Die Hacker kommen!

Modus: Einzelarbeit

Typ: Miniproject

Beschreibung

In diesem Guided Research Projekt setzen Sie sich mit dem Thema Physical Penetration Testing auseinander. Der bekannte Pen-Tester Jayson E. Street erzählt in seinen Vorträgen von erlebten und getesteten Sicherheitslücken und wie er diese ausnutzen kann. Sie sehen sich einige dieser Präsentationen an und dokumentieren bzw. kategorisieren die Sicherheitslücken, die ausgenutzt werden. Mit diesem Wissen über kompromittierte Ziele überlegen Sie, wie sich eine offene Organisation wie die TU Wien gegen Angriffe dieser Art schützen kann. Sie schreiben fiktive Guidelines für Mitarbeiter_innen unterschiedlicher Beschäftigungsgruppen, und erklären Ihre Auswahl.

Ablauf

Führen Sie während des gesamten Prozesses ein Forschungstagebuch (siehe Beschreibung im Anhang). Dokumentieren Sie darin die Aktivitäten, Ergebnisse, Hindernisse und Erfolge sämtlicher Schritte Ihrer Arbeit.

1. Sehen Sie sich die hier verlinkten Videos an. Dokumentieren Sie in einer Struktur die Sie für übersichtlich erachten die unterschiedlichen erklärten Vulnerabilitäten und erarbeiten Sie eine Kategorisierung für all diese Angriffsvektoren.

- Jason E Street, DEFCON 19 talk – https://vimeo.com/28284322
- Tactics of Physical Pen Testers – https://www.youtube.com/watch?v=VJ4FDOw9NcI
- Path of Least Resistance: Red Team Stories – https://www.youtube.com/watch?v=jcVIruSqI6w
- The ULTIMATE Physical Penetration Test – https://www.youtube.com/watch?v=JketdMhzMz0
- Using Food to Bypass Security: Red Team Stories – https://www.youtube.com/watch?v=zgcP_mj9dJE
- I Broke Into The International Security Convention – https://www.youtube.com/watch?v=qM3imMiERdU

2. Finden Sie ein weiteres Video, das ähnlich wie die oben verlinkten Videos das ungefragte Betreten eines beschränkten Bereichs dokumentiert und erklärt, wie das gemacht wurde. Wenden Sie die Kategorisierung, die Sie erarbeitet haben, auf dieses Video an. Dokumentieren Sie Ihre Suche und Ihre Kategorisierung, und fassen Sie das Video kurz zusammen.

3. Denken Sie darüber nach, welche spezielle Art von Sicherheitsproblemen eine offene Organisation wie die TU Wien haben könnte. Denken Sie dabei an mehrere Personengruppen: Studierende, Mitarbeiter_innen, Adminstration, Sicherheitskräfte, nichtwissenschaftliches Personal, Forscher_innen. Machen Sie sich eine Liste potentieller Probleme, die jede dieser Gruppen haben könnte, abgeleitet aus den Videos, die sie sich angeschaut haben.

4. Beobachten Sie sich selbst eine Tag lang, den Sie an der TU verbringen, und machen Sie Fotos von Dingen, die Sie als problematisch für die Sicherheit, in Bezug auf die oben erstellte Liste, einschätzen. Schreiben Sie kurze Szenarien (zB. Studierende verlässt während der Vorlesung den Hörsaal für Toilettebesuch; bei Rückkehr ist der Laptop verschwunden). Die Liste der Maßnahmen ist Teil Ihrer Abgabe.

5. Beschreiben Sie Maßnahmen für die unterschiedlichen Personengruppen, mit deren Einhaltung die dringlichsten Probleme vermieden werden könnten. Bedenken Sie, dass Sie die grundlegend offene Natur der Universität nicht unterwandern wollen (zB. Kontrollen am Eingang). Diese Guidelines sind Teil Ihrer Abgabe.

6. Verfassen Sie Guidelines für jede der oben angesprochenen Personengruppen, mit denen die Maßnahmen umgesetzt werden könnten, und formulieren Sie ein fiktives Schreiben an die TU Wien, das den Verantwortlichen die Maßnahmen und Guidelines in übersichtlicher Form präsentiert. Dieses Schreiben ist Teil Ihrer Abgabe.

