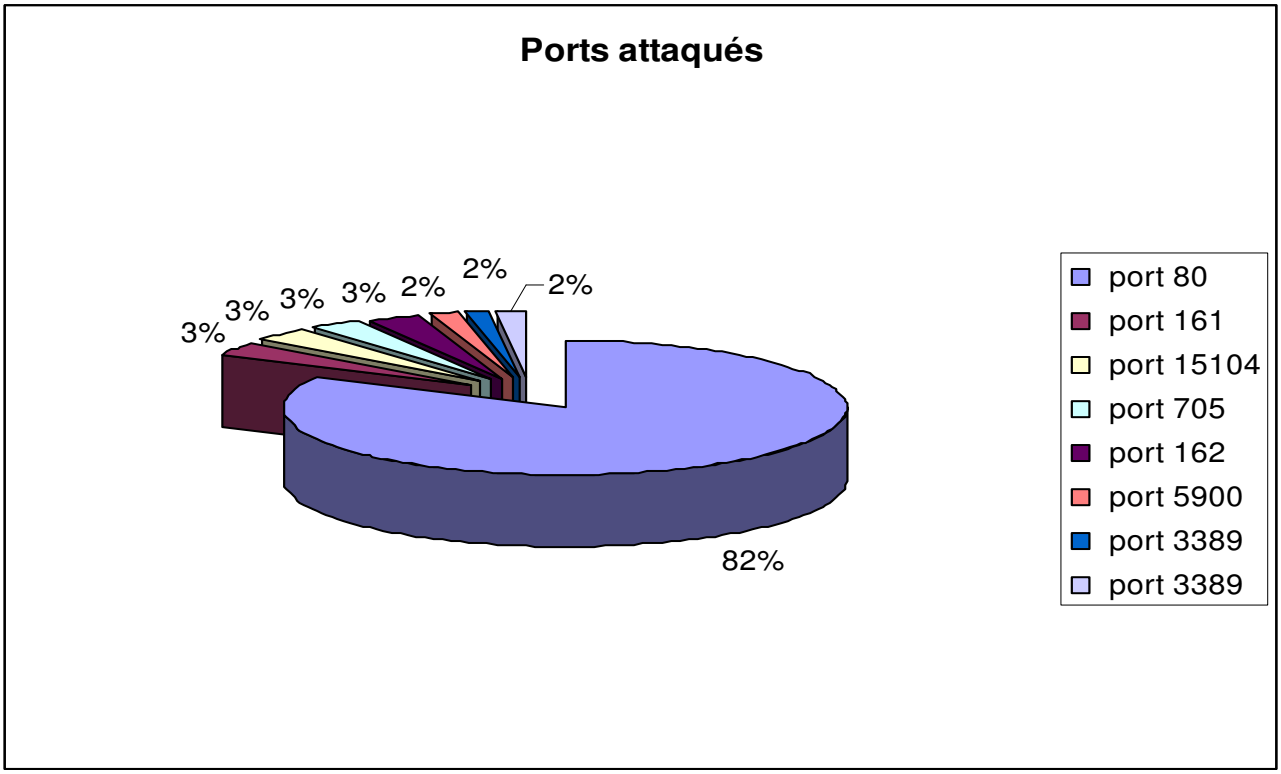
Groupe Analyse
REPORT du 14 oct 2004

I. Attaques recensées contre le serveur Web (172.66.66.5)

ATTAQUE	CLASSIFICATION	PRIORITE	PORT VISE(TCP)	NB DE TENTATIVES	IP DE L'ATTAQUANT	REUSSIE ?
SynSCAN	Scan furtif		Tous	1	172.16.80.250	**OUI**
SNMP request TCP	Vol d'information	2	161	2	172.16.80.250	NON
DDOS mstream client to handler	Deni de service	2	15104	2	172.16.80.250	NON
SNMP AgentX/tcp request	Vol d'information	2	705	2	172.16.80.250	NON
SNMP trap tcp	Vol d'information	2	162	2	172.16.80.250	NON
POLICY VNC server response		3	5900	1	172.16.80.250	**OUI**
MISC MS Terminal server request RDP	Deni de service	3	3389	2	172.16.80.250	**OUI**
WEB-ATTACKS id command attempt	Attaque web	1	80	14	172.16.80.250	?
WEB-MISC whisker tab splice attack	Vol d'information	2	80	35	172.16.80.250	?
WEB-MISC http directory traversal	Vol d'information	2	80	2	172.16.80.250	?
WEB-MISC whisker space splice attack	Vol d'information	2	80	1	172.16.80.250	?
DOS Cisco attempt	Attaque web	1	80	1	172.16.80.250	?

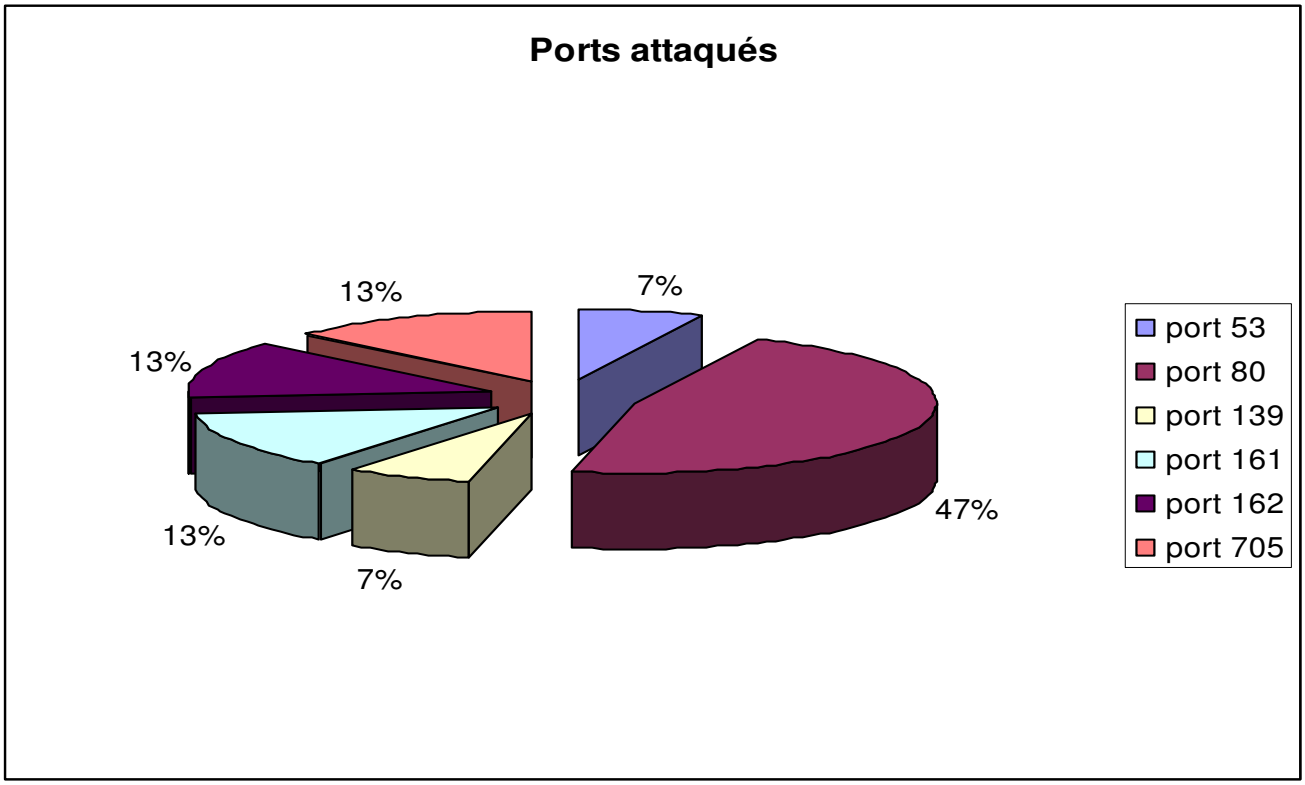
Ci dessous un graphique représentant la quantité d'attaques par port.



II. Attaques recensées contre le serveur BD (172.66.66.6)

ATTAQUE	CLASSIFICATION	PRIORITE	PORT VISE(TCP)	NB DE TENTATIVES	IP DE L'ATTAQUANT	REUSSIE ?
SynSCAN	Scan furtif		Tous	1	172.16.80.250	**OUI**
SNMP AgentX/tcp request	Vol d'information	2	705	2	172.16.80.250	?
SNMP trap tcp	Vol d'information	2	162	2	172.16.80.250	?
DDOS mstream client to handler	Deni de service	2	15104	2	172.16.80.250	?
SNMP request TCP	Vol d'information	2	161	2	172.16.80.250	?
DNS named version attempt	Vol d'information	2	53	1	172.16.80.250	?
WEB-IIS encoding access	Accès à une appli web vulnérable	2	80	3	172.16.80.250	?
WEB-ATTACKS id command attempt	Attaque web	1	80	2	172.16.80.250	?
WEB-MISC http directory traversal	Vol d'information	2	80	2	172.16.80.250	?
NETBIOS SMB IPC$ share access		3	139	1	172.16.80.250	?

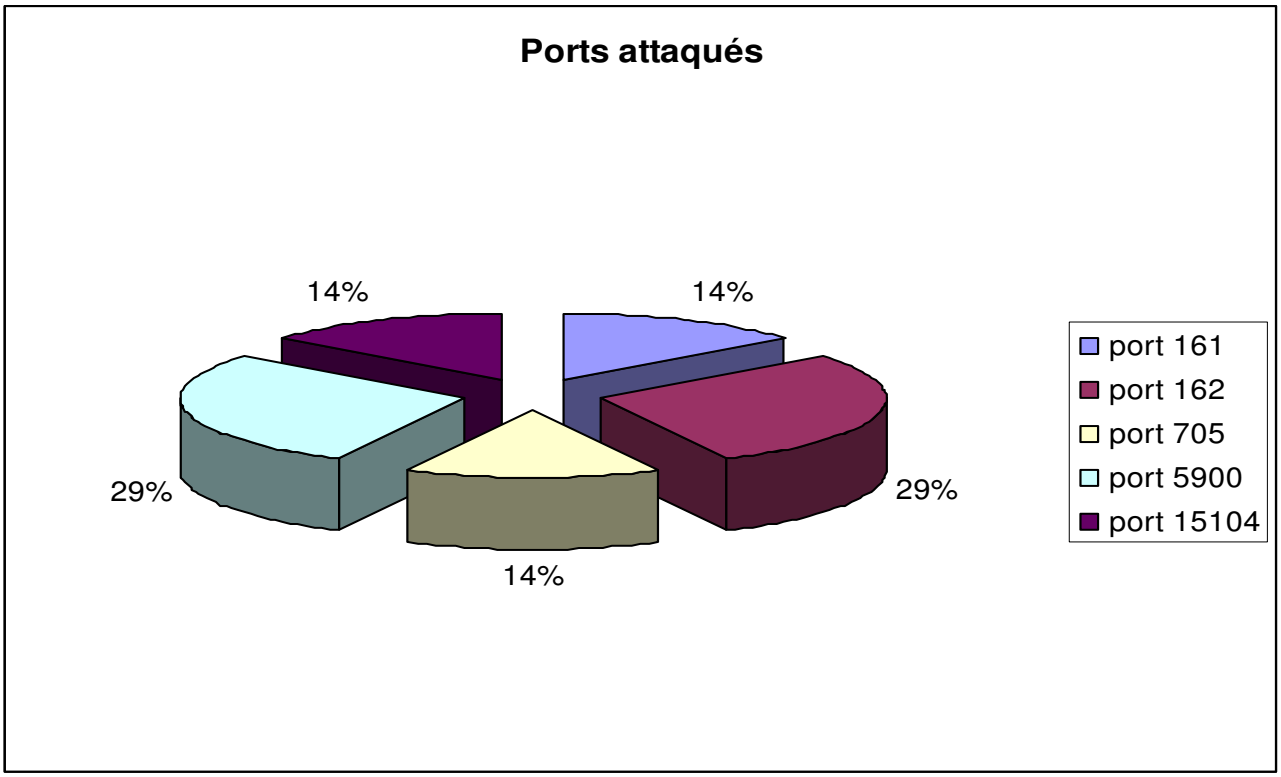
Ci dessous un graphique représentant la quantité d'attaques par port sur la machine 172.66.66.6.



III. Attaques recensées contre le poste client (172.66.66.100)

ATTAQUE	CLASSIFICATION	PRIORITE	PORT VISE(TCP)	NB DE TENTATIVES	IP DE L'ATTAQUANT	REUSSIE ?
SynSCAN	Scan furtif		Tous	1	172.16.80.250	**OUI**
POLICY VNC server response		3	5900	2	172.16.80.251	**OUI**
SNMP trap tcp	Vol d'information	2	162	2	172.16.80.250	?
SNMP request TCP	Vol d'information	2	161	1	172.16.80.250	?
SNMP AgentX/tcp request	Vol d'information	2	705	1	172.16.80.250	?
DDOS mstream client to handler	Deni de service	2	15104	1	172.16.80.250	?

Ci dessous un graphique représentant la quantité d'attaques par port sur la machine 172.66.66.100

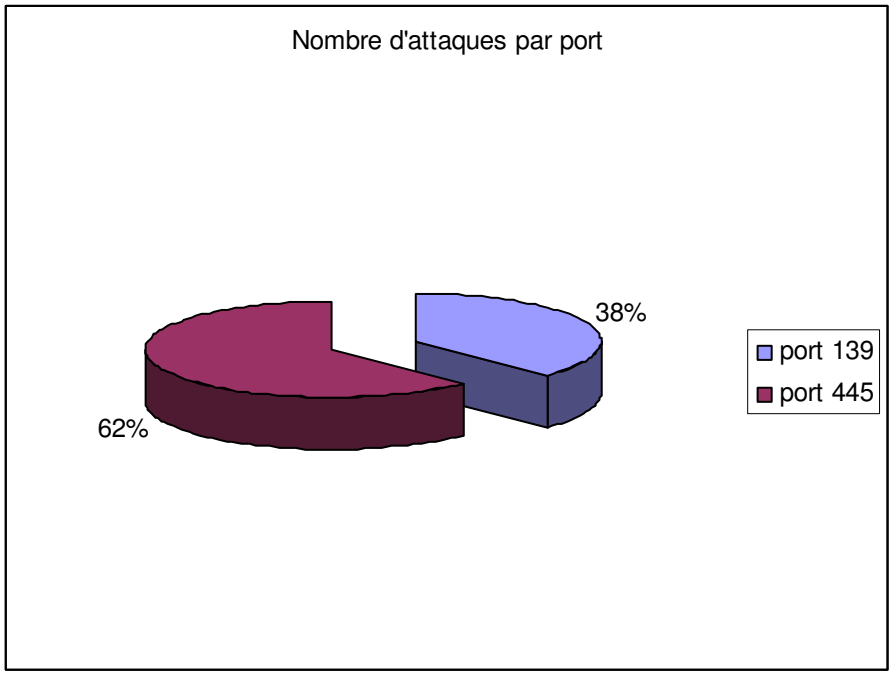


Groupe Analyse
REPORT du 18 oct 2004

IV. Attaques recensées contre le serveur Web (172.66.66.5)

ATTAQUE	CLASSIFICATION	PRIORITE	PORT VISE	PROTOCOLE	NB DE TENTATIVES	IP DE L'ATTAQUANT	REUSSIE ?
NETBIOS SMB share access		3	TCP 139	SMB	6	172.16.80.250	NON
NETBIOS SMB-DS DCERPC NTLMSSP asn1 overflow attempt	tentative d'appropriation de droits admin	1	TCP 445	SMB	7	172.16.80.251	
NETBIOS SMB-DS Session Setup AndX request unicode username overflow attempt	tentative d'appropriation de droits admin	1	TCP 445	SMB	3	172.16.80.251	
TOTAL					**15 tentatives**		

Ci dessous un graphique représentant la quantité d'attaques par port.



