

Management Summary

19.03.2010

Dok-Nr: B_06

HTL Rennweg, 1030 Wien,
Rennweg 89 b

Version: 1.0

Klasse: 5AX

| Projektteam: | Name | Funktion |
|--------------|-----------------|--------------------|
| | Lukas Müller | Projektleiter |
| | Mino Sharkhawy | Projektleiter-Stv. |
| | Michael Hein | Projektmitarbeiter |
| | Simon Wartanian | Projektmitarbeiter |

| Version | Datum | Autor | Änderungen |
|---------|------------|--------------|------------------------------|
| 0.1 | 16.11.2008 | Lukas Müller | Erstellen der Vorlage |
| 1.0 | 19.03.2010 | Lukas Müller | Management Summary erstellen |

Projektstatus



Wir haben einen weiteren Rechner vom Herrn Prof. Buric erhalten, um diesen hinter der ASA als zusätzliche Firewall zu verwenden. Dafür haben wir eine modifizierte Linux-Distribution (IPCop) installiert, die ideal dafür geeignet ist Firewall-Aufgaben zu übernehmen. Zusätzlich haben wir benötigte Tools wie SSL-Strip, SSHArp, Hydra, usw. auf dem Rechner installiert. Für zusätzliche Sicherheit sorgt ein Snort IDS, welches wir implementiert haben.

Damit das Klassennetz der 5AX über den Cisco Access Point ins Internet kommt, haben wir einen neuen, eigenen IP-Range konfiguriert und mittels Policy Based Routing über unsere ASA umgeleitet. Auf der ASA wurde zudem ein IPS mittels des ASDMs implementiert, um die Sicherheit zu erhöhen.

Damit sämtliche Schüler der 5AX Authentifiziert ins WLAN kommen, wurde die X-Authentifizierung auf dem Radius Server mit dem Active Directory gekoppelt.

Am Diplomarbuchs wurde weiter geschrieben und sollte demnächst fertig sein.

Erledigte Arbeiten

| Bearbeiter | PSP | Tätigkeit | Ort | Dauer | Status |
|--------------|-------|--|--------|---------|--------|
| Michael Hein | 1.8.3 | <ul style="list-style-type: none"> Neuer, eigener IP-Range für die Klasse 5AX wurde konfiguriert. Diverse Tools wurden auf dem Rechner installiert wie SSL-Strip, SSHArp, Hydra, usw. IPS wurde mittels ASDM auf der ASA implementiert Weiter an dem Diplomarbuchs geschrieben | Schule | 14 Tage | |
| Lukas Müller | 1.8.4 | <ul style="list-style-type: none"> Ein GRE Tunnel vom Prelude Server (über die ASA) zum Router wurde konfiguriert. Weiteren Rechner von BUR erhalten, um diesen hinter der ASA als zusätzliche Firewall zu verwenden. IPS wurde mittels ASDM auf der ASA implementiert Weiter an dem Diplomarbuchs | Schule | 14 Tage | |

| | | | | | |
|-----------------|-------|---|--------|---------|--|
| | | geschrieben | | | |
| Mino Sharkhawy | 1.8.3 | <ul style="list-style-type: none"> • Policy Based Routing wurde konfiguriert, um den Traffic zu unserer ASA umzuleiten. • Es wurde der Rechner aufgesetzt mittels IPCop (Linux-Firewall-Distribution). • SNORT-IDS wurde konfiguriert und implementiert • Weiter an dem Diplomarbeitsbuch geschrieben | Schule | 14 Tage | |
| Simon Wartanian | 1.8.4 | <ul style="list-style-type: none"> • X-Authentifizierung wurde auf dem Radius-Server mit Active Directory implementiert • Weiter an dem Diplomarbeitsbuch geschrieben | Schule | 14 Tage | |

Ziele

- Technische Dokumentation
- Konfigurationen
- Log - Files
- Weitere Papers

Arbeiten der nächsten Wochen

| Bearbeiter | PSP | Tätigkeit | Dauer |
|-----------------|-------|---|---------|
| Michael Hein | 1.8.5 | <ul style="list-style-type: none"> • IPS funktionsanforderungsgerecht konfigurieren • Automatisierte E-Mail Signierung auf dem Prelude-Server implementieren • Diplomarbeitsbuch fertig stellen | 14 Tage |
| Lukas Müller | 1.8.5 | <ul style="list-style-type: none"> • IPS funktionsanforderungsgerecht konfigurieren • Automatisierte E-Mail Signierung auf dem Prelude-Server implementieren • Website von Herrn Wieninger auf Schwachstellen testen • Hydra modifizieren um Online-Formulare automatisiert ausfüllen zu können (BOT) • Diplomarbeitsbuch fertig stellen | 14 Tage |
| Mino Sharkhawy | 1.8.6 | <ul style="list-style-type: none"> • Snort IDS weiter konfigurieren • Mirror Port einrichten, um Snort IDS sinnvoll einsetzen zu können • Signaturen für IDS beschaffen • Diplomarbeitsbuch fertig stellen | 14 Tage |
| Simon Wartanian | 1.8.3 | <ul style="list-style-type: none"> • X-Authentifizierung mit dem implementierten Active Directory testen • Diplomarbeitsbuch fertig stellen | 14 Tage |

Ergebnisse

- Kommentierte Konfigurationen
- Essentielle Show – Befehle
- Weitere Logfiles
- Dokumentation der Sicherheitsmaßnahmen