Abgabe

7. Ihre Abgabe besteht aus Ihrem Forschungstagebuch, eventuell bereinigt um persönliche Einträge, die Sie nicht preisgeben wollen, sowie den Teilen, die oben als Teile der Abgabe genannt sind. Gliedern Sie dieses Dokument bitte sinnvoll, und bemühen Sie sich, ein gut lesbares Layout zu gestalten. Erzeugen Sie dann daraus ein PDF[1] und geben Sie dieses im entsprechenden Abschnitt in TUWEL ab.

Bitte beachten Sie, dass Aufgaben dieses Typs **nach spätestens 2 Wochen abgegeben** werden müssen (ab der Verfügbarkeit dieser Beschreibung), und dann noch eine Review-Phase (1 Woche) durchlaufen. **Ihr selbst gewählter Termin gilt erst für die Endabgabe!**

Zusatz für Endabgabe

Ein wesentlicher Teil Ihrer Endabgabe ist der Abschnitt *Reflexion & Feedback*. Beantworten Sie dabei die folgenden Fragen für die finale Abgabe, also nachdem Sie die Reviews geschrieben/bekommen haben, und ergänzen Sie Ihr PDF um einen entsprechenden Abschnitt:

- Wurde Ihr Verständnis der gewählten Denkweise durch diese Übungsarbeit verändert?
- Glauben Sie, ein nachhaltiges Verständnis der gewählten Denkweise wird Ihnen im Studium oder danach im Beruf helfen?
- Welche Teile dieser Arbeit fanden Sie besonders schwer, welche zu einfach?
- Welche Aspekte dieser Arbeit haben Ihnen gut gefallen, welche würden Sie ändern?
- Was haben Sie bei dieser Arbeit gelernt? Ist diese Art von Übungsformat Ihrer Meinung nach sinnvoll?
- Hat das Schreiben der Reviews geholfen, Ihre eigene Arbeit zu verbessern? Falls ja: wie?
- Haben die Reviews, die sie bekommen haben geholfen, Ihre eigene Arbeit zu verbessern? Falls ja: wie?
- Sind Sie mit Ihrer Arbeit zufrieden?

---

[1] Beachten Sie bitte, dass inzwischen alle aktuellen Betriebssysteme die Erzeugung von PDFs ohne zusätzliche Software erlauben. Geben Sie keine PDFs ab, bei denen Werbung oder Wasserzeichen von Gratis-Software eingebettet ist. Für Unterstützung befragen Sie bitte die allwissende Müllhalde (das Internet) bzw. https://www.wikihow.com/Convert-a-File-Into-PDF

Beachten Sie: Die Antworten auf die Fragen im Abschnitt *Reflexion und Feedback* gehen **nicht** in die Beurteilung Ihrer Arbeit ein!

Beachten Sie bitte die Richtlinie zur Verwendung von generativer AI, die im PDF »Denkweisen der Informatik 2023« zu finden ist. Wesentliche Teile der Arbeit dürfen nicht durch generative AI-Systeme verfasst werden!

Anhang: Forschungstagebuch

Ein Forschungstagebuch ist ein (physisches oder digitales) Medium, in dem Sie den Fortschritt Ihrer Arbeit und Ihre Gedanken dazu bzw. Probleme damit schriftlich festhalten. Damit Ihr Forschungstagebuch dabei helfen kann, zufällige Ideen oder plötzliche Inspirationen notieren können, sollten Sie es immer bei sich haben (das spricht stark für ein digitales Forschungstagebuch). Für die Zwecke dieser Arbeit genügt eine einfache Text-Datei. Jeder Eintrag ist mit Datum und Uhrzeit versehen.

