Netzwerkumstrukturierung

Konzepte fuer AAA im Entropia e.V.

Authorisation, Authentication und Accounting

Erarbeitung eines Sicherheitskonzeptes

hannes_ - Junior Consultant

Zielsetzung

- Ein von ueberall aus geschuetztes Netzwerk
- Ueberwachbar
- Kontrollierbar

Ich will mit einem guten Gefuehl das Netzwerk des Entropia e.V.s benutzen koennen!

Zu schuetzende Daten

- Warez
- Pr0n
- Moviez
- Mp3z
- Gam3z
- ...

Vorbild sein!

- Wenn der Entropia seine Dienste nicht schuetzt, wer soll es denn sonst tun???

- Warez Traffic zentralisieren!
  - Hier ist euer Warez sicher!
- Verantwortung delegieren!

Angriffsvektoren

- Freier Zugang ueber WLAN
- Unkontrollierbares Kabelnetzwerk
- Keine zentrale Stelle zum Accounting und Logging
- ungesicherte UNIX-Services
- ...

Ungesichertes 802.11a/b/g

- Mitsniffen von Daten in der Luft
- Unauthorisierter Zugang
- Sogar: MIT-Attacken sind moeglich!
  - LORKON
  - airpwn

Analyse

- Wieso haben wir noch keine entsetzten Mitglieder???
- Feingefuehl beim Umgang mit Warez vermitteln

Konzept: LAN

- IP ueber Ethernet soweit wie moeglich vermeiden
- Verbindung ueber PPPoE-Concentrator
- PPP mit eap/pap
  - Authentifizierung des Concentrators
  - Authentifizierung des Clients

Vorteile/Probleme

- PPPoE spricht jedes Betriebssystem
- ggf. Probleme mit EAP-Auth
  - noch zu testen

Konzept: WLAN

- Aehnlich wie LAN
- Ggf. noch WPA2 ueber Radius
  - Probleme: Koennen alle Clients pppoe ueber ein Wlan-Interface fahren?
  - Wpa nicht bei allen Laptops moeglich

IPSEC

- Zusaetzliches roadwarrior-setup
  - x.509
  - xauth
  - gssapi
  - radius

CIPSO

- wenn Netzwerk vom AC-Layer trusted
- Labeling der Pakete und Flow/Accounting Moeglichkeiten
- Applikations/Firewall-Ersatz

Fragen? Anregungen?

Netzwerkumstrukturierung

Konzepte fuer AAA im Entropia e.V.
Authorisation, Authentication und Accounting

Erarbeitung eines Sicherheitskonzeptes

hannes_ - Junior Consultant

Zielsetzung

- Ein von ueberall aus geschuetztes Netzwerk
- Ueberwachbar
- Kontrollierbar

Ich will mit einem guten Gefuehl das Netzwerk des Entropia e.V.s benutzen koennen!

Zu schuetzende Daten

- Warez
- Pr0n
- Moviez
- Mp3z
- Gam3z
- ...

Vorbild sein!

- Wenn der Entropia seine Dienste nicht schuetzt, wer soll es denn sonst tun???

- Warez Traffic zentralisieren!
  - Hier ist euer Warez sicher!
- Verantwortung delegieren!

Angriffsvektoren

- Freier Zugang ueber WLAN
- Unkontrollierbares Kabelnetzwerk
- Keine zentrale Stelle zum Accounting und Logging
- ungesicherte UNIX-Services
- ...

Ungesichertes 802.11a/b/g

- Mitsniffen von Daten in der Luft
- Unauthorisierter Zugang
- Sogar: MIT-Attacken sind moeglich!
  - LORKON
  - airpwn

Analyse

- Wieso haben wir noch keine entsetzten Mitglieder???
- Feingefuehl beim Umgang mit Warez vermitteln

Konzept: LAN

- IP ueber Ethernet soweit wie moeglich vermeiden
- Verbindung ueber PPPoE-Concentrator
- PPP mit eap/pap
  - Authentifizierung des Concentrators
  - Authentifizierung des Clients

Vorteile/Probleme

- PPPoE spricht jedes Betriebssystem
- ggf. Probleme mit EAP-Auth
  - noch zu testen

Konzept: WLAN

- Aehnlich wie LAN
- Ggf. noch WPA2 ueber Radius
  - Probleme: Koennen alle Clients pppoe ueber ein Wlan-Interface fahren?
  - Wpa nicht bei allen Laptops moeglich

IPSEC

- Zusaetzliches roadwarrior-setup
  - x.509
  - xauth
  - gssapi
  - radius

CIPSO

- wenn Netzwerk vom AC-Layer trusted
- Labeling der Pakete und Flow/Accounting Moeglichkeiten
- Applikations/Firewall-Ersatz

Fragen? Anregungen?

- Click to add an outline