

Sécurité : les 11 commandements pour la PME
eric@netline.be

Forum telecom
10 décembre 2002

netline

Croissance exponentielle
des attaques



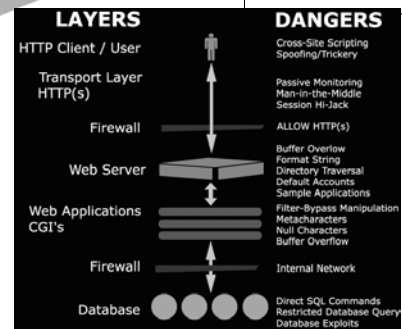
netline

11 points critiques

1. OCTAVE methodology
Operationally Critical Threat, Asset and Vulnerability
Evaluation methodology.
2. Authentication
3. Firewalls
4. Intrusion-detection systems
5. Virus scanners
6. Policy management software
7. Vulnerability testing
8. Encryption
9. Proper system administration
10. Active content filtering
11. Incident response plan/ continuity of operations

netline

Méthodologie



netline

Authentication

o [Http://www.10pht.com](http://www.10pht.com)

netline

Firewall

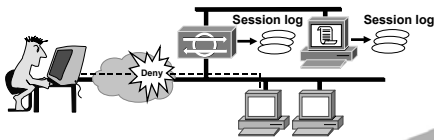
netline

Détection d'intrusion

- o BlackIce (<http://www.iss.net>)
- o Snort (<http://www.snort.org>)

IP Logging

capture automatique du trafic suspect



netPine

Virus SPAM

- o détection en ligne
 - <http://housecall.anti-virus.com>
 - <http://www.bitdefender.com>
- o spyware
- o trojan
- o <http://www.rootkit.com>
- o spamassassin
- o blacklist
- o MailScanner.info

netPine

© spamcop.net

Query bl.spamcop.net

Blocklist query for 207.202.47.156

207.202.47.156 is and should be blocked:1 spamtrap reports counted x2; 24.84% spam report rate exceeds 2% threshold

Traffic analysis: MetricQty.Most Recent

Total traffic:	157	Tue Mar 12 07:30:31 2002 GMT
Reported:	37	Mon Mar 11 22:33:10 2002 GMT
Relay Closed:	2	Sat Mar 9 16:55:44 2002 GMT
Traps:	1	Sat Mar 9 05:43:26 2002 GMT

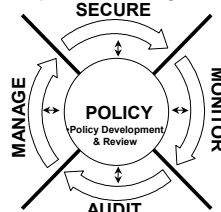
Listing history:

listed: Fri Mar 8 21:17:02 2002 GMT

netPine

Police de sécurité

- ID/Authentication
- Encryption & VPN
- Firewalls & ACLs
- Security Design & Implementation/Integration



- Logging and Event Notification
- Trend Analysis
- Management Reports
- Incident Response

- Real-Time Intrusion Detection & Response
- 7x24 Monitoring

- Vulnerability Scanning & Analysis
- Security Posture Assessment
- Risk Assessment

netPine

Test vulnérabilité

- o Serveur d'attaque
 - www.nessus.org
- o Spider web
 - www.whitehatsec.com



netPine

Encryption

- o SSL
 - web
 - email
 - tunnel vpn



netPine

Questions ?

netline