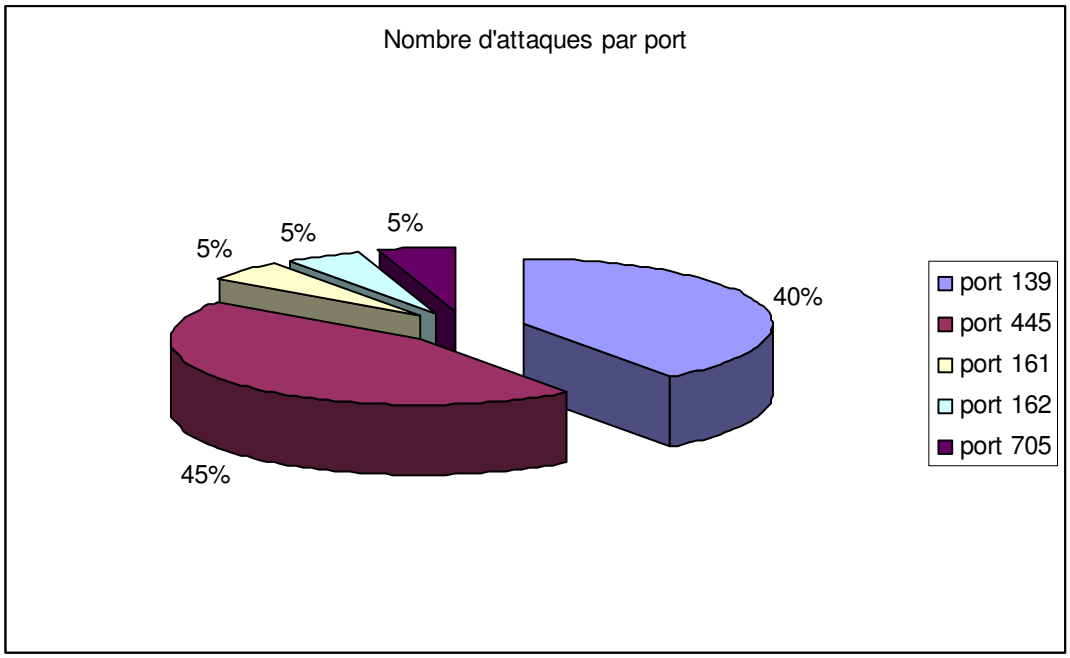
V. Attaques recensées contre le serveur BD (172.66.66.6)

ATTAQUE	CLASSIFICATION	PRIORITE	PORT VISE	PROTOCOLE	NB DE TENTATIVES	IP DE L'ATTAQUANT	REUSSIE
NETBIOS SMB share access		3	TCP 139	SMB	2	172.16.80.250	NON
TOTAL					**3 tentatives**		

VI. Attaques recensées contre la machine 172.66.66.81(client)

ATTAQUE	CLASSIFICATION	PRIORITE	PORT VISE	PROTOCOLE	NB DE TENTATIVES	IP DE L'ATTAQUANT	REUSSIE
SynScan	Scan de ports furtif					172.16.80.250	OUI
SNMP request tcp	Vol d'information	2	TCP 161	SNMP	1	172.16.80.250	NON
SNMP trap tcp	Vol d'information	2	TCP 162	SNMP	1	172.16.80.250	NON
SNMP AgentX/tcp request	Vol d'information	2	TCP 705	SNMP	1	172.16.80.250	NON
NETBIOS SMB share access		3	TCP 139	SMB	7	172.16.80.250	NON
NETBIOS SMB-DS DCERPC NTLMSSP asn1 overflow attempt	tentative d'appropriation de droits admin	1	TCP 445	SMB	9	172.16.80.251	NON
NETBIOS SMB DCERPC NTLMSSP asn1 overflow attempt	tentative d'appropriation de droits admin	1	TCP 139	SMB	1	172.16.80.251	NON
TOTAL					**135 tentatives**		

Ci dessous un graphique représentant la quantité d'attaques par port sur la machine 172.66.66.81.



Groupe Analyse
REPORT du 21 oct 2004

VII. Attaques recensées contre le serveur Web (172.66.66.5)

OBSERVATIONS	PROTOCOLE	NB DE TENTATIVES	IP
ICMP Echo Reply	ICMP	4	172.16.80.1(routeur)

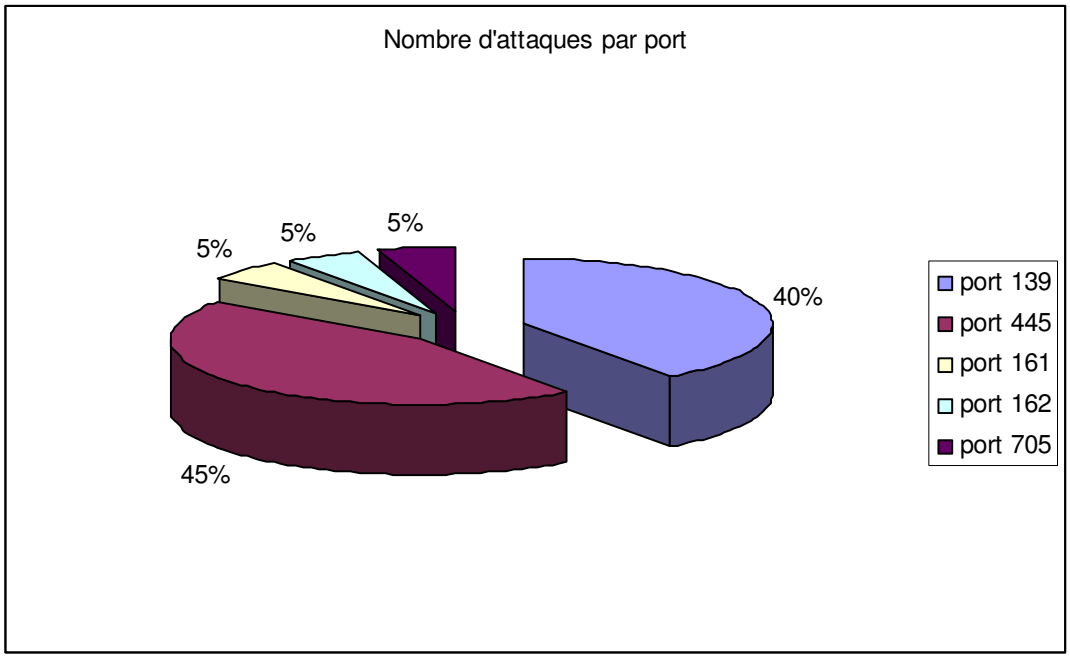
VIII. Attaques recensées contre le serveur BD (172.66.66.6)

ATTAQUE	CLASSIFICATION	PRIORITE	PORT VISE	PROTOCOLE	NB DE TENTATIVES	IP DE L'ATTAQUANT	REUSSIE
NETBIOS SMB share access		3	TCP 139	SMB	2	172.16.80.250	NON
TOTAL					**3 tentatives**		

IX. Attaques recensées contre la machine 172.66.66.81(client)

ATTAQUE	CLASSIFICATION	PRIORITE	PORT VISE	PROTOCOLE	NB DE TENTATIVES	IP DE L'ATTAQUANT	REUSSIE
SynScan	Scan de ports furtif					172.16.80.250	OUI
SNMP request tcp	Vol d'information	2	TCP 161	SNMP	1	172.16.80.250	NON
SNMP trap tcp	Vol d'information	2	TCP 162	SNMP	1	172.16.80.250	NON
SNMP AgentX/tcp request	Vol d'information	2	TCP 705	SNMP	1	172.16.80.250	NON
NETBIOS SMB share access		3	TCP 139	SMB	7	172.16.80.250	NON
NETBIOS SMB-DS DCERPC NTLMSSP asn1 overflow attempt	tentative d'appropriation de droits admin	1	TCP 445	SMB	9	172.16.80.251	NON
NETBIOS SMB DCERPC NTLMSSP asn1 overflow attempt	tentative d'appropriation de droits admin	1	TCP 139	SMB	1	172.16.80.251	NON
TOTAL					**135 tentatives**		

Ci dessous un graphique représentant la quantité d'attaques par port sur la machine 172.66.66.81.



Groupe Analyse
REPORT du 26 oct 2004
au 3 nov 2004

I. Activité du 26 octobre 2004

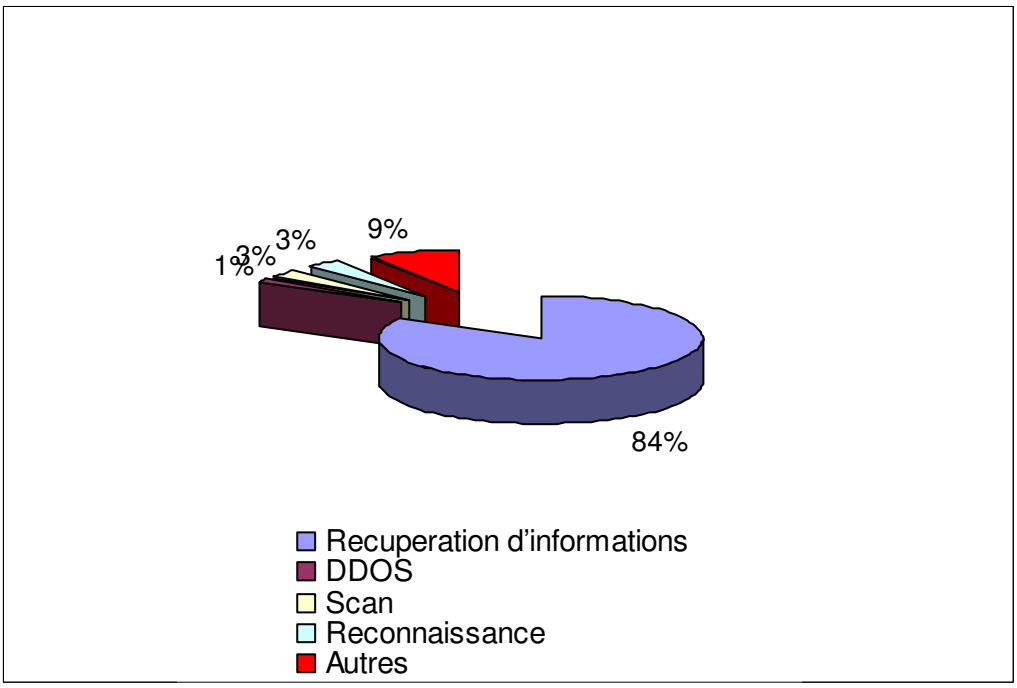
1. Attaques recensées contre 172.55.55.254(routeur inter vlan)

ATTAQUE	BUT ?	PORT VISE	PROTOCOLE	NB DE TENTATIVES	IP DE L'ATTAQUANT	COMMENTAIRES
SNMP request udp	Recuperation d'informations	161	SNMP	648	172.16.80.250	L'attaquant envoie un paquet sur le port 161 de udp et attend une réponse du demon SNMP pour tenter une attaque
SNMP public access udp	Recuperation d'informations	161	SNMP	84	172.16.80.250	SNMP v1 possede un champ *community* qui par défaut est *public ou private* sur beaucoup d'implémentations.
SNMP missing community string attempt	Recuperation d'informations	161	SNMP	36	172.16.80.250	Une communication SNMP a été etablie sans nom de communauté.
MS-SQL ping attempt	Recherche d'une base MS-SQL	1434		24	172.16.80.250	L'attaquant semble avoir utilisé Nessus pour chercher l'existence d'une base MS-SQL.
SCAN Amanda client version request	Scan de ports			24	172.16.80.250	
SNMP private access udp	Recuperation d'informations	161	SNMP	24	172.16.80.250	SNMP v1 possede un champ *community* qui par défaut est *public ou private* sur beaucoup d'implémentations.
DNS named version attempt	Reconnaissance	53	DNS	12	172.16.80.250	L'attaquant a tenter de découvrir la version de BIND utilisée et donc de savoir si la machine heberge un serveur de nom.
MISC xdmcp info query		177	UDP	12	172.16.80.250	L'attaquant tente de se connecter en XDMCP
DNS named authors attempt	Reconnaissance	53	DNS	12	172.16.80.250	Cette attaque permet à l'auteur de savor si la version de BIND utilisée est 9.x ou non.
SNMP trap udp	Recuperation d'informations	162	SNMP	12	172.16.80.250	L'attaquant envoie un trap et attend une réponse du demon.
MISC AFS access	Accèe non autorisé	7001	UDP	12	172.16.80.250	AFS est un système de fichiers partagés utilisant des ACL. L'attaquant a tenté d'accéder à AFS malgré ces ACL.
(spo_bo) Back Orifice Traffic detected				12	172.16.80.250	
SynScan	Scan de ports furtif	tous	TCP	10	172.16.80.250	L'attaquant envoie des paquets TCP avec le flag SYN armé et attend une réponse de type SYN ACK pour connaître les ports ouverts.
MISC UPnP malformed advertisement	Deni de service ou accès non autorisé	1900	UPnP	10	172.16.80.250	L'attaquant utilise un exploit connu pour envoyer un *Notify* malformé qui va provoqué un buffer overflow.
TFTP Get		69	TFTP	6	172.16.80.250	
SNMP request tcp	Recuperation d'informations	161	SNMP	6	172.16.80.250	L'attaquant envoie un paquet sur le port 161 de tcp et attend une réponse du demon SNMP pour tenter une attaque.
SNMP trap tcp	Recuperation d'informations	162	SNMP	6	172.16.80.250	L'attaquant envoie un trap et attend une réponse du demon.

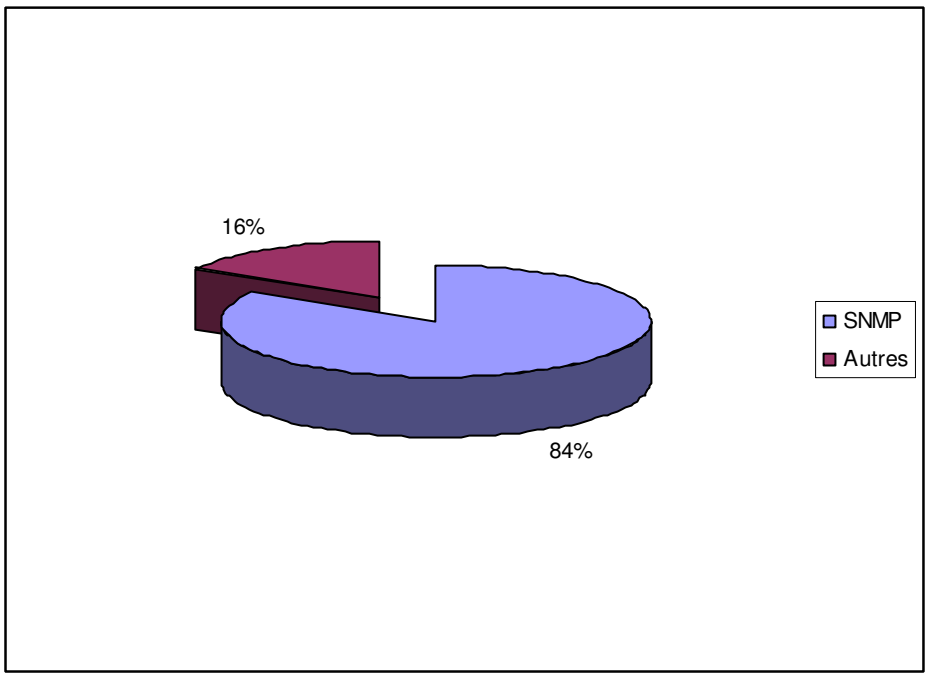
SNMP AgentX/tcp request	Deni de service	705	SNMP	6	172.16.80.250	L'attaquant peut essayer d'utiliser un exploit connu et envoyé un paquet malformé pour tenter un deni de service ou l'execution de code.
TFTP GET passwd	Reconnaissance	69	TFTP	4	172.16.80.250	Il semblerait que l'attaquant ait essayé de scaner le réseau à la recherche de serveurs TFTP.
MISC source route lssr	Informations sur la topologie du réseau			3	172.16.80.250	L'attaquant semble avoir tenté de découvrir la topologie du réseau en utilisant des outils comme traceroute.
MISC source route lssre				3	172.16.80.250	L'attaquant a tenté avec des paquets routés par la source de modifier la configuration de la machine en termes de sourcerouting(exploit pour W9x et NT)
ICMP PING NMAP	Reconnaissance	Tous	ICMP	3	172.16.80.250	L'attaquant a utilisé Nmap pour voir quels sont les hotes actifs du réseau.
DDOS shaft handler to agent	Deni de service distribué	18753	UDP	2	172.16.80.250	
DDOS TFN Probe	Deni de service distribué			2	172.16.80.250	L'attaquant a essayé de corrompre un host en le faisant devenir client TFN(tribal flood network) puis a tenté de communiquer avec lui.
DDOS Trin00 Master to Daemon default password attempt	Deni de service distribué	27444	UDP	2	172.16.80.250	L'attaquant a essayé de corrompre un host en lui plaçant un démon puis a tenté de communiquer avec ce démon(en utilisant un paquet udp port 27444 avec la chaîne "144adsl" dans le payload) pour lancer des attaques.
TFTP root directory	Execution de code ou vole de fichiers	69	TFTP	2	172.16.80.250	L'attaquant a essayé d'utiliser un exploit dans TFTP qui peut permettre l'execution de code ou bien le vol de fichiers.
DDOS mstream client to handler	Deni de service distribué	15104	UDP	2	172.16.80.250	L'attaquant a essayé de corrompre un host en le faisant mstream handler puis a tenté de communiquer avec lui pour lancer des attaques.
DDOS mstream handler ping to agent	Deni de service distribué	10498	UDP	2	172.16.80.250	L'attaquant a essayé de corrompre un host en le faisant mstream handler puis verifie si les autres agents sont actifs(en utilisant un paquet UDP port 10498 avec la chaine "ping" comme payload)
TFTP parent directory	Execution de code ou vole de fichiers	66	TFTP	2	172.16.80.250	L'attaquant a essayé d'utiliser un exploit dans TFTP qui peut permettre l'execution de code ou bien le vol de fichiers.
TOTAL				**983**		

