kerby@parsifal

Thomas Calderon Olivier Levillain

ANSSI

5 juin 2014

Parsifal : plaquette publicitaire (juin 2013)

- Écriture de *parsers* grâce à du code **concis**
- **Efficacité** des programmes produits
- **Robustesse** des outils développés
- Méthodologie de développement adaptée à l'écriture **incrémentale** de *parsers* flexibles

- Parsifal permet aussi de construire les objets décrits
- Exemple : client DNS en 200 lignes

- Objectifs de Parsifal
  - outils d'analyse maîtrisés
  - brique de base pour des outils de dépollution

* mais ne protège pas des XSS

Formats décrits avec Parsifal

- SSL/TLS
  - analyse de données (ACSAC 2012)
- X.509 et requêtes de certifications
  - outils de vérification
- DNS
  - micro client
- PCAP/IP/TCP/UDP
- MRT/BGP
- NTP
- PE/UEFI firmware
- OpenPGP
- DVI
- PNG

- Kerberos

Analyse d'un message Kerberos capturé

parsifal --pcap-tcp 88 -T kerberos_tcp trace.pcap

Analyse d'un message Kerberos capturé

parsifal --pcap-tcp 88 -T kerberos_tcp trace.pcap

```
msg_type: TGS_REQ (0x0c)
...
ticket {
  realm: "DEMO.LOCAL"
  sname: "krbtgt", "DEMO.LOCAL"
  enc_tkt_part {
    encryption_type: AES256_CTS_HMAC_SHA1_96 (0x12)
    [Unparsed]_cipher: f3e1becbf885... (905 bytes)
  }
  ...
} req_body {
  realm: "DEMO.LOCAL"
  sname: "cifs", "dc-2012-01.demo.local"
  ...
```

Décapsulation du ticket

```
parsifal  --pcap-tcp 88 -T kerberos_tcp
          --kerberos-aes-key ks-aes.key
          trace.pcap
```

Décapsulation du ticket

```
parsifal  --pcap-tcp 88 -T kerberos_tcp
          --kerberos-aes-key ks-aes.key
          trace.pcap
ticket {
  realm: "DEMO.LOCAL"
  name_string: "krbtgt", "DEMO.LOCAL"
  enc_tkt_part {
    encryption_type: AES256_CTS_HMAC_SHA1_96 (0x12)
    kvno: 2
    cipher {
      crealm: "DEMO.LOCAL" (10 bytes)
      cname: "Client"
      ...
      authorization_data { ... }
  }
}
```

Inspection du contenu de la PAC

```
authorization_data {
    ...
    effective_name_real: "Client"
    full_name_real: "Client"
    group_ids {
        513 (0x00000201)
        512 (0x00000200)
        516 (0x00000204)
        518 (0x00000206)
        519 (0x00000207)
        123456 (0x0001e240)
    }
    ...
    extra_sids {
        "S-1-5-18"
        "S-1-1234-1337"
        "S-1-12345678-1111111-2222222-3333333"
    }
...
}
```

Conclusion

- Parsifal permet d'analyser les messages de manière autonome
- Objectif : détecter des anomalies
- Très peu d'outils existants
- Travail futur
  - nettoyer l'interprétation de la PAC
  - outil d'extraction des messages `AP_REQ`
  - outil d'extraction des PAC
- Code bientôt dispo sur Github

Questions ?

Merci de votre attention.

https://github.com/ANSSI-FR/parsifal