Dokumentation der Meetings

Intern 06.11.2016

- Dokument "Angriffe" mit Inhalten aus dem Paper updaten
- Angriffe besprechen und aufteilen
- Test Konzept entwerfen
- Kapitel für Studienarbeit vorschreiben (Rohtext)
- ? Ergebnisse verlinkter Seiten anzeigen
- ? Verlinkte Seiten ohne Ergebnisse zur Prüfung vorschlagen
- ? SauceLabs als Frontend testing suite
- clamav als CLI File-Virusscanner (https://www.virustotal.com/)
- SAD erstellt
- Metasploit für Anwendungs-Tests

Extern 07.11.2016

- Erwartungen bis Weihnachten (Anwendung, Dokumentation)
- Angriffe besprechen
- Weitere Ideen von ihm
- Vorstellung Konzept (SAD)
- Metasploit, Virenscanner (clamav, virustotal)

Intern 09.11.2016

- Schnittstelle definieren

Intern 17.11.2016

- Multi-Header-Check (Browser-Integrity-Check) nur als Warnung
- Virusscan fertig, noch kein Code-Review
- Virusscan wird über offiziell anerkannte *infizierte* Datei geprüft
- Tester haben einen optionalen Parameter **-i** für die Mitgabe einer ID
- URL-resolving über java.net.HttpURLConnection: werden hier maliziöse Daten heruntergeladen?
- Server kaufen
- Gliederung der Studienarbeit verfeinert

Intern 24.11.2016

- Daniel
    - header inspection test fertig implementiert, ohne Docker
    - E-Mail Martin
        - Link zum Server (webifier.de)
        - Link zur Gliederung
    - E-Mail Herr Freudenmann wegen Förderung
- Samuel:
    - Server setup
    - Recherche Resolving URL / Reachable check
- Jan-Eric
    - Test fertig
- Datenbankmodell planen

Intern 01.12.2016

- Daniel
    - Team Kapitel Rohaufschrieb
    - URL-Parameter akzeptieren
    - ID-Parameter akzeptieren
    - Output-Format definieren (Tester)
    - Java-Klasse in webifier-tester erstellen (Beispiel)
- Samuel
    - Einleitung
    - URL Resolving “PreTest”
- Jan-Eric
    - Test fertig
- Fördergelder

Intern 08.12.2016

- Daniel
    - Team Kapitel Rohaufschrieb
    - Java-Klasse in webifier-tester erstellen (Beispiel)
    - 3€ für Domains an Samuel
- Samuel
    - Einleitung schreiben
- Jan-Eric
    - 3€ für Domains an Samuel
- Stand Studienarbeit

Intern 15.12.2016

- Daniel
    - schreiben
    - Result-Klasse in webifier-tester schreiben (nicht ergänzend zur Info-Klasse)
    - 3€ für Domains an Samuel
- Samuel
    - schreiben
- Jan-Eric
    - schreiben
    - Test in webifier-tester integrieren
    - 3€ für Domains an Samuel

Extern 19.12.2016

- HtmlUnit als reiner Java-Browser, mit dem sich Standardverhalten (z.B. über Links navigieren) einstellen lässt
- #neuer Test: IP-Scan Test
- neuer Test: auftretende Links testen
    - Externe Blacklist
    - Interne Datenbank
- #neuer Test: JS-Analyse
    - Ice Shield (Paper) zur statischen JS-Code-Analyse
- Idee: Phishing, schwer umsetzbar, ggf. wenn Zeit ist Testkonzept erstellen
- Idee: Live-Übertragung der Tests (Screencast) oder einfacher Screenshot der Seite
- Idee: Crawler, "Google für maliziöse Seiten"
- Idee: Browser Plugin
- Priorisierung: Sheet

Intern 22.12.2016

- Daniel
    - http://www.reliply.org/tools/requestheaders.php
- Samuel
- Jan-Eric
- gemeinsam
    - Definition Test Ergebnis (Gewichtung)
    - malicious-Boolean durch Enum ersetzen
- 2017
    - Daniel

    - Samuel
        - Performance für Test optimieren, parallelisieren, mutlithreading bzw. -processing
    - Jan-Eric
    - Treffen im nächsten Jahr für Retro und Planung der Weiterarbeit während der Praxisarbeit
    - welche Aufgaben, nur Kleinigkeiten? Schreiben?