2. Statistiques des attaques contre 172.55.55.254(routeur inter vlan)

Types d'attaques :



Protocoles :



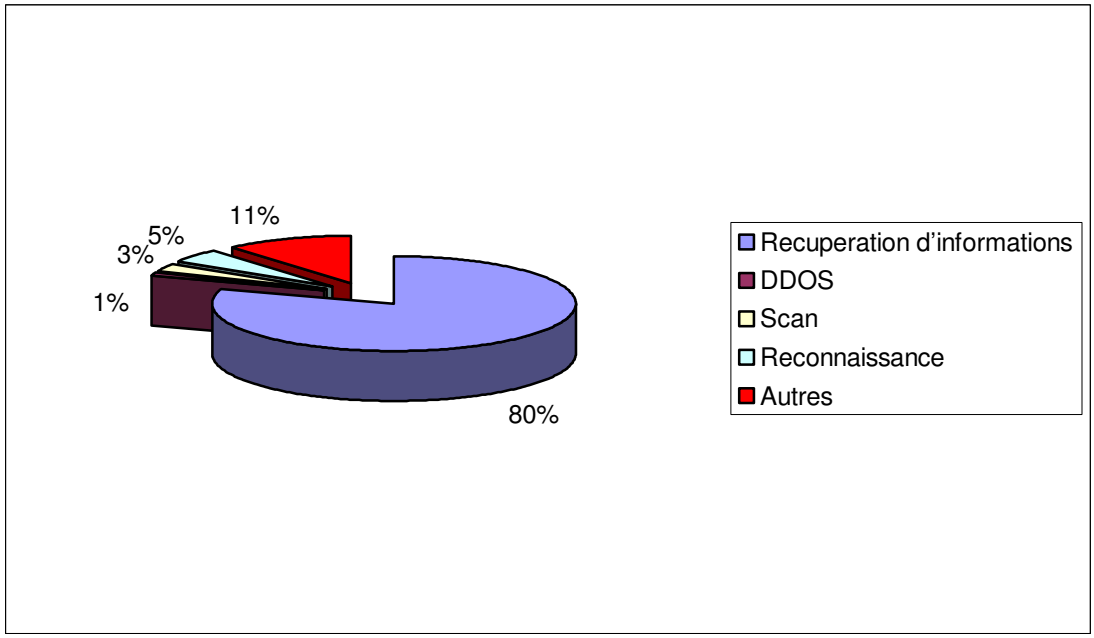
3. Attaques recensées contre la machine 172.55.55.1(routeur)

ATTAQUE	BUT ?	PORT VISE	PROTOCOLE	NB DE TENTATIVES	IP DE L'ATTAQUANT	COMMENTAIRES
SNMP request udp	Recuperation d'informations	161	SNMP	592	172.16.80.250	L'attaquant envoie un paquet sur le port 161 de udp et attend une réponse du demon SNMP pour tenter une attaque
SNMP public access udp	Recuperation d'informations	161	SNMP	82	172.16.80.250	SNMP v1 possede un champ *community* qui par défaut est *public ou private* sur beaucoup d'implémentations.
SNMP private access udp	Recuperation d'informations	161	SNMP	22	172.16.80.250	SNMP v1 possede un champ *community* qui par défaut est *public ou private* sur beaucoup d'implémentations.
SCAN Amanda client version request	Scan de ports			18	172.16.80.250	
ICMP PING NMAP	Reconnaissance	Tous	ICMP	17	172.16.80.250	L'attaquant a utilisé Nmap pour voir quels sont les hotes actifs du réseau.
SNMP missing community string attempt	Recuperation d'informations	161	SNMP	16	172.16.80.250	Une communication SNMP a été etablie sans nom de communauté.
MS-SQL ping attempt	Recherche d'une base MS-SQL	1434		12	172.16.80.250	L'attaquant semble avoir utilisé Nessus pour chercher l'existence d'une base MS-SQL.
DNS named version attempt	Reconnaissance	53	DNS	12	172.16.80.250	L'attaquant a tenter de découvrir la version de BIND utilisée et donc de savoir si la machine heberge un serveur de nom.
SNMP trap udp	Recuperation d'informations	162	SNMP	12	172.16.80.250	L'attaquant envoie un trap et attend une réponse du demon.
(spo_bo) Back Orifice Traffic detected				12	172.16.80.250	
MISC UPnP malformed advertisement	Deni de service ou accès non autorisé	1900	UPnP	10	172.16.80.250	L'attaquant utilise un exploit connu pour envoyer un *Notify* malformé qui va provoqué un buffer overflow.
DNS named authors attempt	Reconnaissance	53	DNS	6	172.16.80.250	Cette attaque permet à l'auteur de savor si la version de BIND utilisée est 9.x ou non.
TFTP Get		69	TFTP	6	172.16.80.250	
SNMP request tcp	Recuperation d'informations	161	SNMP	6	172.16.80.250	L'attaquant envoie un paquet sur le port 161 de tcp et attend une réponse du demon SNMP pour tenter une attaque.
SNMP trap tcp	Recuperation d'informations	162	SNMP	6	172.16.80.250	L'attaquant envoie un trap et attend une réponse du demon.
SNMP AgentX/tcp request	Deni de service	705	SNMP	6	172.16.80.250	L'attaquant peut essayer d'utiliser un exploit connu et envoyé un paquet malformé pour tenter un deni de service ou l'execution de code.
MISC AFS access	Accèe non autorisé	7001	UDP	4	172.16.80.250	AFS est un système de fichiers partagés utilisant des ACL. L'attaquant a tenté d'accéder à AFS malgré ces ACL.
SynScan	Scan de ports furtif	tous	TCP	4	172.16.80.250	L'attaquant envoie des paquets TCP avec le flag SYN armé et attend une réponse de type SYN ACK pour connaître les ports ouverts.

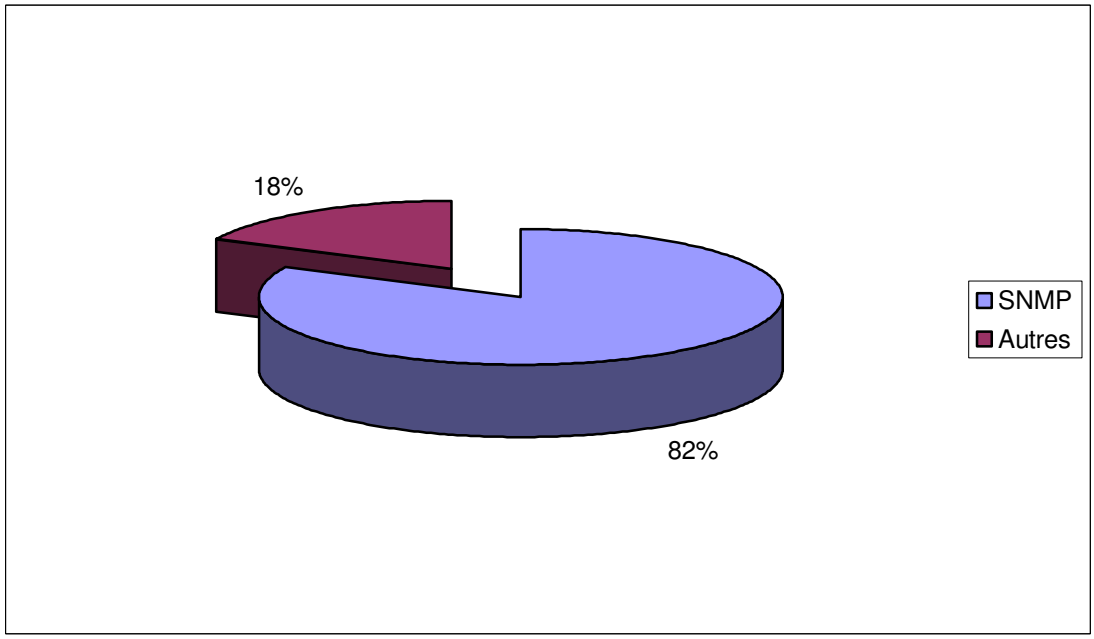
TFTP GET passwd	Reconnaissance	69	TFTP	4	172.16.80.250	Il semblerait que l'attaquant ait essayé de scaner le réseau à la recherche de serveurs TFTP.
MISC source route lssr	Informations sur la topologie du réseau			3	172.16.80.250	L'attaquant semble avoir tenté de découvrir la topologie du réseau en utilisant des outils comme traceroute.
MISC source route lssre				3	172.16.80.250	L'attaquant a tenté avec des paquets routés par la source de modifier la configuration de la machine en termes de sourcerouting(exploit pour W9x et NT)
MISC xdmcp info query		177	UDP	2	172.16.80.250	L'attaquant tente de se connecter en XDMCP
DDOS shaft handler to agent	Deni de service distribué	18753	UDP	2	172.16.80.250	
DDOS TFN Probe	Deni de service distribué			2	172.16.80.250	L'attaquant a essayé de corrompre un host en le faisant devenir client TFN(tribal flood network) puis a tenté de communiquer avec lui.
DDOS Trin00 Master to Daemon default password attempt	Deni de service distribué	27444	UDP	2	172.16.80.250	L'attaquant a essayé de corrompre un host en lui plaçant un démon puis a tenté de communiquer avec ce démon(en utilisant un paquet udp port 27444 avec la chaîne "144adsl" dans le payload) pour lancer des attaques.
TFTP root directory	Execution de code ou vole de fichiers	69	TFTP	2	172.16.80.250	L'attaquant a essayé d'utiliser un exploit dans TFTP qui peut permettre l'execution de code ou bien le vol de fichiers.
DDOS mstream client to handler	Deni de service distribué	15104	UDP	2	172.16.80.250	L'attaquant a essayé de corrompre un host en le faisant mstream handler puis a tenté de communiquer avec lui pour lancer des attaques.
DDOS mstream handler ping to agent	Deni de service distribué	10498	UDP	2	172.16.80.250	L'attaquant a essayé de corrompre un host en le faisant mstream handler puis verifie si les autres agents sont actifs(en utilisant un paquet UDP port 10498 avec la chaine "ping" comme payload)
TFTP parent directory	Execution de code ou vole de fichiers	66	TFTP	2	172.16.80.250	L'attaquant a essayé d'utiliser un exploit dans TFTP qui peut permettre l'execution de code ou bien le vol de fichiers.
TOTAL				**869**		

4. Statistiques des attaques contre 172.55.55.1

Types d'attaques :



Protocoles :



5. Autres attaques

Ce soir là nous avons également observé 14 ICMP redirect host avec comme adresse IP source 172.16.80.1:

- 3 à destination de 172.16.80.251
- 11 à destination de 172.16.80.250

Ceci signifie que l'attaque a tenté de se faire passer pour la machine 172.16.80.1(serveur DNS?) pour intercepter du trafic.

II. Attaques du 2 novembre 2004

ATTAQUE	BUT ?	PORT VISE	PROTOCOLE	NB DE TENTATIVES	IP DE L'ATTAQUANT	COMMENTAIRES
ICMP Redirect Host	Interception du trafic		ICMP	82	172.16.80.250	L'attaquant a tenté de se faire passer pour la machine 172.16.80.1(serveur DNS?) pour intercepter du trafic
ICMP Redirect Host	Interception du trafic		ICMP	21	172.16.80.61	L'attaquant a tenté de se faire passer pour la machine 172.16.80.1(serveur DNS?) pour intercepter du trafic
ICMP Redirect Host	Interception du trafic		ICMP	2	172.16.80.71	L'attaquant a tenté de se faire passer pour la machine 172.16.80.1(serveur DNS?) pour intercepter du trafic
TOTAL				**105**		

III. Attaques du 3 novembre 2004

1. Attaques recensées contre la machine 172.77.77.100(client XP)

ATTAQUE	BUT ?	PORT VISE	PROTOCOLE	NB DE TENTATIVES	IP DE L'ATTAQUANT	COMMENTAIRES
BAD-TRAFFIC loopback traffic	DoS			16836	Adresses Spoofées (adresses de loopback)	L'attaquant a essayé d'envoyer un très grand nombre de paquets(avec des adresses sources spoofées)au client.
SNMP trap tcp	Recuperation d'informations ou DoS	162	SNMP	45	Adresses Spoofées	L'attaquant envoie un trap et attend une réponse du demon. Tentative de DoS
SNMP AgentX/tcp request	Deni de service (DoS)	705	SNMP	41	Adresses Spoofées	L'attaquant peut essayer d'utiliser un exploit connu et envoyé un paquet malformé pour tenter un deni de service ou l'execution de code.
SNMP request tcp	Recuperation d'informations ou DoS	161	SNMP	38	Adresses Spoofées	L'attaquant envoie un paquet sur le port 161 de tcp et attend une réponse du demon SNMP pour tenter une attaque. Tentative de DoS
SNMP trap udp	Recuperation d'informations	162	SNMP	2	172.16.80.250	L'attaquant envoie un trap et attend une réponse du demon.
SNMP request udp	Recuperation d'informations	161	SNMP	2	172.16.80.250	L'attaquant envoie un paquet sur le port 161 de udp et attend une réponse du demon SNMP pour tenter une attaque
ICMP PING NMAP	Reconnaissance	Tous	ICMP	2	172.16.80.250	L'attaquant a utilisé Nmap pour voir quels sont les hotes actifs du réseau.
DOS Bay/Nortel Nautica Marlin	DoS	161	SNMP	2	172.16.80.250	Si un pont Bay/Nortel Nautica Marlin recoit une cette requette il va etre mi hors d'usage => DoS
TOTAL				**16968**		

2. Attaques recensées contre la machine 172.66.66.5 (Serveur Web)

ATTAQUE	BUT ?	PORT VISE	PROTOCOLE	NB DE TENTATIVES	IP DE L'ATTAQUANT	COMMENTAIRES
(http_inspect) NON-RFC HTTP DELIMITER		80	HTTP	86	172.16.80.250	
TOTAL				**86**		

3. Autres attaques

ATTAQUE	BUT ?	PORT VISE	PROTOCOLE	NB DE TENTATIVES	IP DE L'ATTAQUANT	COMMENTAIRES
ICMP Redirect Host	Interception du trafic		ICMP	63	172.16.80.250	L'attaquant a tenté de se faire passer pour la machine 172.16.80.1(serveur DNS?) pour intercepter du trafic
ICMP Redirect Host	Interception du trafic		ICMP	2	172.16.80.62	L'attaquant a tenté de se faire passer pour la machine 172.16.80.1(serveur DNS?) pour intercepter du trafic
TOTAL				**65**		

