombre de sessions maximums supportées
  - Dupliquer la cible afin d'obtenir N fois le nombre de sessions maximums
  - Mettre en oeuvre des boîtiers de repartissions de charge des sessions TCP
  - Implémenter une console IDS détectant l'attaque afin de bloquer l'IP attaquante