Intern 04.01.2017

6. Semester:

- Code-Review am Anfang
- Rechnung von netcup an Hüneborg → Genehmigung → Fördermittel über Braun an Samuel
- Analyse
    - Datenbankmodell für Platform
    - Blacklist durchlaufen lassen

Projektmeeting mit Martin 06.03.2017 12:15 in der Kantine

- Vorstellung der aktuellen webanwendung
- bisher
    - viele tests hinzugefügt
    - batch-verarbeitung (100.000 Einträge reduziert -> sonst zu viel Last)
    - datenbank nimmt erste daten an
    - einzelne neue tests besprochen
- nächste Schritte
    - analyse der daten
    - auswertung visualisieren
- Vorschläge von Martin
    - google-service/open-dns `isMalicious("URL")` einbinden, auch Phishing-Dienste
    - optional: e-mail analyse: alle urls der email checken und ergebnis zurückliefern (ggf. auch Screenshot)
- nächster Termin: in 4 Wochen
    - alle Features implementiert
- Aufaben
    - E-Mail an Heinrich Braun bzgl. Server
    - ice-shield fertigstellen (bei Fragen gerne über Martin)

Projektmeeting mit Martin 03.04.2017 12:00 Uhr in der Kantine (alle sind da)

Vorstellung der ergebnisse:
- analyse läuft seit letzten Dienstag
- Statistiken:
  - pro Test
    - Gesamt
- E-Mail
  - läuft noch nicht so rund (Keine Rückmeldung über Ergebnisse)

Gliederung Studienarbeit:
- Aufteilung ist schon ziemlich fix
- Fazit wird wahrscheinlich zusammen geschrieben
- Ausblick nicht zum Schluss, besser vorher, für positives Ende
- Nicht mehrere Lösungsansätze (Architekturen) beschreiben
- eher weniger bei Standardtechnologien (nicht mehr als notwendig)
- wichtiger: Angriffstypen beschreiben
- Optische Entscheidungen (Visualisierung),
- Analyse braucht mehr Struktur! noch keine Unterpunkte

  - Vorschläge: chron-job um schlechte seiten regelmäßig zu überprüfen (haben sie sich verändert)

- Martin wird nicht die gesamte Arbeit Probelesen können
- Draft schreiben
- unsichere Kapitel zur Prüfung bei Martin einreichen

Folgetermin: 24.04.2017 12:00 Uhr

Internes Meeting 24.04.2017 12:00 Uhr in der Kantine

Martin ist nicht da, ohne Abmeldung

- todo
  - testspezifische auswertungen
  - ergebnisse nach domain [prozentual]
  - Daniel
    - erkenntnisse
  - Anzahl der Tests pro Tag hängt stark von Webseitengröße ab
- Inhalte

    - Analyse: woher kommen die Listen
    - Screenshots
    - GitHub und Slack im Team-Kapitel
- Rechnerinfrastruktur erläutern
- Überleitung Diagramme
    - Daten in MongoDB
- Fragen
    - Wie steht Martin zu Wikipedia als Quelle?
    - Hat Martin Literaturvoschläge
        - Phishing
- **Deadline: 05.05.2017**

Meeting 03.05.2017 11:00 Uhr

- Ausblick: Länderkarte → IP Geodaten Auswertung
- Übergabe der Test- und Auswertungsdaten, am besten in Drive hochladen
- Wikipedia nur ungern als Quelle, vlt. bei Historien, nicht bei technischen Daten
    - lieber dort verwendete Primärquellen
- Literatur über Phishing → wurde per Mail verschickt
- Analyse
    - nicht nur Datenquellen und Ergebnisse, sondern auch Diskussion also was können wir aus den Ergebnissen lernen, Zusammennhänge
    - Zusammenhänge zwischen den Tests
    - Schwellwerte
- Umsetzung
    - Statistics: wieso wurden die Ergebnisse so umgesetzt
    - Generell können wir viel über Implementierung schreiben
- Für Definitionen lieber Bücher oder noch besser wissenschaftliche Paper