Groupe Analyse
REPORT du 8 nov 2004
au 12 nov 2004

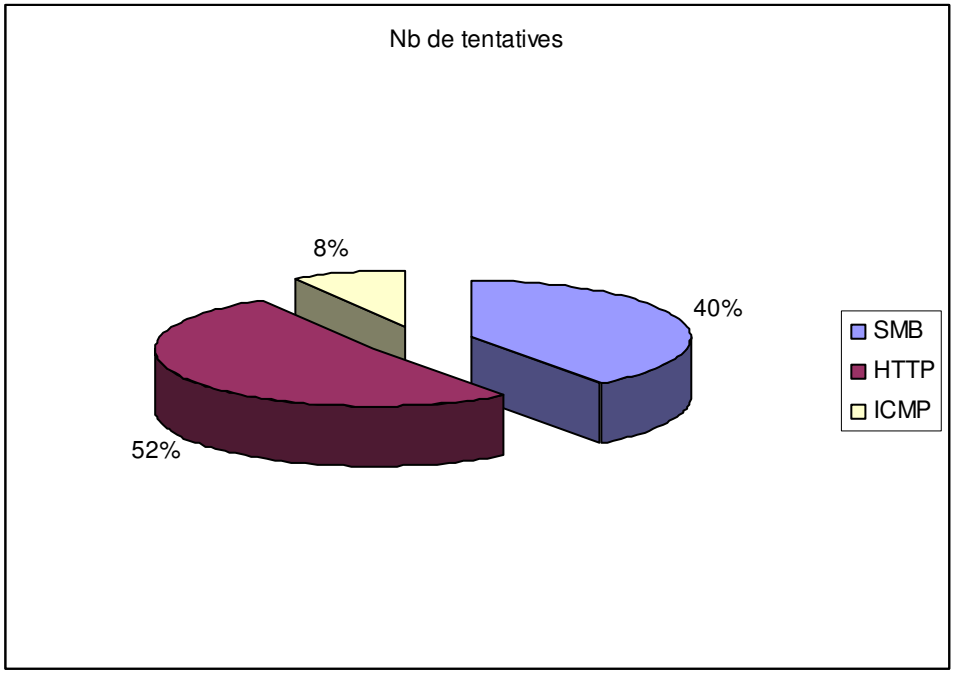
IV. Activité du 8 novembre 2004

1. Attaques recensées contre 172.44.44.1(firewall)

ATTAQUE	BUT ?	PORT VISE	PROTOCOLE	NB DE TENTATIVES	IP DE L'ATTAQUANT	COMMENTAIRES
NETBIOS SMB-DS Session Setup AndX request unicode username overflow attempt	Déni de service Execution de code	445	SMB	60	172.99.99.200	L'attaquant a tenté d'utilisé un exploit connu pour executer du code sur la machine ou pour provoquer un DoS. Les systèmes visés par cette attaque sont ceux utilisant ISS RealSecure ou BlackICE
WEB-CGI perl.exe access	Execution de code Accès non autorisé	80	HTTP	16	172.99.99.200	L'attaquant a tenté d'utilisé le fait que certains serveurs http supportant des applis CGI sont vulnérables.
ICMP PING NMAP	Reconnaissance		ICMP	16	172.99.99.200	L'attaquant a utilisé Nmap pour voir quels sont les hotes actifs du réseau.
WEB-IIS *.idc attempt	Execution de code	80	HTTP	10	172.99.99.20	IIS supporte les fichiers de type *.idc et un exploit existe et permet l'execution de code à distance.
WEB-IIS newdsn.exe access	Création de fichier	80	HTTP	8	172.99.99.200	IIS 3.0 a une vulnérabilité connu et un attaquant peut en fabriquant une url créer une base access sur le serveur cible.
WEB-IIS view source via translate header	Vol d'informations	80	HTTP	8	172.99.99.200	IIS 5.0 a une vulnérabilité connu et un attaquant peut en fabriquant une url obtenir des informations.
WEB-FRONTPAGE /_vti_bin/ access	Vol d'informations	80	HTTP	8	172.99.99.200	Cette attaque est une des nombreuses répertoriées contre Frontpage Server Extentions.
WEB-IIS fpcount access	Vol d'informations DoS Execution de code	80	HTTP	8	172.99.99.200	Cette attaque est une des nombreuses répertoriées contre IIS.
WEB-MISC queryhit.htm access	Vol d'informations Execution de code	80	HTTP	8	172.99.99.200	Exploitation d'une faille connue
WEB-MISC *%0a.pl access	Vol d'informations Execution de code	80	HTTP	8	172.99.99.200	Exploitation d'une faille connue
WEB-IIS perl access	Vol d'informations Acces non autorisé	80	HTTP	8	172.99.99.200	L'attaquant a tenté d'executer des script perl.
WEB-IIS perl-browse newline attempt	Vol d'informations Acces non autorisé	80	HTTP	8	172.99.99.200	Cette attaque est une des nombreuses répertoriées contre IIS.
WEB-CGI /cgi-bin/ access	Vol d'informations Acces non autorisé	80	HTTP	8	172.99.99.200	Tentatives d'accès aux scripts CGI d'un serveur Web
NETBIOS SMB-DS IPC$ share unicode access	Vol d'informations Acces non autorisé	445	SMB	6	172.99.99.200	Tentatives d'accès aux partages réseaux Windows de la machine cible.
NETBIOS SMB-DS C$ share unicode access	Vol d'informations Acces non autorisé	445	SMB	4	172.99.99.200	Tentatives d'accès aux partages réseaux Windows de la machine cible.
NETBIOS SMB-DS D$ share unicode access	Vol d'informations Acces non autorisé	445	SMB	4	172.99.99.200	Tentatives d'accès aux partages réseaux Windows de la machine cible.
NETBIOS SMB-DS ADMIN$ share unicode access	Vol d'informations Acces non autorisé	445	SMB	2	172.99.99.200	Tentatives d'accès aux partages réseaux Windows de la machine cible.
TOTAL				**190**		

2. Statistiques des attaques contre 172.44.44.1(firewall)

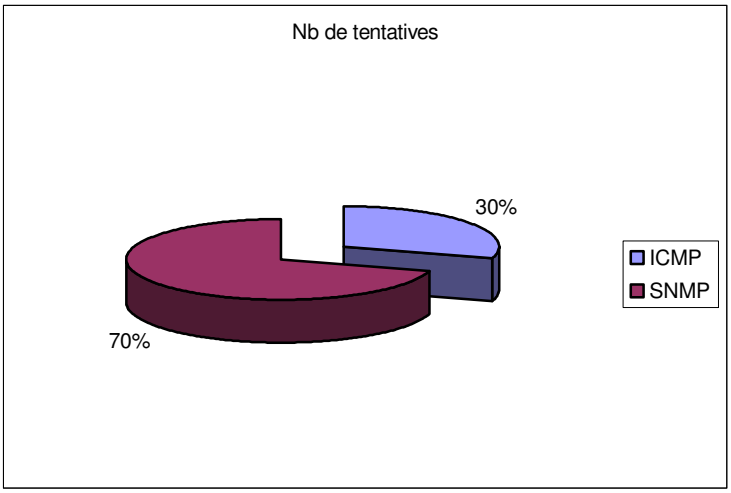
Protocoles :



3. Attaques recensées contre la machine 172.44.44.2(pot de miel)

ATTAQUE	BUT ?	PORT VISE	PROTO COLE	NB DE TENTATIVES	IP DE L'ATTAQUANT	COMMENTAIRES
ICMP PING NMAP	Reconnaissance		ICMP	8	172.99.99.200	L'attaquant a utilisé Nmap pour voir quels sont les hotes actifs du réseau.
SNMP trap tcp	Recuperation d'informations ou DoS	162	SNMP	7	172.99.99.200	L'attaquant envoie un trap et attend une réponse du demon. Tentative de DoS
SNMP AgentX/tcp request	Deni de service (DoS)	705	SNMP	7	172.99.99.200	L'attaquant peut essayer d'utiliser un exploit connu et envoyé un paquet malformé pour tenter un deni de service ou l'execution de code.
SNMP request tcp	Recuperation d'informations ou DoS	161	SNMP	5	172.99.99.200	L'attaquant envoie un paquet sur le port 161 de tcp et attend une réponse du demon SNMP pour tenter une attaque. Tentative de DoS

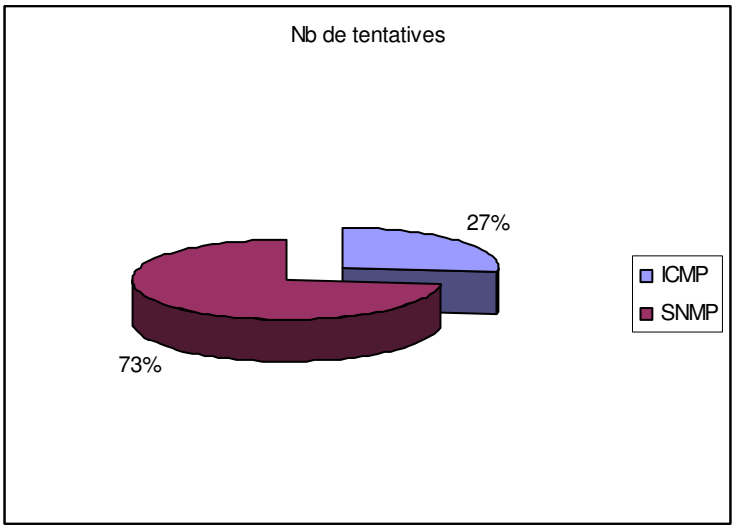
4. Statistiques des attaques contre 172.44.44.2(pot de miel)



5. Attaques recensées contre la machine 172.55.55.1(routeur)

ATTAQUE	BUT ?	PORT VISE	PROTOCOLE	NB DE TENTATIVES	IP DE L'ATTAQUANT	COMMENTAIRES
ICMP PING NMAP	Reconnaissance		ICMP	4	172.99.99.200	L'attaquant a utilisé Nmap pour voir quels sont les hotes actifs du réseau.
SNMP trap tcp	Recuperation d'informations ou DoS	162	SNMP	4	172.99.99.200	L'attaquant envoie un trap et attend une réponse du demon. Tentative de DoS
SNMP AgentX/tcp request	Deni de service (DoS)	705	SNMP	4	172.99.99.200	L'attaquant peut essayer d'utiliser un exploit connu et envoyé un paquet malformé pour tenter un deni de service ou l'execution de code.
SNMP request tcp	Recuperation d'informations ou DoS	161	SNMP	3	172.99.99.200	L'attaquant envoie un paquet sur le port 161 de tcp et attend une réponse du demon SNMP pour tenter une attaque. Tentative de DoS

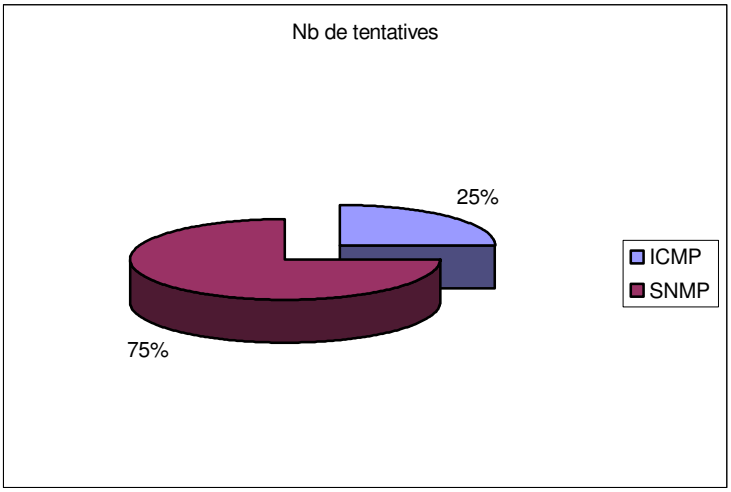
6. Statistiques des attaques contre 172.55.55.1



7. Attaques recensées contre la machine 172.77.77.100(client)

ATTAQUE	BUT ?	PORT VISE	PROTOCOLE	NB DE TENTATIVES	IP DE L'ATTAQUANT	COMMENTAIRES
ICMP PING NMAP	Reconnaissance		ICMP	2	172.99.99.200	L'attaquant a utilisé Nmap pour voir quels sont les hotes actifs du réseau.
SNMP trap tcp	Recuperation d'informations ou DoS	162	SNMP	2	172.99.99.200	L'attaquant envoie un trap et attend une réponse du demon. Tentative de DoS
SNMP AgentX/tcp request	Deni de service (DoS)	705	SNMP	2	172.99.99.200	L'attaquant peut essayer d'utiliser un exploit connu et envoyé un paquet malformé pour tenter un deni de service ou l'execution de code.
SNMP request tcp	Recuperation d'informations ou DoS	161	SNMP	2	172.99.99.200	L'attaquant envoie un paquet sur le port 161 de tcp et attend une réponse du demon SNMP pour tenter une attaque. Tentative de DoS

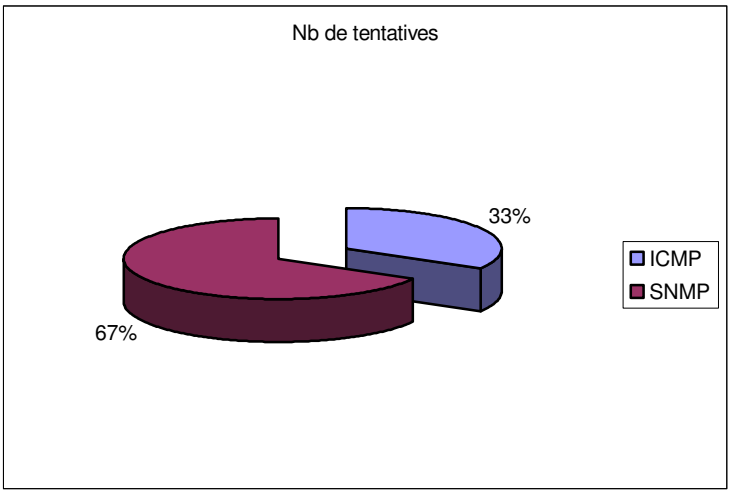
8. Statistiques des attaques contre 172.77.77.100(client)



9. Attaques recensées contre la machine 172.88.88.200(observation)

ATTAQUE	BUT ?	PORT VISE	PROTOCOLE	NB DE TENTATIVES	IP DE L'ATTAQUANT	COMMENTAIRES
ICMP PING NMAP	Reconnaissance		ICMP	2	172.99.99.200	L'attaquant a utilisé Nmap pour voir quels sont les hotes actifs du réseau.
SNMP AgentX/tcp request	Deni de service (DoS)	705	SNMP	2	172.99.99.200	L'attaquant peut essayer d'utiliser un exploit connu et envoyé un paquet malformé pour tenter un deni de service ou l'execution de code.
SNMP request tcp	Recuperation d'informations ou DoS	161	SNMP	2	172.99.99.200	L'attaquant envoie un paquet sur le port 161 de tcp et attend une réponse du demon SNMP pour tenter une attaque. Tentative de DoS

10. Statistiques des attaques contre 172.88.88.200(observation)



11. Autres attaques

Les attaquants ont lancé des PING NMAP en masse sur le réseau pour pouvoir obtenir une cartographie de celui-ci.
L'attaque du 8 novembre est plutot une attaque de reconaissance pour identifier les machines et frapper ulterieurement.

V. Activité du 9 novembre 2004

1. Attaques recensées contre la machine 172.44.44.1(firewall)

ATTAQUE	BUT ?	PORT VISE	PROTO COLE	NB DE TENTATIVES	IP DE L'ATTAQUANT	COMMENTAIRES
ICMP PING NMAP	Reconnaissance		ICMP	8	172.99.99.200	L'attaquant a utilisé Nmap pour voir quels sont les hotes actifs du réseau.

2. Attaques recensées contre la machine 172.44.44.2(pot de miel)

ATTAQUE	BUT ?	PORT VISE	PROTO COLE	NB DE TENTATIVES	IP DE L'ATTAQUANT	COMMENTAIRES
ICMP PING NMAP	Reconnaissance		ICMP	2	172.99.99.200	L'attaquant a utilisé Nmap pour voir quels sont les hotes actifs du réseau.
ICMP PING speedera	DoS		ICMP	156293	172.99.99.200	L'attaquant envoie une grande quantité de pings pour tenter de provoquer un deni de service. Cette tentative a echouée car la machine a continué d'emettre des paquets après l'attaque.

