

Blinken Bluetooth

Autor: Bastian Ballmann (balle@chaostal.de)

Blinken Bluetooth ist eine Sammlung an Tools, um Blinkenmovies ueber Bluetooth Devices abzuspielen. Die Software reagiert auf den Bluetooth Device Namen und Type und spielt dementsprechend vorkonfigurierte Videos ab. Desweiteren loesen Bluetooth Events wie l2ping oder iscan Animationen aus. Es gibt noch einen zu 99% fertigen OBEX Server mit dem man Nachrichten per Vcard einsenden kann (es fehlt nur die Ermittlung des Dateinamen der eingesendeten Datei).

Get the source [<http://www.chaostal.de/members/balle/bluetooth/blueblink.tgz>]

Bluediving - Bluetooth pentesting suite

Autor: Bastian Ballmann (balle@chaostal.de)

Bluediving ist eine Bluetooth Pentesting Suite und implementiert u.a. Attacken wie Bluebug, BlueSnarf, BlueSnarf++, BlueSmack sowie Features wie Bluetooth Address Spoofing.

Sourceforge Project Page [<http://sf.net/projects/bluediving/>]

Bluechase - The Reallife Bluetooth Adventure Game

Autor: Bastian Ballmann (balle@chaostal.de)

Das Chaostal hat die Arbyte an dem Reallife Bluetooth Adventure Game im Stil von Mister X aufgenommen, welches auf dem 21C3 organisiert werden soll.

Chaostal Mitglieder finden mehr Informationen über dieses Projekt im Chaostal Wiki [<http://www.chaostal.de/wiki/>] .

Mehr wird zur Zeit noch nicht verraten! ;)

Bluetooth Spielereien

Autor: Bastian Ballmann (balle@chaostal.de)

Marcel und ich spielen schon seid längerer Zeit mit Bluetooth rum. In dieser Zeit

sind nen paar Skripte und ein kleiner Vortrag entstanden. Die Klamotten stelle ich hiermit mal online.

Blue-CMD [/members/balle/bluetooth/blue-cmd.txt] - Führe ein beliebiges Kommando aus, wenn sich ein Bluetooth Device im bzw. ausserhalb des Empfangsbereichs befindet. Ideal zum automatischen (ent)locken des Laptop, wenn man sich mit seinem Bluetooth Handy durch die Kneipe bewegt ;)

Blue-CMD Hotplug [/members/balle/bluetooth/blue-cmd-hotplug.tgz] - Blue-CMD als Hotplug Script. Programmiert von Suran vom CCC Freiburg [<https://www.ccc-fr.de>] .

Blue-Scanner [/members/balle/bluetooth/blue-scanner.txt] - Ein kleines Script, das ich auf dem 20C3 geschrieben habe. Es scannt nach Bluetooth Devices, liest die vorhandenen Profile via SDP aus und versucht mit OBEX Push eine Vcard hoch zu laden.

Vcard [/members/balle/bluetooth/all_your_base_are_belong_to_us.vcf] - Ein Beispiel für eine Vcard.

Blue-Trace [/members/balle/bluetooth/blue-trace.txt] - Loggt alle vorbei fliegenden Bluetooth Devices mit Timestamp in eine Logdatei und checkt, ob sie schon bekannt sind und wann sie schon mal vorbei gekommen sind.

Bluetooth for fun and profit [/cgi-bin/parser.cgi?input=article/bluetooth] - Ein Artikel der sowohl den Bluetooth Protokoll Stack und die Einrichtung von Bluetooth unter Linux 2.4 / 2.6 als auch typische Anwendungen wie Datenaustausch, Aufbau eines Netzwerks, Scannen nach Devices und Diensten und die Programmierung einfacher Anwendungen unter Verwendung der BlueZ Libraries beschreibt.

Bluetooth Vortrag [/members/balle/bluetooth/Bluetooth.sxi] - Ein kleiner Vortrag, den Marcel und ich mal Chaostal intern über Bluetooth gehalten haben. Von der Theorie (Protokollstack usw.) zur Praxis (Einrichten, Nutzen, Programmieren).

