

Penetration Test Outpost Desktop Firewall.

Auf einem WindowsXP System mit normaler Konfiguration und der Desktop Firewall OutPost von Agnitum, haben wir einen kleinen Test durchgeführt um die Firewall auf die Stabilität zu prüfen.

Gegen zufällig erstellte Datenpakete (kurze oder kleine IGMP oder ICMP Pakete) kann man sagen, daß die Outpost Firewall recht stabil ist und diese "Angriffe" erkennt jedoch im gesamten Arbeitsverhalten schwer abbremst.

Die Outpost arbeitet nicht mehr in gewohnter Schnelligkeit und kann die Datenpakete nicht eindeutig verarbeiten.

Diese Datenpakete wurden per Zufallsgenerator eindeutig definiert und können dazu führen, daß bei einem sehr lang andauernden "Angriff" dieser Art, die Firewall die Arbeit aufgibt.

Im Einzelfall bedeutet es, daß man von einer Angriffszeit von mehr als 10 Minuten ausgehen, innerhalb eines Netzwerkes (LAN) dürfte diese Zeit bei ca. 2-3 Minuten liegen.

Anschliessend wurden eine Menge von ACK Paketen auf eine IP geschickt, die von der Outpost Firewall geschützt werden sollte. Diese Datenpakete (ACK) sind in der Regel reine Bestätigungspakete innerhalb existierender Verbindungen. (ACK bedeutet einfach: das hier Datenpakettransfer über ACK lediglich quittiert werden)

Bei einem sogenannten Stream-Angriff werden Datenpakete generiert, die eigentlich nicht zu einer bestehenden Verbindung gehören. Da die Outpost Firewall überprüft, welche Pakete zur bestehenden Verbindung gehören um Portscans zu entdecken, wurde die Outpost allein durch diese Überprüfung während der Attacke so stark überlastet, sodaß vorübergehend das System zum Stillstand kam.

Folge daraus: Das Betriebssystem hat über die Zeit des Angriffes totalen Stillstand, da die Outpost Firewall fast die gesamten Ressourcen für die Berechnung benötigt.

Wird der Angriff jedoch aber abgebrochen, kann es in einzelnen Fällen auftreten, daß die Outpost Firewall anschliessend nicht mehr sauber arbeitet und neu gestartet werden muß. Das System ist dann ungeschützt und ist aber in dieser Form stabil gegen die Angriffe geblieben und arbeitete weiter.

Ein Bluescreen konnte jedoch nicht erzeugt werden, lediglich hat die Firewall Outpost die Arbeit verweigert.

Was das interne IDS (Intrusion Detection System) anbelangt kann man sagen, daß es nicht 100% zuverlässig reagierte auf ankommende Angriffe wie oben beschrieben.

Das IDS hatte zunehmend Probleme die tatsächliche Subnetmaske zu blockieren oder gar die Verbindung zum Internet oder zum LAN zu blockieren.

Daher ist das IDS bei massivem Angriff fast nutzlos, da es kaum reagieren kann.

Die Outpost Firewall ist aber dennoch eine saubere Firewall für den Windows Nutzer, der ein wenig mehr sehen möchte was tatsächlich im Netzwerk geschieht.

Die Chance, dass eine solcher Attacken tatsächlich ausgeführt wird ist sehr gering. Das Verständnis dieser Angriffstechniken ist schon sehr fachspezifisch und kann nicht auf die schnelle ausgeführt werden.

Durch den Test kann man abschliessend sagen, die Firewall Outpost macht einen recht interessanten und durchaus stabilen Eindruck.

Der Test wurde mit einem WindowsXP System durchgeführt und das angreifende System war ein RedHat Linux System.

Was nicht vergessen werden darf, das für Attacken auf eine Firewall wie die Outpost eine IP Adresse konkret erforderlich ist.

Schwer ist es aber eine IP Adresse zu erhalten, wenn man nicht auffällig ist durch unachtsames Surfverhalten.