Groupe Analyse
REPORT du 26 oct 2004
au 3 nov 2004

VI. Activité du 26 octobre 2004

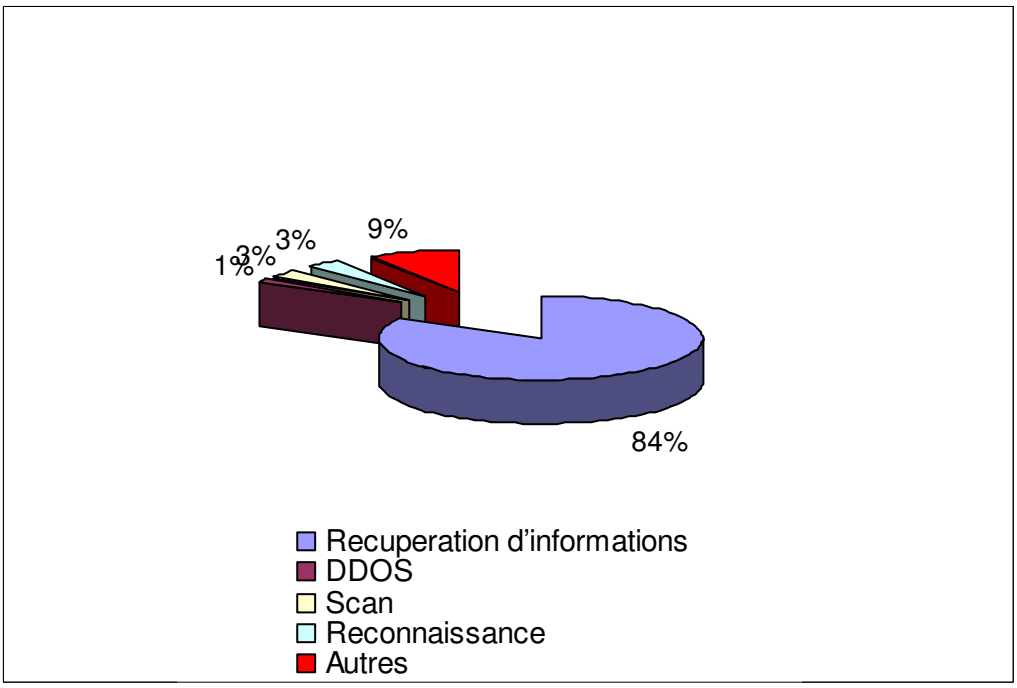
1. Attaques recensées contre 172.55.55.254(routeur inter vlan)

ATTAQUE	BUT ?	PORT VISE	PROTOCOLE	NB DE TENTATIVES	IP DE L'ATTAQUANT	COMMENTAIRES
SNMP request udp	Recuperation d'informations	161	SNMP	648	172.16.80.250	L'attaquant envoie un paquet sur le port 161 de udp et attend une réponse du demon SNMP pour tenter une attaque
SNMP public access udp	Recuperation d'informations	161	SNMP	84	172.16.80.250	SNMP v1 possede un champ *community* qui par défaut est *public ou private* sur beaucoup d'implémentations.
SNMP missing community string attempt	Recuperation d'informations	161	SNMP	36	172.16.80.250	Une communication SNMP a été etablie sans nom de communauté.
MS-SQL ping attempt	Recherche d'une base MS-SQL	1434		24	172.16.80.250	L'attaquant semble avoir utilisé Nessus pour chercher l'existence d'une base MS-SQL.
SCAN Amanda client version request	Scan de ports			24	172.16.80.250	
SNMP private access udp	Recuperation d'informations	161	SNMP	24	172.16.80.250	SNMP v1 possede un champ *community* qui par défaut est *public ou private* sur beaucoup d'implémentations.
DNS named version attempt	Reconnaissance	53	DNS	12	172.16.80.250	L'attaquant a tenter de découvrir la version de BIND utilisée et donc de savoir si la machine heberge un serveur de nom.
MISC xdmcp info query		177	UDP	12	172.16.80.250	L'attaquant tente de se connecter en XDMCP
DNS named authors attempt	Reconnaissance	53	DNS	12	172.16.80.250	Cette attaque permet à l'auteur de savor si la version de BIND utilisée est 9.x ou non.
SNMP trap udp	Recuperation d'informations	162	SNMP	12	172.16.80.250	L'attaquant envoie un trap et attend une réponse du demon.
MISC AFS access	Accèe non autorisé	7001	UDP	12	172.16.80.250	AFS est un système de fichiers partagés utilisant des ACL. L'attaquant a tenté d'accéder à AFS malgré ces ACL.
(spo_bo) Back Orifice Traffic detected				12	172.16.80.250	
SynScan	Scan de ports furtif	tous	TCP	10	172.16.80.250	L'attaquant envoie des paquets TCP avec le flag SYN armé et attend une réponse de type SYN ACK pour connaître les ports ouverts.
MISC UPnP malformed advertisement	Deni de service ou accès non autorisé	1900	UPnP	10	172.16.80.250	L'attaquant utilise un exploit connu pour envoyer un *Notify* malformé qui va provoqué un buffer overflow.
TFTP Get		69	TFTP	6	172.16.80.250	
SNMP request tcp	Recuperation d'informations	161	SNMP	6	172.16.80.250	L'attaquant envoie un paquet sur le port 161 de tcp et attend une réponse du demon SNMP pour tenter une attaque.
SNMP trap tcp	Recuperation d'informations	162	SNMP	6	172.16.80.250	L'attaquant envoie un trap et attend une réponse du demon.

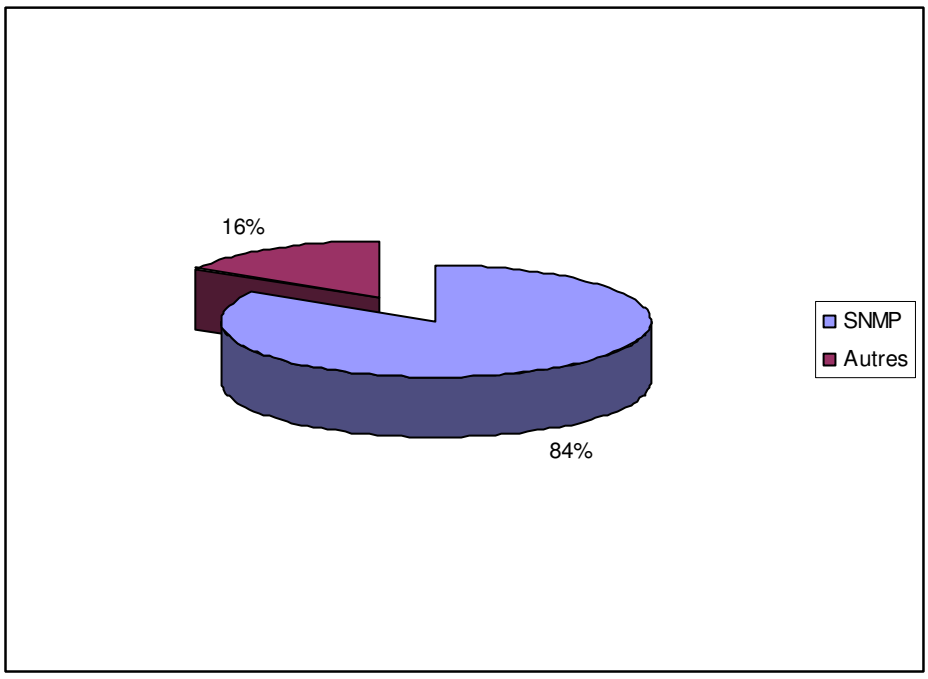
SNMP AgentX/tcp request	Deni de service	705	SNMP	6	172.16.80.250	L'attaquant peut essayer d'utiliser un exploit connu et envoyé un paquet malformé pour tenter un deni de service ou l'execution de code.
TFTP GET passwd	Reconnaissance	69	TFTP	4	172.16.80.250	Il semblerait que l'attaquant ait essayé de scaner le réseau à la recherche de serveurs TFTP.
MISC source route lssr	Informations sur la topologie du réseau			3	172.16.80.250	L'attaquant semble avoir tenté de découvrir la topologie du réseau en utilisant des outils comme traceroute.
MISC source route lssre				3	172.16.80.250	L'attaquant a tenté avec des paquets routés par la source de modifier la configuration de la machine en termes de sourcerouting(exploit pour W9x et NT)
ICMP PING NMAP	Reconnaissance	Tous	ICMP	3	172.16.80.250	L'attaquant a utilisé Nmap pour voir quels sont les hotes actifs du réseau.
DDOS shaft handler to agent	Deni de service distribué	18753	UDP	2	172.16.80.250	
DDOS TFN Probe	Deni de service distribué			2	172.16.80.250	L'attaquant a essayé de corrompre un host en le faisant devenir client TFN(tribal flood network) puis a tenté de communiquer avec lui.
DDOS Trin00 Master to Daemon default password attempt	Deni de service distribué	27444	UDP	2	172.16.80.250	L'attaquant a essayé de corrompre un host en lui plaçant un démon puis a tenté de communiquer avec ce démon(en utilisant un paquet udp port 27444 avec la chaîne "144adsl" dans le payload) pour lancer des attaques.
TFTP root directory	Execution de code ou vole de fichiers	69	TFTP	2	172.16.80.250	L'attaquant a essayé d'utiliser un exploit dans TFTP qui peut permettre l'execution de code ou bien le vol de fichiers.
DDOS mstream client to handler	Deni de service distribué	15104	UDP	2	172.16.80.250	L'attaquant a essayé de corrompre un host en le faisant mstream handler puis a tenté de communiquer avec lui pour lancer des attaques.
DDOS mstream handler ping to agent	Deni de service distribué	10498	UDP	2	172.16.80.250	L'attaquant a essayé de corrompre un host en le faisant mstream handler puis verifie si les autres agents sont actifs(en utilisant un paquet UDP port 10498 avec la chaine "ping" comme payload)
TFTP parent directory	Execution de code ou vole de fichiers	66	TFTP	2	172.16.80.250	L'attaquant a essayé d'utiliser un exploit dans TFTP qui peut permettre l'execution de code ou bien le vol de fichiers.
TOTAL				**983**		

2. Statistiques des attaques contre 172.55.55.254(routeur inter vlan)

Types d'attaques :



Protocoles :



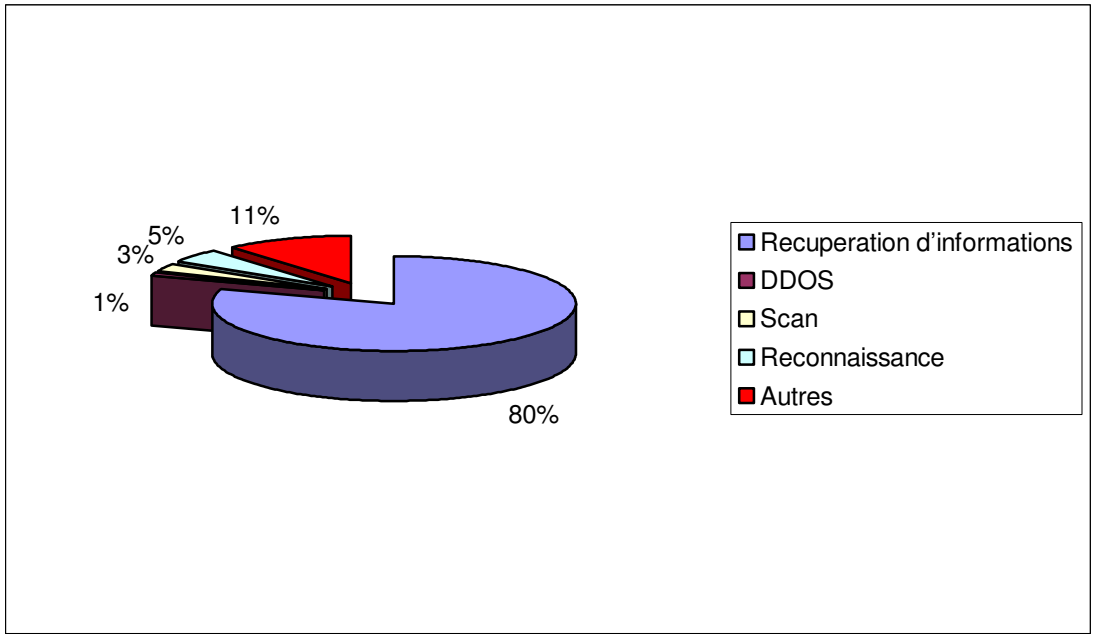
3. Attaques recensées contre la machine 172.55.55.1(routeur)

ATTAQUE	BUT ?	PORT VISE	PROTOCOLE	NB DE TENTATIVES	IP DE L'ATTAQUANT	COMMENTAIRES
SNMP request udp	Recuperation d'informations	161	SNMP	592	172.16.80.250	L'attaquant envoie un paquet sur le port 161 de udp et attend une réponse du demon SNMP pour tenter une attaque
SNMP public access udp	Recuperation d'informations	161	SNMP	82	172.16.80.250	SNMP v1 possede un champ *community* qui par défaut est *public ou private* sur beaucoup d'implémentations.
SNMP private access udp	Recuperation d'informations	161	SNMP	22	172.16.80.250	SNMP v1 possede un champ *community* qui par défaut est *public ou private* sur beaucoup d'implémentations.
SCAN Amanda client version request	Scan de ports			18	172.16.80.250	
ICMP PING NMAP	Reconnaissance	Tous	ICMP	17	172.16.80.250	L'attaquant a utilisé Nmap pour voir quels sont les hotes actifs du réseau.
SNMP missing community string attempt	Recuperation d'informations	161	SNMP	16	172.16.80.250	Une communication SNMP a été etablie sans nom de communauté.
MS-SQL ping attempt	Recherche d'une base MS-SQL	1434		12	172.16.80.250	L'attaquant semble avoir utilisé Nessus pour chercher l'existence d'une base MS-SQL.
DNS named version attempt	Reconnaissance	53	DNS	12	172.16.80.250	L'attaquant a tenter de découvrir la version de BIND utilisée et donc de savoir si la machine heberge un serveur de nom.
SNMP trap udp	Recuperation d'informations	162	SNMP	12	172.16.80.250	L'attaquant envoie un trap et attend une réponse du demon.
(spo_bo) Back Orifice Traffic detected				12	172.16.80.250	
MISC UPnP malformed advertisement	Deni de service ou accès non autorisé	1900	UPnP	10	172.16.80.250	L'attaquant utilise un exploit connu pour envoyer un *Notify* malformé qui va provoqué un buffer overflow.
DNS named authors attempt	Reconnaissance	53	DNS	6	172.16.80.250	Cette attaque permet à l'auteur de savor si la version de BIND utilisée est 9.x ou non.
TFTP Get		69	TFTP	6	172.16.80.250	
SNMP request tcp	Recuperation d'informations	161	SNMP	6	172.16.80.250	L'attaquant envoie un paquet sur le port 161 de tcp et attend une réponse du demon SNMP pour tenter une attaque.
SNMP trap tcp	Recuperation d'informations	162	SNMP	6	172.16.80.250	L'attaquant envoie un trap et attend une réponse du demon.
SNMP AgentX/tcp request	Deni de service	705	SNMP	6	172.16.80.250	L'attaquant peut essayer d'utiliser un exploit connu et envoyé un paquet malformé pour tenter un deni de service ou l'execution de code.
MISC AFS access	Accèe non autorisé	7001	UDP	4	172.16.80.250	AFS est un système de fichiers partagés utilisant des ACL. L'attaquant a tenté d'accéder à AFS malgré ces ACL.
SynScan	Scan de ports furtif	tous	TCP	4	172.16.80.250	L'attaquant envoie des paquets TCP avec le flag SYN armé et attend une réponse de type SYN ACK pour connaître les ports ouverts.

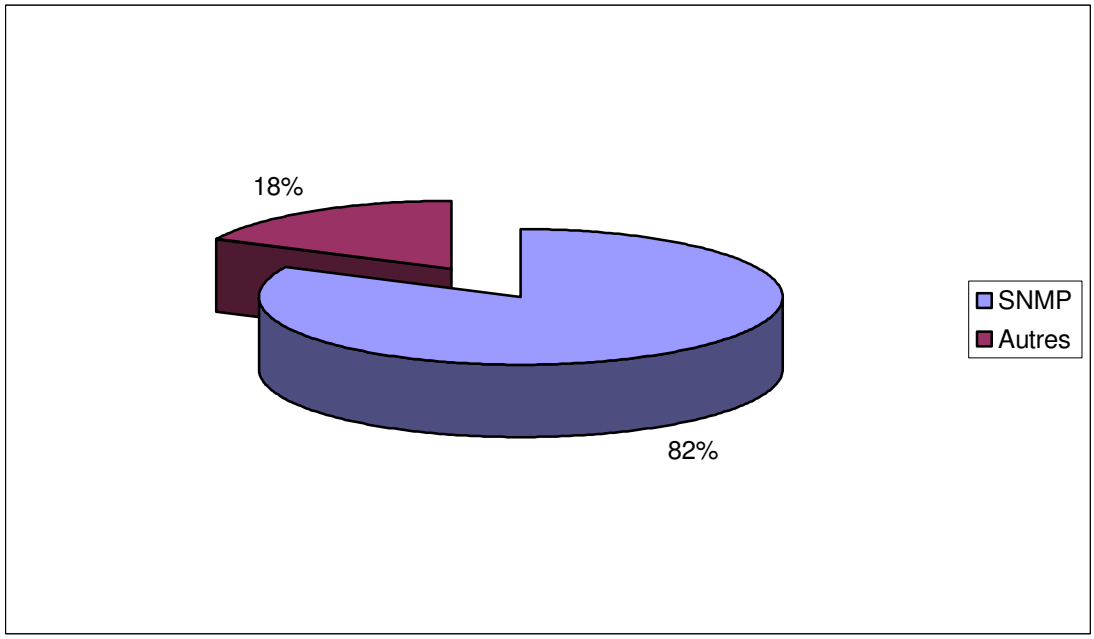
TFTP GET passwd	Reconnaissance	69	TFTP	4	172.16.80.250	Il semblerait que l'attaquant ait essayé de scaner le réseau à la recherche de serveurs TFTP.
MISC source route lssr	Informations sur la topologie du réseau			3	172.16.80.250	L'attaquant semble avoir tenté de découvrir la topologie du réseau en utilisant des outils comme traceroute.
MISC source route lssre				3	172.16.80.250	L'attaquant a tenté avec des paquets routés par la source de modifier la configuration de la machine en termes de sourcerouting(exploit pour W9x et NT)
MISC xdmcp info query		177	UDP	2	172.16.80.250	L'attaquant tente de se connecter en XDMCP
DDOS shaft handler to agent	Deni de service distribué	18753	UDP	2	172.16.80.250	
DDOS TFN Probe	Deni de service distribué			2	172.16.80.250	L'attaquant a essayé de corrompre un host en le faisant devenir client TFN(tribal flood network) puis a tenté de communiquer avec lui.
DDOS Trin00 Master to Daemon default password attempt	Deni de service distribué	27444	UDP	2	172.16.80.250	L'attaquant a essayé de corrompre un host en lui plaçant un démon puis a tenté de communiquer avec ce démon(en utilisant un paquet udp port 27444 avec la chaîne "144adsl" dans le payload) pour lancer des attaques.
TFTP root directory	Execution de code ou vole de fichiers	69	TFTP	2	172.16.80.250	L'attaquant a essayé d'utiliser un exploit dans TFTP qui peut permettre l'execution de code ou bien le vol de fichiers.
DDOS mstream client to handler	Deni de service distribué	15104	UDP	2	172.16.80.250	L'attaquant a essayé de corrompre un host en le faisant mstream handler puis a tenté de communiquer avec lui pour lancer des attaques.
DDOS mstream handler ping to agent	Deni de service distribué	10498	UDP	2	172.16.80.250	L'attaquant a essayé de corrompre un host en le faisant mstream handler puis verifie si les autres agents sont actifs(en utilisant un paquet UDP port 10498 avec la chaine "ping" comme payload)
TFTP parent directory	Execution de code ou vole de fichiers	66	TFTP	2	172.16.80.250	L'attaquant a essayé d'utiliser un exploit dans TFTP qui peut permettre l'execution de code ou bien le vol de fichiers.
TOTAL				**869**		

4. Statistiques des attaques contre 172.55.55.1

Types d'attaques :



Protocoles :



5. Autres attaques

Ce soir là nous avons également observé 14 ICMP redirect host avec comme adresse IP source 172.16.80.1:

- 3 à destination de 172.16.80.251
- 11 à destination de 172.16.80.250

Ceci signifie que l'attaque a tenté de se faire passer pour la machine 172.16.80.1(serveur DNS?) pour intercepter du trafic.