Einträge im Forschungstagebuch werden zB. zu folgenden Anlässen gemacht:

- Artikel gelesen (mit kurzer Anmerkung der Relevanz für Ihr Thema, Auflistung für SIe wesentlicher Punkte)
- Gute Suchbegriffe für Ihr Thema
- In einem Gespräch etwas relevantes gehört, mit Ideen, wie Sie das weiterverfolgen könnten
- Teil der Arbeit geschrieben, mit Einschätzung der Qualität

Sie können auch persönliche Dinge im Forschungstagebuch festhalten, also erfreuliche (zB. Gute Quelle gefunden!) wie unerfreuliche (zB. heute gar nichts weitergegangen, sehr frustrierend). Für die Abgabe des Forschungstagebuchs können Sie Teile, die Sie nicht preisgeben wollen, entfernen.

Anhang: Qualität von Quellen

Ein wesentlicher Teil der Recheche im Internet ist die Einschätzung der Qualität von Quellen. Dazu gibt es, nicht ganz unironisch, viele Hilfestellungen im Internet. Wir haben einige davon für Sie zusammengestellt, denen wir vertrauen:

- Saferinternet, Quellen richtig beurteilen – https://www.saferinternet.at/news-detail/online-quellen-richtig-beurteilen-aber-wie
- Lehrerfortbildung Baden-Württemberg, Arbeitstechnik 2: Überprüfung von Quellen im Internet – https://lehrerfortbildung-bw.de/u_gewi/gk/gym/bp2016/fb5/2_komp/6_vorlagen/3_methode/02_technik2/
- Wer es ganz genau will: Qualitätskriterien für wissenschaftliches Arbeiten – https://soztheo.de/forschung/qualitaetskriterien-fuer-wissenschaftliches-arbeiten/

Anhang: wie man einen wissenschaftlichen Artikel liest

Wissenschaftliche Artikel sind meistens nicht dafür geschrieben, von vorne bis hinten gelesen zu werden. In Ihrem Studium werden Sie aber viele wiss. Publikationen lesen. Da hilft es oft, eine klare Strategie zu haben, wie man das angeht.

Ich habe hier für Sie die Ultrakurzversion zusammengeschrieben. Sie finden nach diesem kurzen Guide einige Links zu längeren Versionen. Dieser Guide gilt für »typische« wissenschaftliche Texte, also solche, die dem üblichen Aufbau folgen.

1. Überfliegen Sie das Abstract. Sie werden dann verstehen, um was es im Artikel geht, warum die Arbeit verfasst wurde, und in wenigen Worten üblicherweise auch, was das Ergebnis der Arbeit war. Das hilft Ihnen, den Rest besser einordnen zu können.

2. Lesen Sie jetzt den letzten Abschnitt des Papers, üblicherweise »Conclusions« oder »Discussion« genannt. Damit sollten Sie jetzt wissen, was die Autor_innen gemacht haben, und warum Sie es gemacht haben. Sie wissen auch, was dabei herausgekommen ist.

3. Der Abschnitt vor den Schlussfolgerungen sind üblicherweise »Results«. Überfliegen Sie diesen Teil, um zu sehen, wie relevant er für Sie ist.

4. Sehen Sie sich die Abbildungen an. In groben Zügen können Sie jetzt verstehen, um was es in diesem Paper geht, und was die Autor_innen gemacht haben. Zugegeben, das wird einfacher, je öfter Sie es machen.

5. Es sollte einen Abschnitt geben, der die Methodologie beschreibt, meistens »Methods« o.ä. Versuchen Sie grob zu verstehen, wie die Autor_innen gearbeitet haben (qualitativ, quantitativ, etc.).

Sie haben jetzt ein gutes Bild davon, um was es geht, und können entscheiden, ob Sie den Rest des Papers auch lesen wollen (zB. weil es relevant oder interessant ist). Eventuell ist aber auch nur noch der Abschnitt »Related Work« (o.ä.) für Sie spannend, weil Sie dort weitere Papers finden, die sich mit derselben oder einer ähnlichen Fragestellung beschäftigen – und vielleicht suchen Sie ja genau solche Arbeiten.

Weitere Guides:

- https://drewdennis.medium.com/how-to-read-scientific-papers-quickly-efficiently-e7030c4018fa
- https://www.bmj.com/about-bmj/resources-readers/publications/how-read-paper
- https://paperpile.com/g/read-scientific-paper/