Der RaumChaos. - Donnerstag is do imma Clubtuch!

Autor: Marcel Wegermann (Marcel@chaostal.de)

Dank "Miner" bekam das Chaostal im Dezember die Moeglichkeit geboten, einen Clubraum kostenlos anzumieten. Einzige Bedingung - Wir sollten uns mal um die hauseigene Telefonanlage kuemmern. Das hoerte sich ja gut an, eine Telefonanlage zu betreiben, das gehoert doch praktisch zu unseren Kernkompetenzen *hust*. Nach einer kurzen Abstimmung war es also beschlossen.

- Wir bekommen einen Clubraum..! -

Nebenbei sollte gesagt werden, das sich der Clubraum bis dato nicht gerade in einem Zustand der Vollkommenheit befand - mehr so wie nach einem Bombenangriff.

Chaostaler:...aaAAA (Aber was macht das schon, viele helfende Haende, werden das schon schaffen!)

Kaum war dieser Satz ausgesprochen befand sich derjenige, der dies gesagt

hatte, allein im Raum. - Nur ER und ein vorbeifliegender Strohhallen *g* Okay, ganz so schlimm ist es nicht, es arbeiten regelmaessig in der Woche etwa 6-8 Leute an dem Raum und es geht langsam aber stetig vorwaerts. Den Aktuellen Stand, bekommt ihr hier. - Aktueller Stand vom RaumChaos [/cgi-bin/parser.cgi?input=news/raum]

P.A.T.H. - Perl Advanced TCP Hijacking

Autor: Bastian Ballmann (balle@chaostal.de)

P.A.T.H. ist eine Sammlung von Netzwerk Hijacking Tools geschrieben in Perl. Die aktuelle Version ist 0.8. Das Projekt besteht zur Zeit aus einem Paketgenerator (ARP|TCP|UDP|ICMP / IP) , einem flexibel konfigurierbaren RST daemon, einem Netzwerksniffer (der auch einen speziellen Mail- und Telnet-Sniffin-Modus implementiert hat), einem ICMP Redirection Tool (zum umlenken von Netzwerkverbindungen ohne ARP Poison Attacks), einem ARP Redirection Tool (zur Implementierung von ARP Man-in-the-middle Attacken), einem NIDS Testing Tool, sowie einem automatischem Hijacking Daemon für Plain Protokolle.

Jedes Tool beinhaltet eine GUI- und eine Terminal-Version.

Das Tool wurde getestet unter Linux (Debian Woody, SuSe 7.3, 8.0, Redhat 7.3, 8.0) und FreeBSD 5.0, 5.1

P.A.T.H. Homepage [<http://p-a-t-h.sourceforge.net>]

Windows Paketgenerator Bibliothek

Autor: Martin Zoellner (MiNeR@chaostal.de)

Kleine Windows Paketgenerator-Bibliothek in C/C++. Mögliche Protokolle sind Ethernet, ARP, TCP/IP, UDP/IP, ICMP(-Redirect) und DNS. Desweiteren ist als Beispielprogramm ein Paketgenerator dabei, der die gesamte Bibliothek nutzt. Dieser bietet zudem noch eine Snifffunktion und einen kleinen Reset-Daemon. Als zweites Beispielprogramm ist ein TCP/IP Connection-Spoofing dabei. Dieser baut im Ethernet über ARP-Poisoning eine gefakte Verbindung zu einem Host auf und sendet den Inhalt einer übergebenen Datei.

Die Programme und Beispiele setzen auf der wpcap Bibliothek auf. Diese besitzt zwar eine Sniff- und Sendemethode, aber ohne Funktionen um die Header zu generieren oder auszulesen. (deswegen die Paketgeneration Bibliothek) Programme und Bibliothek wurden mit Borland C++ Builder erstellt. Die Projektdateien sind somit nicht kompatibel zu MSVC++.

Wurde getestet unter Windows 98/2k/XP.

windows packet generation library.zip [

<http://ccc.wtaler.de/members/miner/windows%20packet%20generation%20library.zip>