VII. Attaques du 2 novembre 2004

ATTAQUE	BUT ?	PORT VISE	PROTOCOLE	NB DE TENTATIVES	IP DE L'ATTAQUANT	COMMENTAIRES
ICMP Redirect Host	Interception du trafic		ICMP	82	172.16.80.250	L'attaquant a tenté de se faire passer pour la machine 172.16.80.1(serveur DNS?) pour intercepter du trafic
ICMP Redirect Host	Interception du trafic		ICMP	21	172.16.80.61	L'attaquant a tenté de se faire passer pour la machine 172.16.80.1(serveur DNS?) pour intercepter du trafic
ICMP Redirect Host	Interception du trafic		ICMP	2	172.16.80.71	L'attaquant a tenté de se faire passer pour la machine 172.16.80.1(serveur DNS?) pour intercepter du trafic
TOTAL				**105**		

VIII. Attaques du 3 novembre 2004

1. Attaques recensées contre la machine 172.77.77.100(client XP)

ATTAQUE	BUT ?	PORT VISE	PROTOCOLE	NB DE TENTATIVES	IP DE L'ATTAQUANT	COMMENTAIRES
BAD-TRAFFIC loopback traffic	DoS			16836	Adresses Spoofées (adresses de loopback)	L'attaquant a essayé d'envoyer un très grand nombre de paquets(avec des adresses sources spoofées)au client.
SNMP trap tcp	Recuperation d'informations ou DoS	162	SNMP	45	Adresses Spoofées	L'attaquant envoie un trap et attend une réponse du demon. Tentative de DoS
SNMP AgentX/tcp request	Deni de service (DoS)	705	SNMP	41	Adresses Spoofées	L'attaquant peut essayer d'utiliser un exploit connu et envoyé un paquet malformé pour tenter un deni de service ou l'execution de code.
SNMP request tcp	Recuperation d'informations ou DoS	161	SNMP	38	Adresses Spoofées	L'attaquant envoie un paquet sur le port 161 de tcp et attend une réponse du demon SNMP pour tenter une attaque. Tentative de DoS
SNMP trap udp	Recuperation d'informations	162	SNMP	2	172.16.80.250	L'attaquant envoie un trap et attend une réponse du demon.
SNMP request udp	Recuperation d'informations	161	SNMP	2	172.16.80.250	L'attaquant envoie un paquet sur le port 161 de udp et attend une réponse du demon SNMP pour tenter une attaque
ICMP PING NMAP	Reconnaissance	Tous	ICMP	2	172.16.80.250	L'attaquant a utilisé Nmap pour voir quels sont les hotes actifs du réseau.
DOS Bay/Nortel Nautica Marlin	DoS	161	SNMP	2	172.16.80.250	Si un pont Bay/Nortel Nautica Marlin recoit une cette requette il va etre mi hors d'usage => DoS
TOTAL				**16968**		

2. Attaques recensées contre la machine 172.66.66.5 (Serveur Web)

ATTAQUE	BUT ?	PORT VISE	PROTOCOLE	NB DE TENTATIVES	IP DE L'ATTAQUANT	COMMENTAIRES
(http_inspect) NON-RFC HTTP DELIMITER		80	HTTP	86	172.16.80.250	
TOTAL				**86**		

3. Autres attaques

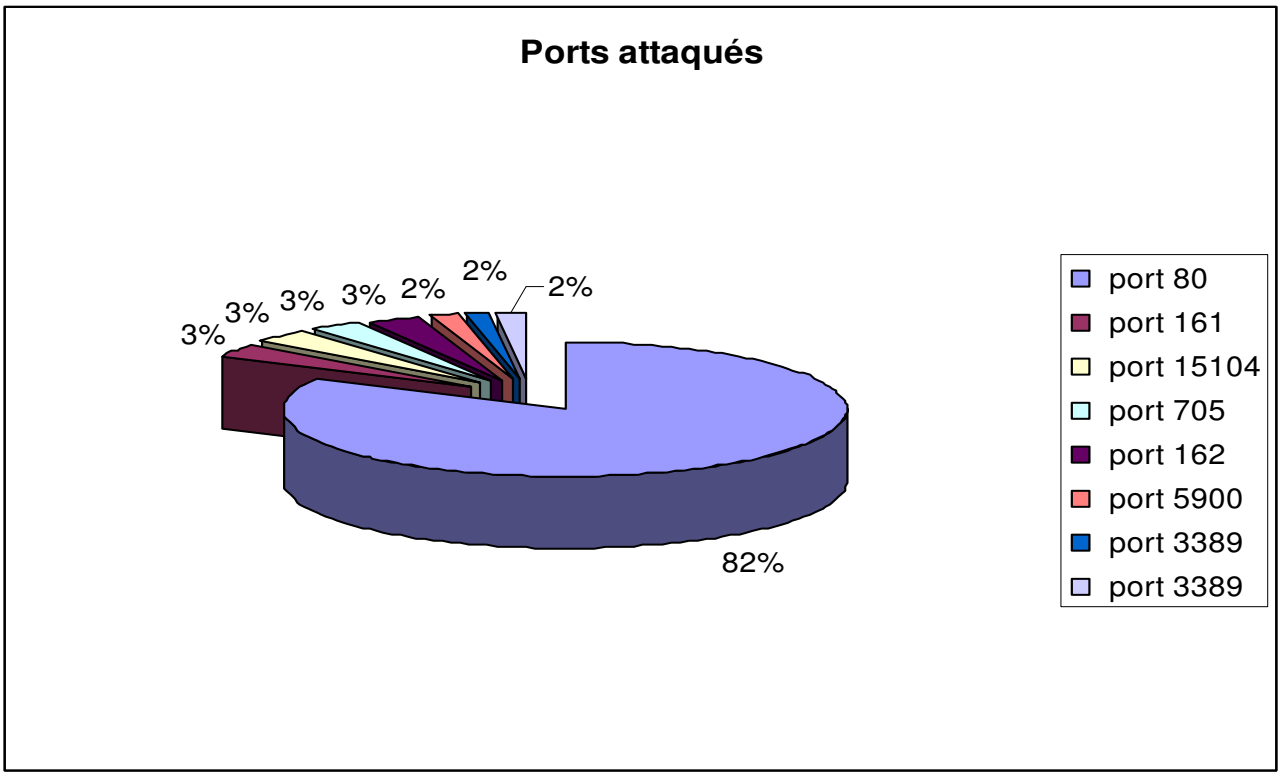
ATTAQUE	BUT ?	PORT VISE	PROTOCOLE	NB DE TENTATIVES	IP DE L'ATTAQUANT	COMMENTAIRES
ICMP Redirect Host	Interception du trafic		ICMP	63	172.16.80.250	L'attaquant a tenté de se faire passer pour la machine 172.16.80.1(serveur DNS?) pour intercepter du trafic
ICMP Redirect Host	Interception du trafic		ICMP	2	172.16.80.62	L'attaquant a tenté de se faire passer pour la machine 172.16.80.1(serveur DNS?) pour intercepter du trafic
TOTAL				**65**		

RAPPORT DU 14 OCTOBRE 2004

I. Attaques recensées contre le serveur Web (172.66.66.5)

ATTAQUE	CLASSIFICATION	PRIORITE	PORT VISE(TCP)	NB DE TENTATIVES	IP DE L'ATTAQUANT	REUSSIE ?
SynSCAN	Scan furtif		Tous	1	172.16.80.250	**OUI**
SNMP request TCP	Vol d'information	2	161	2	172.16.80.250	NON
DDOS mstream client to handler	Deni de service	2	15104	2	172.16.80.250	NON
SNMP AgentX/tcp request	Vol d'information	2	705	2	172.16.80.250	NON
SNMP trap tcp	Vol d'information	2	162	2	172.16.80.250	NON
POLICY VNC server response		3	5900	1	172.16.80.250	**OUI**
MISC MS Terminal server request RDP	Deni de service	3	3389	2	172.16.80.250	**OUI**
WEB-ATTACKS id command attempt	Attaque web	1	80	14	172.16.80.250	?
WEB-MISC whisker tab splice attack	Vol d'information	2	80	35	172.16.80.250	?
WEB-MISC http directory traversal	Vol d'information	2	80	2	172.16.80.250	?
WEB-MISC whisker space splice attack	Vol d'information	2	80	1	172.16.80.250	?
DOS Cisco attempt	Attaque web	1	80	1	172.16.80.250	?

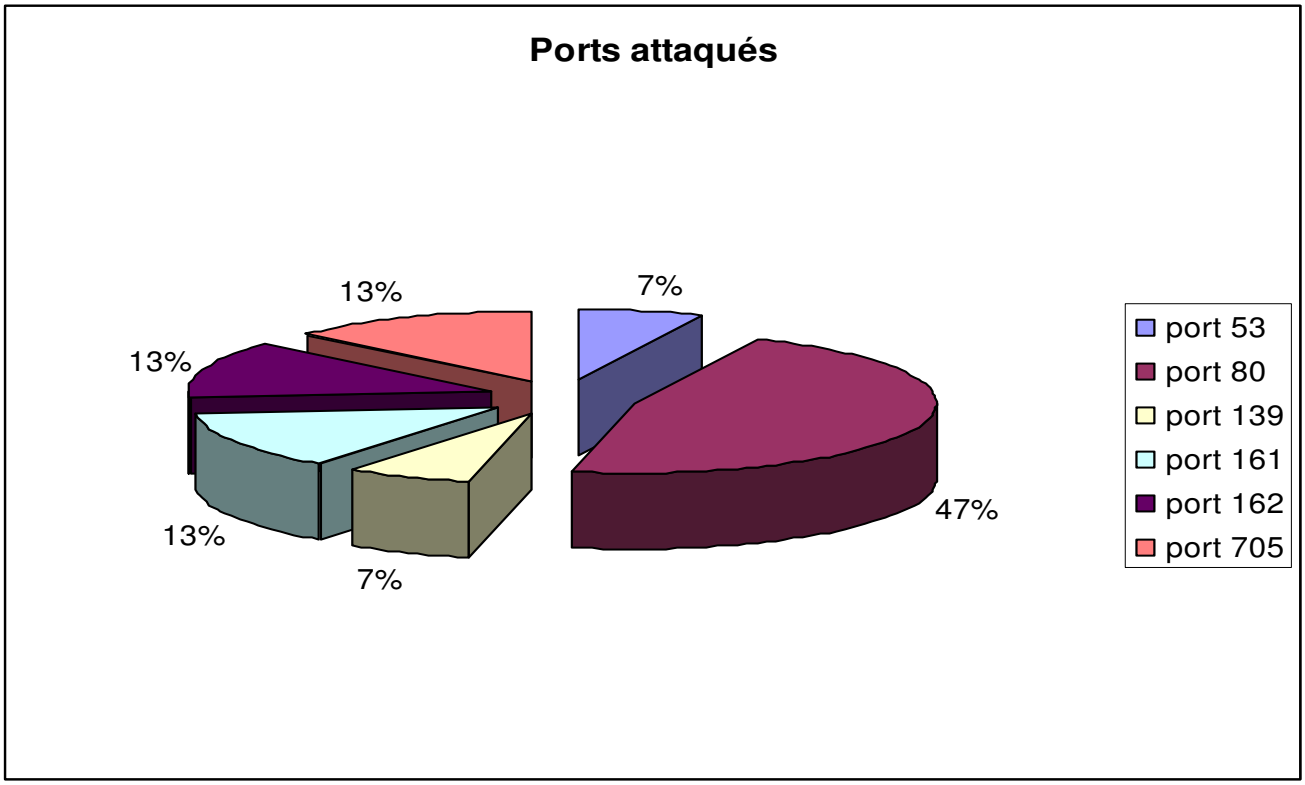
Ci dessous un graphique représentant la quantité d'attaques par port.



X. Attaques recensées contre le serveur BD (172.66.66.6)

ATTAQUE	CLASSIFICATION	PRIORITE	PORT VISE(TCP)	NB DE TENTATIVES	IP DE L'ATTAQUANT	REUSSIE ?
SynSCAN	Scan furtif		Tous	1	172.16.80.250	**OUI**
SNMP AgentX/tcp request	Vol d'information	2	705	2	172.16.80.250	?
SNMP trap tcp	Vol d'information	2	162	2	172.16.80.250	?
DDOS mstream client to handler	Deni de service	2	15104	2	172.16.80.250	?
SNMP request TCP	Vol d'information	2	161	2	172.16.80.250	?
DNS named version attempt	Vol d'information	2	53	1	172.16.80.250	?
WEB-IIS encoding access	Accès à une appli web vulnérable	2	80	3	172.16.80.250	?
WEB-ATTACKS id command attempt	Attaque web	1	80	2	172.16.80.250	?
WEB-MISC http directory traversal	Vol d'information	2	80	2	172.16.80.250	?
NETBIOS SMB IPC$ share access		3	139	1	172.16.80.250	?

Ci dessous un graphique représentant la quantité d'attaques par port sur la machine 172.66.66.6.