Die Chance einer zufälligen IP Folge ist sehr gering, da nicht eindeutig erkennbar ist was für

ein Firewallsystem dort wirklich auf das System achtet.

Vielleicht sollte erwähnt werden, dass die Updates von Outpost auf jeden Fall einmal wöchentlich geprüft werden sollten, um sicher zu gehen immer die neueste Version zu haben. Das Team von Agnitum arbeitet recht fieberhaft an Verbesserungen und an Neuerungen, um Fehler und Schwächen zu beseitigen.

Nach dem Test der durch Mixer und mich durchgeführt wurde, haben wir umgehend das Team von Agintum informiert und über die augetretenen Schwächen informiert.

Testversion aktuell: 1.0.1817.1645

Marko Rogge - Brain-Pro Security in Kooperation mit Mixersecurity ; 30.12.2001

In diesem Sinne ein Danke an Mixer.

Deutsche Anleitung zur Outpost Firewall

Dieser Test sowie Auszüge daraus dürfen nicht ohne Genehmigung vervielfältigt werden!

©2001-2002 by M.Rogge & Mixer

Original E-Mail an Agnitum, verfasst von Mixer:

Greetings,

attached is a translation of the German-Secure article about the Outpost Firewall test.

~Mixer

Agnitum's Outpost Desktop Firewall

A brief penetration test of the Outpost Desktop Firewall.

We did a small test on a Windows XP system with standard configuration and the Desktop Firewall OutPost from Agnitum to test its stability. The Outpost Firewall is pretty stable when it comes to attacks based on randomly created data packets (short packets and small IGMP- and ICMP messages among others), as it recognizes such "attacks", though it can be slowed down significantly by them. The Outpost ceases to work in the usual speed and the system fails to process some of the packets. The mentioned kind of packets are created by a random generator. They contain specifically crafted parts of known DoS attacks, and can lead to a termination of the firewall after a long period of attack. In some cases this means you have to estimate an attack period of over ten minutes, for an attack from within a network (LAN) this time is around two to three minutes.

As the next test we sent a large amount of ACK packets to an IP that was protected by the Outpost firewall. ACK packets are usually only an acknowledgement within existing TCP connections (ACK is a notification that another part of the tcp session data has been received). During this so-called "stream"-attack, single ACK packets are sent that do not belong to established connections. Since the Outpost firewall will check which packets belong to an established connection, in order to detect portscans, only through this attack the Outpost has been overloaded so much that the system came to a temporary halt, since the Outpost firewall consumes practically all resources for the CPU-intensive ACK packet computations.

As the attack is stopped, in some cases the Outpost Firewall ceases to work reliably and has

to be restarted. In that situation, the system is unprotected, however stable despite further ACK floods and continued to work. A bluescreen could not be produced, only the Outpost Firewall could be forced to cease its service.

Regarding the internal IDS (Intrusion Detection System), it is not 100% reliable when it comes to detecting attacks as above. The IDS had increasingly problems to block the actual subnet mask of the source addresses of incoming packets and enforce filtering of such packets going to LAN or back to the Internet. Therefore, the IDS is almost useless during a massively spoofed attack, since it can barely react.

Nevertheless, the Outpost is a cleanly running firewall for the Windows user who wants to explore the network traffic in realtime. The chance of attacks as described above being executed is quite rare. The understanding of such penetration methods is quite specific and is usually not done quickly. The test was performed against a Windows XP system and a RedHat Linux system acted as the attacking party. All in all, the test shows that the Outpost Firewall is an interesting product which seems to be stable in most situations. One should not forget that targeted attacks against a firewall such as the Outpost do usually require insider knowledge about the IP address. The chance of a random hit is quite rare, since one cannot recognize directly what firewall is running on and watching over any given remote system.

What should also be mentioned is that the official updates for Outpost should be checked for at least once per week, to make certain to always have the most recent version. The team of Agnitum worked quite intensively on new features and improvements to remove bugs and weaknesses.

A german-language manual is now available here at Brain-Pro Security as well.

[German manual for the Outpost Firewall](#)

Brain-Pro Security
in cooperation with
Mixer security