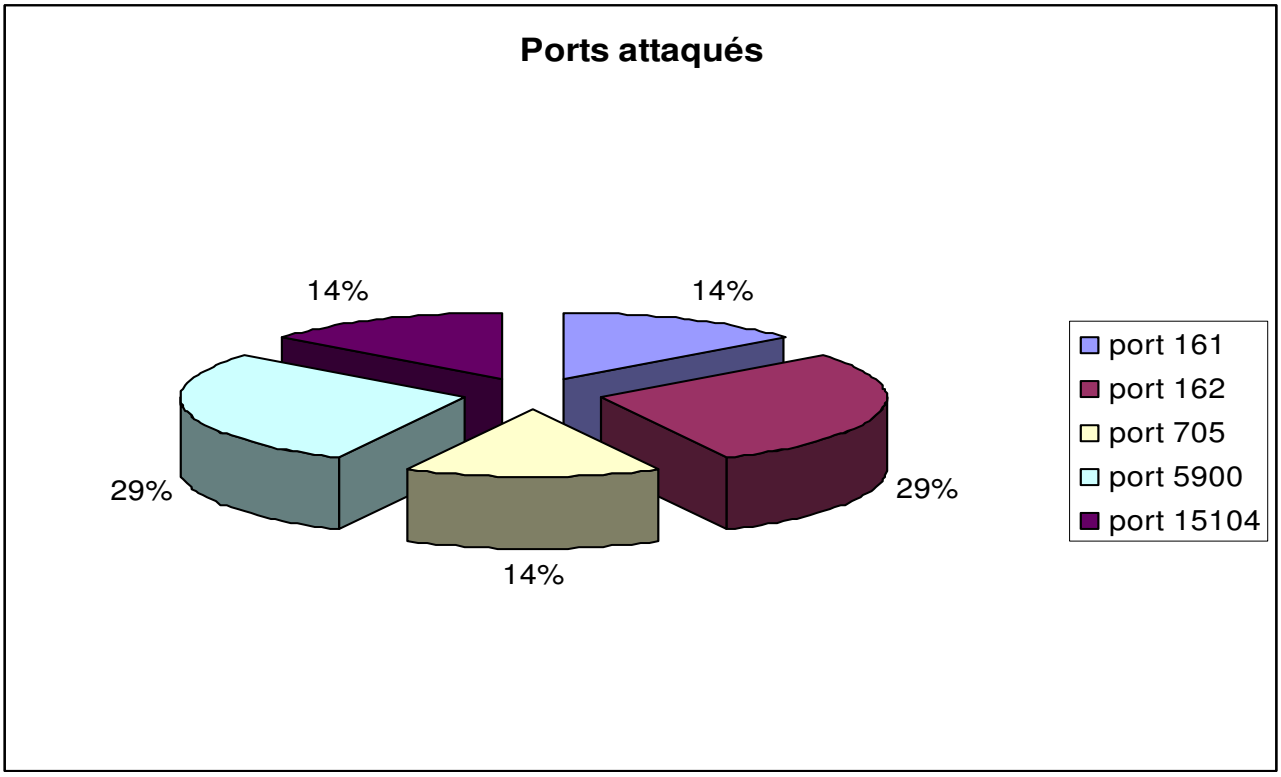


XI. Attaques recensées contre le poste client (172.66.66.100)

ATTAQUE	CLASSIFICATION	PRIORITE	PORT VISE(TCP)	NB DE TENTATIVES	IP DE L'ATTAQUANT	REUSSIE ?
SynSCAN	Scan furtif		Tous	1	172.16.80.250	**OUI**
POLICY VNC server response		3	5900	2	172.16.80.251	**OUI**
SNMP trap tcp	Vol d'information	2	162	2	172.16.80.250	?
SNMP request TCP	Vol d'information	2	161	1	172.16.80.250	?
SNMP AgentX/tcp request	Vol d'information	2	705	1	172.16.80.250	?
DDOS mstream client to handler	Deni de service	2	15104	1	172.16.80.250	?

Ci dessous un graphique représentant la quantité d'attaques par port sur la machine 172.66.66.100

XII.

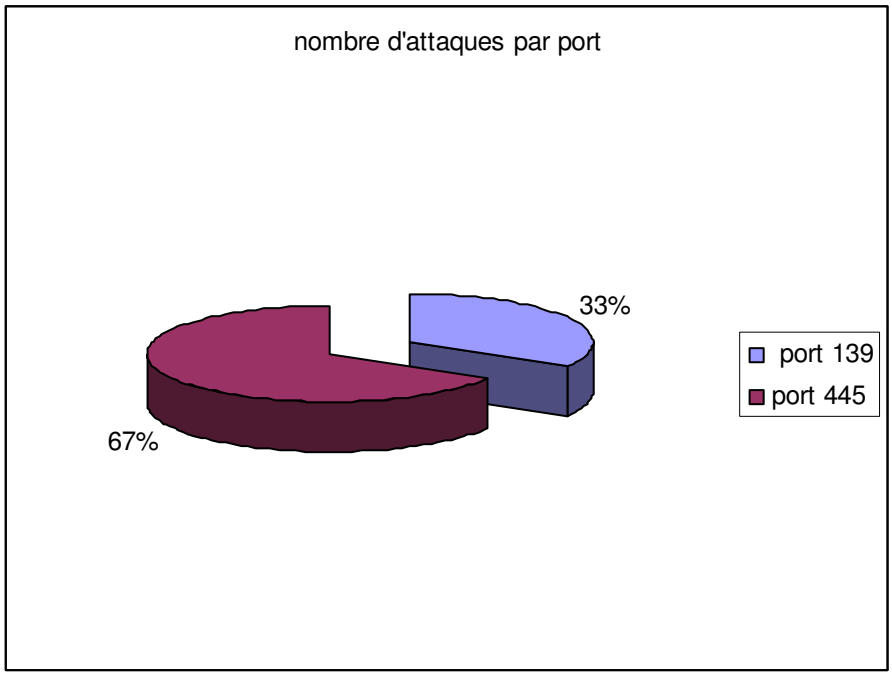


RAPPORT DU 18 OCTOBRE 2004

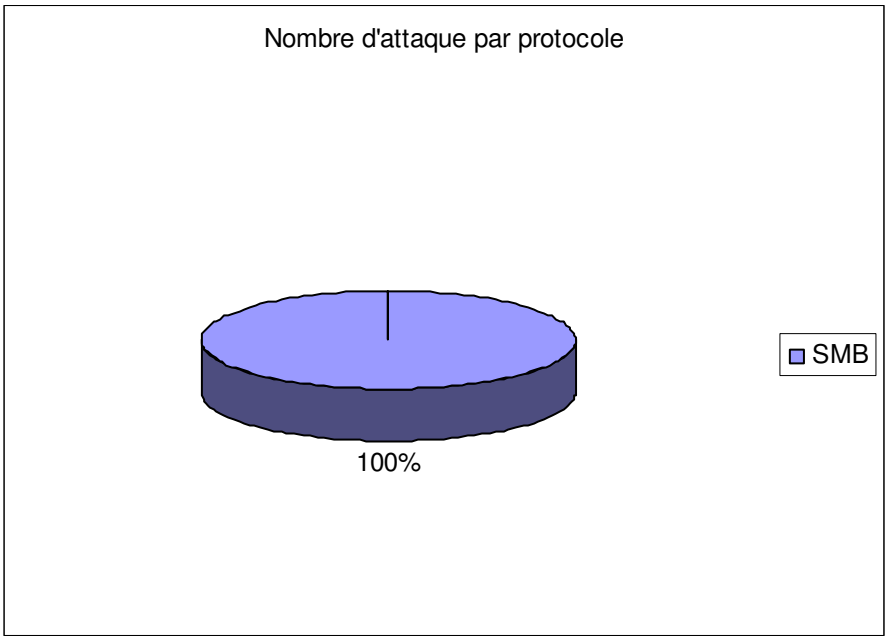
I. .Attaques recensées contre le serveur Web (172.66.66.5)

ATTAQUE	CLASSIFICATION	PRIORITE	PORT VISE	PROTOCOLE	NB DE TENTATIVES	IP DE L'ATTAQUANT	REUSSIE ?
NETBIOS SMB share access		3	TCP 139	SMB	5	172.16.80.250	NON
NETBIOS SMB-DS DCERPC NTLMSSP asn1 overflow attempt	tentative d'appropriation de droits admin	1	TCP 445	SMB	7	172.16.80.251	
NETBIOS SMB-DS Session Setup AndX request unicode username overflow attempt	tentative d'appropriation de droits admin	1	TCP 445	SMB	3	172.16.80.251	
TOTAL					**15 tentatives**		

Ci dessous un graphique représentant la quantité d'attaques par port.



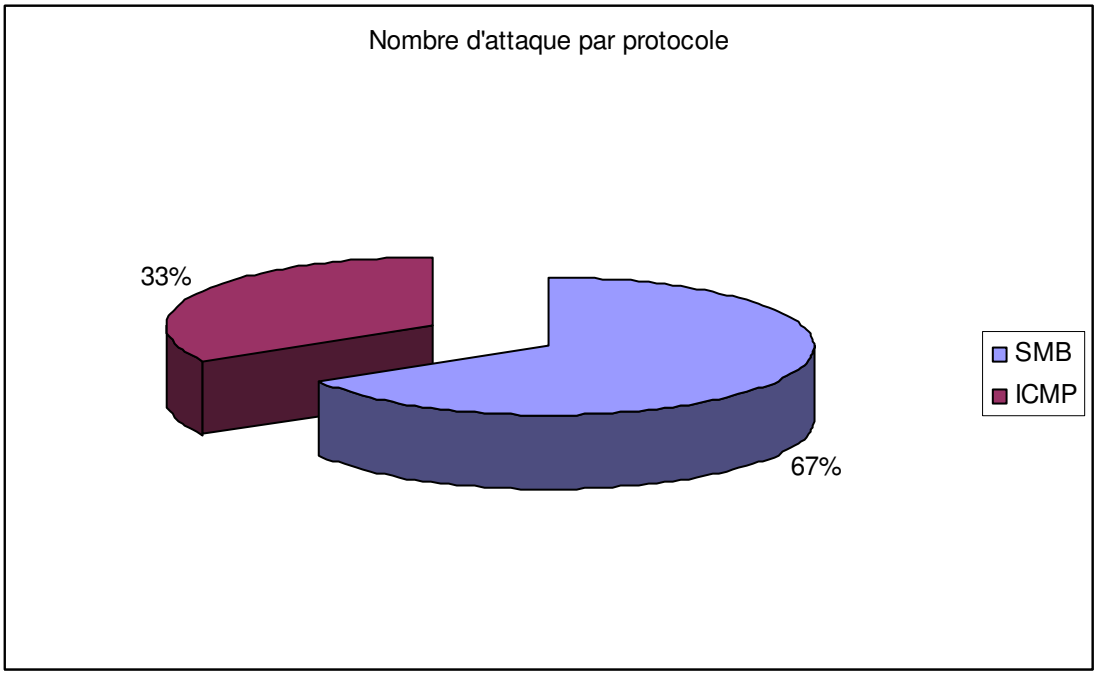
Et un autre graphique représentant le nombre d’attaques par protocole



II. Attaques recensées contre le serveur BD (172.66.66.6)

ATTAQUE	CLASSIFICATION	PRIORITE	PORT VISE	PROTOCOLE	NB DE TENTATIVES	IP DE L'ATTAQUANT	REUSSIE
ICMP Destination Unreachable Fragmentation Needed and DF bit was set		3		ICMP	1	172.16.80.1	
NETBIOS SMB share access		3	TCP 139	SMB	2	172.16.80.250	NON
TOTAL					**3 tentatives**		

Ci dessous un graphique représentant la quantité d'attaques par protocole sur la machine 172.66.66.6.



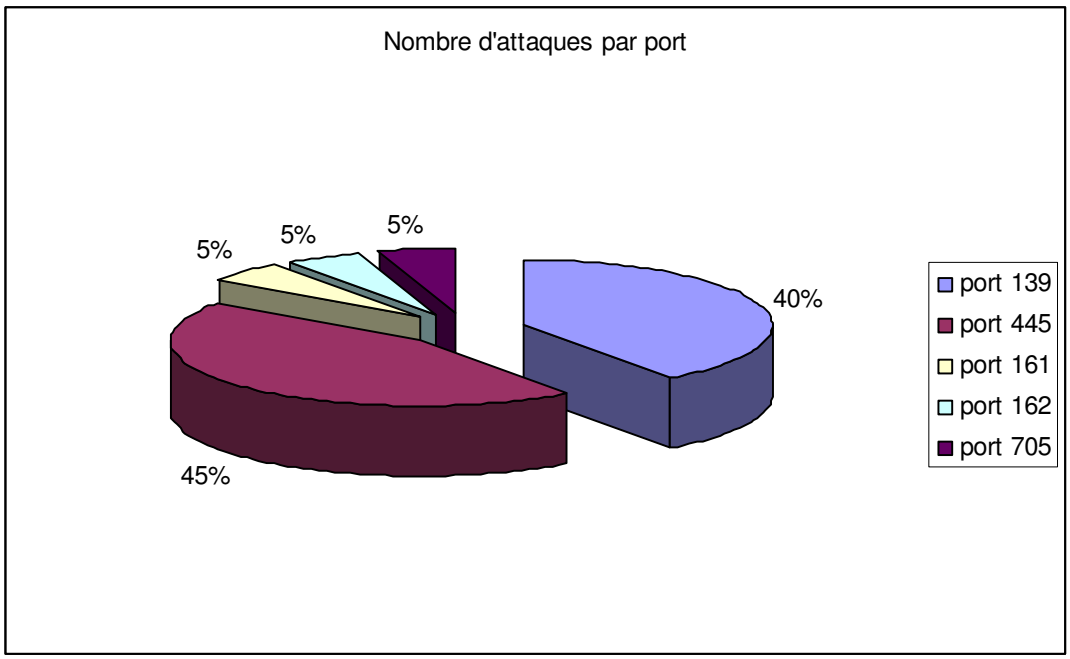
III. Attaques recensées contre le poste client (172.66.66.100)

Aucune attaque n'a été portée contre le client.

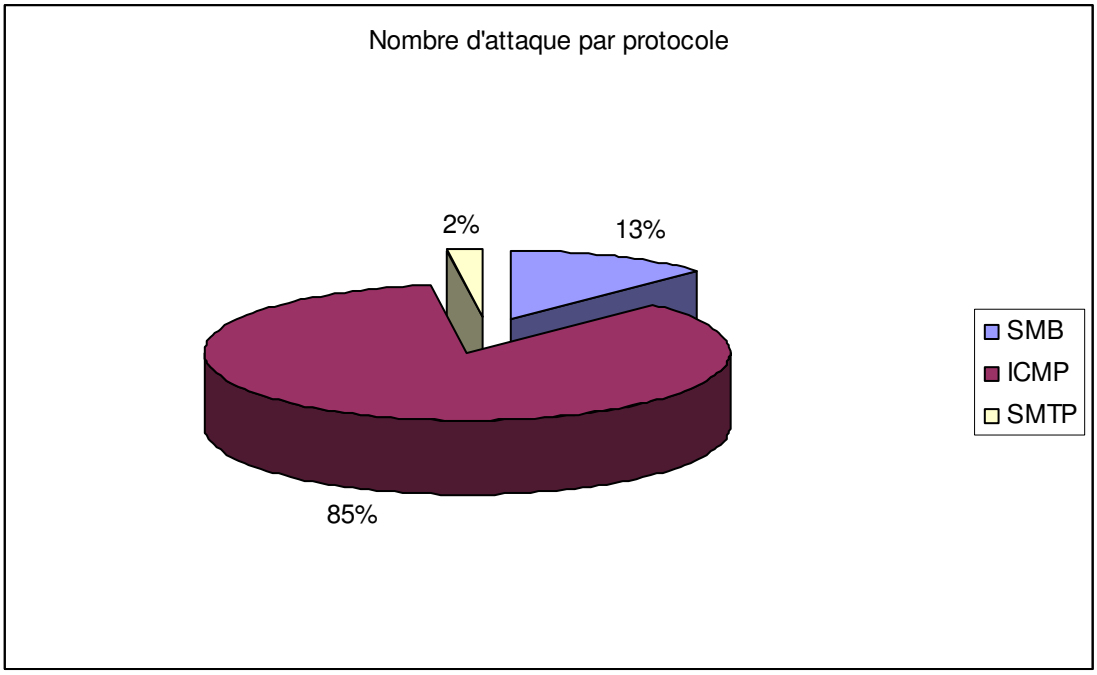
IV. Attaques recensées contre la machine 172.66.66.81

ATTAQUE	CLASSIFICATION	PRIORITE	PORT VISE	PROTOCOLE	NB DE TENTATIVES	IP DE L'ATTAQUANT	REUSSIE
SynScan	Scan de ports furtif					172.16.80.250	OUI
ICMP Destination Unreachable Fragmentation Needed and DF bit was set		3		ICMP	115	172.16.80.1	
SNMP request tcp	Vol d'information	2	TCP 161	SNMP	1	172.16.80.250	NON
SNMP trap tcp	Vol d'information	2	TCP 162	SNMP	1	172.16.80.250	NON
SNMP AgentX/tcp request	Vol d'information	2	TCP 705	SNMP	1	172.16.80.250	NON
NETBIOS SMB share access		3	TCP 139	SMB	7	172.16.80.250	NON
NETBIOS SMB-DS DCERPC NTLMSSP asn1 overflow attempt	tentative d'appropriation de droits admin	1	TCP 445	SMB	9	172.16.80.251	NON
NETBIOS SMB DCERPC NTLMSSP asn1 overflow attempt	tentative d'appropriation de droits admin	1	TCP 139	SMB	1	172.16.80.251	NON
TOTAL					**135 tentatives**		

Ci dessous un graphique représentant la quantité d'attaques par port sur la machine 172.66.66.81.



Et un autre graphique représentant le nombre d'attaques par protocole :



Détails des failles déterminées par Snort

Sources : http://www.snort.org/snort-db/

WEB-IIS encoding access

Message	WEB-IIS encoding access
Résumé	Cet événement se produit lors d'une tentative d'exploitation d'une vulnérabilité connue du serveur web IIS du serveur Microsoft.
Impact	Les informations et l'intégrité du système sont compromis. Accès possible avec les droits admin non autorisé au serveur ou à l'application. Deny of Service possible.
Détail	Cet événement se produit lorsqu'une tentative est faite de compromettre un serveur utilisant IIS de Microsoft . De nombreuses vulnérabilités sont connus sur cette plateforme.
Systèmes Affectés	Tous les systèmes utilisant Microsoft IIS
Scénarios d'Attaque	Beaucoup de vecteurs d'attaque sont possibles dans des conditions de débordement de tampon.
Facilité d'attaque	Simple. Beaucoup d'exploits existent.
Modalité de reprise	S'assurez que le système emploie une version à jour du logiciel et appliquer tous les patchs fournis par Microsoft.

DNS named version attempt

Message	DNS named version attempt
Résumé	Cet événement est produit quand une tentative est faite pour déterminer la version du BIND utilisé sur un serveur DNS.
Impact	Cette activité peut indiquer une attaque imminente.
Détail	Une machine à distance a essayé de déterminer la version du BIND fonctionnant sur un serveur DNS.
Systèmes Affectés	Tous les serveur de DNS
Scénarios d'Attaque	En tant qu'élément de la reconnaissance menant jusqu'à une tentative potentielle d'intrusion, l'attaquant peut essayer de déterminer la version de BIND qui est en service. Ainsi, une version vulnérable peut être employée comme vecteur d'attaque.
Facilité d'attaque	Simple.

Correctif	Neutralisez les capacités pour des machines distantes à déterminer le nom de la version.

Netbios SMB share Access

Message	Netbios SMB share Access
Résumé	Cet événement se produit lorsqu'une tentative est faite d'accéder aux partages par défaut d'un hote Windows.
Impact	Sérieux. Accès possible d'administration à l'hote. Révélation d'informations.
Détail	Par défaut, les hotes Windows utilisent le format %DRIVE_LETTER% + $ pour leur partage par défaut des disques durs. N'importe qui peut accéder à distance aux partages avec les droits d'administration.
Systèmes Affectés	Hotes Windows.
Scénarios d'Attaque	Un attaquant peut essayer d'accéder à des dossiers localisés sur lecteur C de l'hote.
Facilité d'attaque	Simple.
Correctif	Rejetez l'accès Netbios des réseaux externes (port 139 de tcp).

DOS Cisco attempt

Message	DOS Cisco attempt
Résumé	Cet événement est produit quand un potentiel Dénie de Service (DoS) est détecté sur le réseau.
Impact	Sérieux. Une attaque de DoS peut être en cours.
Détail	Cet événement indique qu'un trafic de DoS a été détecté. Un hacker peut être en train d'essayer d'épuiser des ressources sur une machine, rendant cette machine indisponible pour un usage légitime.
Systèmes Affectés	tous
Facilité d'attaque	Simple à difficile.

Correctif	Exécutez une analyse appropriée sur la machine suspecté pour découvrir les moyens de compromission.Puis utiliser un Firewall pour bloquer le trafic inadéquat.

WEB_MISC whisker space splice attack

Message	WEB_MISC whisker space splice attack
Résumé	Cet événement se produit quand une tentative est faite pour tester un IDS dans une possible attaque WEB en envoyant une requête cachée dans de petits morceaux.
Détail	Dans des circonstances normales, une requête WEB correspond à un paquet. Cependant, il est possible de dissimuler une attaque WEB en envoyant un caractère à la fois. Ceci peut permettre d'éviter les systèmes de détection d'intrusions. Des outils comme whisker peuvent être configurer pour faire cela.
Systèmes Affectés	Tous les Serveurs Web
Scénarios d'Attaque	Un attaquant peut utiliser un outil automatisé, comme whisker, pour lancer une attaque contre un web server.
Facilité d'attaque	Simple. Les exploits et les outils sont largement disponibles.
correctif	Examinez le serveur web pour détecter des signes de compromissions

---

NETBIOS SMB-DS DCERPC NTLMSSP asn1 overflow attempt

Message	NETBIOS SMB-DS DCERPC NTLMSSP asn1 overflow attempt
Résumé	Cet événement se produit lors d'une tentative d'exploitation d'une vulnérabilité connue au niveau des bibliothèque ASN.1 de Microsoft
Impact	Sérieux. Exécution de code arbitraire, Deny of Service.

Détail	Une condition de débordement de tampon dans l'exécution des bibliothèques ASN.1 de Microsoft. Un hacker peut exploiter cette condition en envoyant des paquet d'authentification de manière astucieuse sur un système d'exploitation vulnérable Quand le système cible décode les données ASN.1, le code peut être inclus dans les données qui vont être exécutées sur le serveur avec des droits de niveau système. Le service peut ainsi ne plus répondre, ce qui entraîne l'état Deny of Service attendu.
Systèmes Affectés	Microsoft Windows NT Microsoft Windows NT Terminal Server Edition Microsoft Windows 2000 Microsoft Windows XP Microsoft Windows 2003
Facilité d'attaque	Simple. Le code d'exploit existe.
Modalité de reprise	Appliquez les patchs fournis par Microsoft

---

NETBIOS SMB-DS Session Setup AndX request unicode username overflow attempt

Message	NETBIOS SMB-DS Session Setup AndX request unicode username overflow attempt
Résumé	Cet événement se produit produit lors d'une tentative d'exploitation d'une vulnérabilité connue dans ISS RealSecure et les produits de BlackICE.
Impact	Sérieux. Exécution du code arbitraire, Deny of Service.
Détail	Une condition de débordement de tampon dans le module d'analyse d'ISS peut être déclenchée par un attaquant envoyant un paquet simple de SMB contenant un AccountName supérieur à 300 bytes. Lorsqu'un system utilise un produit ISS affecté, il va décoder les paquets SMB incluant le code exploit qui va s'exécuter sur la machine avec des privilèges de niveau de système. Le service peut ainsi ne plus répondre, ce qui entraîne l'état Deny of Service attendu.

Systèmes Affectés	RealSecure Network 7.0, XPU 20.15 through 22.9 Real Secure Server Sensor 7.0 XPU 20.16 through 22.9 Proventia A Series XPU 20.15 through 22.9 Proventia G Series XPU 22.3 through 22.9 Proventia M Series XPU 1.3 through 1.7 RealSecure Desktop 7.0 eba through ebh RealSecure Desktop 3.6 ebr through ecb RealSecure Guard 3.6 ebr through ecb RealSecure Sentry 3.6 ebr through ecb BlackICE PC Protection 3.6 cbr through ccb BlackICE Server Protection 3.6 cbr through ccb
Scénarios d'Attaque	Un attaquant peut utiliser cette vulnérabilité pour neutraliser des sondes d'ISS sur le réseau ou pour prendre le contrôle d'une machine utilisant un des produits affectés.
Facilité d'attaque	Simple.
Modalité de reprise	Appliquez les patchs fournis par le fournisseur approprié.

WEB-MISC whisker tab splice attack

Message	WEB-MISC whisker tab splice attack
Résumé	Cet événement se produit quand une tentative est faite pour tester un IDS dans une possible attaque WEB en envoyant une requête cachée dans des tabulations.
Impact	Inconnu.
Détail	Quelques serveurs WEB (par exemple, certaines versions d'Apache) interpréteront des tabulations comme des espaces dans des requêtes WEB. Ceci est employé par quelques outils (par exemple, whisker) afin d'essayer d'éviter des IDS.
Systèmes Affectés	Tous les systèmes utilisant un serveur web.
Scénarios d'Attaque	Un attaquant utilise un outil automatisé, comme whisker, contre un serveur web, ou peut essayer une attaque manuelle avec une URL semblable à GET<tab>/<tab>HTML/1.0
Facilité d'attaque	Simple. Les outils automatisés sont disponibles.
Correctif	Examiner le paquet pour voir si une requête WEB a été faite. Essayez de déterminer ce qu'était l'élément demandé (par exemple, un fichier ou un cgi), et déterminer à partir de la configuration du serveur web si c'est une menace ou pas (par exemple, si le fichier ou le cgi demandé existe ou s'il est vulnérable).

WEB-MISC http directory traversal

Message	WEB-MISC http directory traversal

Résumé	Cet événement se produit lors d'une tentative d'attaque par balayage de répertoire.
Impact	Révélation de l'information, exposition possible d'information sensible du système.
Détail	Les attaques par balayage de répertoire visent habituellement des cibles WEB, des applications WEB et des serveurs ftp qui ne vérifient pas correctement le chemin d'un dossier dans les requêtes d'un client. Ceci peut mener à la révélation d'information sensible du système qui peut être utilisé par un attaquant pour compromettre encore plus le système.
Scénarios d'Attaque	Un utilisateur autorisé ou un utilisateur anonyme peut employer le balayage de répertoire, pour passer en revue des chemins hors du répertoire racine du serveur ftp. L'information recueilli peut être employé dans d'autres attaques contre le serveur WEB.
Facilité d'attaque	Simple. Aucun logiciel d'exploit n'est exigé.
Correctif	Appliquez les patchs fournis par le fournisseur approprié Mettre à jour le logiciel

---

MISC MS Terminal server request RDP

Message	MISC MS Terminal server request RDP (1:1447)
Résumé	Cet évènement se produit quand un paquet infecté est envoyé sur le port du serveur du terminal Microsoft.
Impact	Deny of service. L'envoi répété de paquets infectés peut causer un DoS en consommant toutes les ressources de mémoire disponibles.
Détail	Une faille existe sur le port du serveur terminal de Microsoft sur certaines versions de Windows qui peuvent causer un DoS du serveur en consommant toutes les ressources de mémoire disponibles.
Systèmes affectés	Microsoft Windows 2000 Advanced Server SP2 Microsoft Windows 2000 Advanced Server SP1 Microsoft Windows 2000 Advanced Server Microsoft Windows 2000 Datacenter Server SP2 Microsoft Windows 2000 Datacenter Server SP1 Microsoft Windows 2000 Datacenter Server Microsoft Windows 2000 Server SP2 Microsoft Windows 2000 Server SP1 Microsoft Windows 2000 Server Microsoft Windows NT Terminal Server 4.0
Scénario	Un attaquant peut tenter un DoS sur le serveur en envoyer plusieurs paquets infectés.
Difficulté de l'attaque	Simple.
Corrective Action	Il faut appliquer les patches Microsoft Security Bulletin MS01-040. Bloquer l'accès au port du serveur Microsoft depuis le réseau.

WEB-ATTACKS id command attempt

Message	WEB-ATTACKS id command attempt (1:1333)
Résumé	Tentative d'accès via internet par la commande id.
Impact	Tentative d'accéder aux informations sur les utilisateurs et groupes qui existent sur la machine en utilisant la commande id.
Détail	C'est une attaque permettant d'obtenir des informations sur les utilisateurs du serveur web. « id » est une commande UNIX qui retourne les informations système des utilisateurs et groupes. Ces informations sont très utiles pour un hacker qui souhaite connaître les login et mot de passe des utilisateurs. Cette attaque est d'autant plus efficace pour connaître les utilisateurs et groupes qui possèdent de nombreux privilèges. Cette commande « id » retourne les informations sur les utilisateurs (gid et uid) et sur les groupes. La règle ne détecte pas si la commande "id" a réussi à trouver les informations de l'utilisateur. La présence de la commande « id web traffic » indique qu'un hacker tente de se connecter au serveur web avec une session non valide. Autrement, cette règle peut déclencher une connexion tunnelling HTTP non cryptée au serveur ou peut déclencher une nouvelle connexion au serveur web.
Scénario	1. L'attaquant peut faire une requête HTTP standard qui contient '/usr/bin/id' dans l'URL qui peut alors retourner des informations sensibles sur les groupes et utilisateurs présents sur la machine. 2. Cette commande peut aussi être faite pour accéder à la machine d'un utilisateur. 3. L'attaquant utilise la commande "id" via une connexion au serveur web pour analyser quel utilisateur a une session ouverte sur le serveur web. Il cherche alors parmi les fichiers en écriture par l'utilisateur le fichier de configuration au serveur web.
Facilité de l'attaque	Il s'agit d'une simple requête http.
Correctif	Les serveurs web ne devraient pas autoriser de voir et d'exécuter les fichiers en dehors de ceux qui sont désigné par la table de routage ou en dehors des scripts cgi-bin.

Port 161 et 162 => SNMP request TCP and Trap TCP : Vol d'information
Port 705 => SNMP AgentX/tcp request : vol d'information

Les vulnérabilités du protocole SNMP en terme de requêtes de la version 1 de SNMP autorisent les attaques distantes pouvant causer des dénis de service ou des vols d'informations (gain de privilèges) par l'intermédiaire des messages GetRequest, GetNextRequest, et SetRequest.
Les attaques distantes utilisent également le système d'alertes SNMP (SNMP trap) pour causer les dénis de service et les gains de privilèges

N.B : c'est comme si la requête se fendait en plusieurs requêtes, une ou plusieurs requêtes pour les machines cibles. Ces messages SNM sont mis à jour lorsque les informations sont disponibles.

L'attaque distante envoie simplement une requête SNMP malformée au client SNMP créant ainsi un déni de service ou un vol d'information. L'appareil attaqué peu s'éteindre ou nécessiter un redémarrage dans le cas d'un déni de service.

Les vulnérabilities des messages d'alertes SNMP

Les traps SNMP sont des messages envoyés depuis un agent vers les stations d'administrations. Ils notifient l'administrateur qu'un évènement s'est produit ou fournit des information sur l'état de l'agent.
Les vulnerabilities du protocole SNMP sont reconnues exitantes au niveau du processus de décodage et d'interprétation des traps d'alertes.

Ainsi les conséquences possibles sont le déni de service et l'ouverture à d'autres attaques pouvant compromettre les machines affectées.
Microsoft a confirmé que les attaques distantes peuvent exécuter un code arbitraire sur les hôtes vulnérables si le service SNMP est activé.
HP a confirmé que la majorité des traps causeront des crashs du logiciel de supervision Openview Network Node Manager.

Port 15104 => DDOS mstream client to handler: déni de service

Sur le système, on trouve un programme d'attaque distribuée de déni de service d'installer tel qu'un maître, agent ou zombie. Par exemple (1) Trinoo, (2) Tribe Flood Network (TFN), (3) Tribe Flood Network 2000 (TFN2K), (4) stacheldraht, (5) mstream, ou (6) shaft.

IDS111 "TROJAN-ACTIVE-BLA"

Cet évènement indique qu'un trojan connu opère sur l'hôte. Ce n'est pas un scan, mais un e connexion réussie. Cet évènement est spécifique à une tâche particulière mais la charge du paquet n'est pas considérée comme une signature permettant de détecter l'attaque. Le paquet a été transmis avec une session TCP correctement établie indiquant que l'adresse IP source n'a pas été dérobée. SI on utilise un parefeu qui supporte l'inspection complète des états et qui n'est pas vulnérable au séquençage de nombres d'attaques, alors on peut certainement déduire que l'adresse IP source est exacte. En effet il est indiqué que l'émetteur attend ou désire une réponse à ces paquets (un acquittement) donc on est certain que l'adresse IP source n'a pas été volée. Il existe un rapport d'incidents où le trafic autorisé peut causer une détection d'intrusion au système, augmentant ainsi le

nombre de fausse alerte positive pour cet évènement Les détails suivants sont rapportés: La signature montre le port par défaut du trojan. Il est possible qu'un autre logiciel écoute sur le même port.

GEN:SID	1:249
Message	DDOS mstream client to handler
Rule	alert tcp $EXTERNAL_NET any -> $HOME_NET 15104 (msg:"DDOS mstream client to handler"; flow:stateless; flags:S,12; reference:arachnids,111; reference:cve,2000-0138; classtype:attempted-dos; sid:249; rev:8;)
résumé	Cet évènement est généré quand un client DDoS mstream prend contact avec une base de traitement mstream.
Impact	Severe. Si la source IP capture est sur notre réseau, ça peut être un client mstream. Si l'adresse IP destination est sur notre réseau, ça peut être la machine de traitement mstream.
Détails	Mstream DDoS utilise une structure d'hôtes compromise pour coordonner et participer à la distribution d'attaque de dénis de service. A un niveau supérieur, les clients communiquent avec les supports de traitement pour les informer du lancement des attaques. Un client peut contacter le support traitement en utilisant le packet TCP SYN à destination du port 15104.
Systèmes infectés	Un hôte mstream compromis.
Scénarios d'attaques	Après qu'un hôte ne devienne une base de traitement mstream, le client attend de rentrer en communication avec lui.
Diificulté d'attaque	Simple. Le code mstream est facilement disponible.
False Positives	Le port légitime 15104 causera cette règle. Cette règle va générer aussi une fausse alerte positive si le port 15104 est sélectionné comme un port FTP.
False Negatives	Il existe d'autres clients en adéquation avec le port 15104.
Correctifs	Analyser le serveur compromis pour en extraire les moyens de compromis. Reconstruire l'hôte infecté. Configurer le parefeu pour bloquer le trafic inapproprié que le réseau afin d'éviter d'éventuelles infections d'hôtes.