Miniprojekt "Criminal Thinking" Forschungstagebuch

1 Videos ansehen und Kategorisierung

1.1 Aufgabe

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.

1.2 Prozess

Datum	Uhrzeit	Eintrag
20.01.2024	17:00	Erstes Video[1] angesehen und Schwachstellen herausgeschrieben.
20.01.2024	18:00	Zweites Video[2] angesehen und Schwachstellen herausgeschrieben.
20.01.2024	19:00	Drittes Video[3] angesehen und Schwachstellen herausgeschrieben.
20.01.2024	19:10	Viertes Video[4] angesehen und Schwachstellen herausgeschrieben.
20.01.2024	19:20	Fünftes Video[5] angesehen und Schwachstellen herausgeschrieben.
20.01.2024	19:30	Sechstes Video[6] angesehen und Schwachstellen herausgeschrieben.
20.01.2024	20:00	Die herausgeschriebenen Angriffsvektoren durchgegangen und eine Kategorisierung ausgearbeitet.

1.3 Ergebnis

Schwachstellen:

- Jason E Street, DEFCON 19 talk[1]:
  - Anhand von Abnutzungserscheinungen die möglichen PIN-Kombinationen bei PIN-Eingabefeldern reduzieren
  - Den Schließmechanismus einer Tür blockieren
  - Mit einem Stück Karton den Türriegel zurückschieben und die Türe somit öffnen
  - EMails fälschen um Leute glauben zu lassen man seie rechtmäßig hier
  - Das Seil von einem „Kensingon“ Schloss nirgends festmachen
  - Unsichere PINs wie 0000, 1111, ... oder bei Zahlenschlössern die Zahl nur um eine Stelle verdrehen
  - Schlüssel an unsicheren Orten wie der Büroschublade lagern
  - Mitarbeiter erpressen
  - Sich als behindert ausgeben um mit Mitleid das Wachpersonal zu überwinden
  - Informationen an einem Ort sichern (z.B. Computersystem) aber an anderen Orten (z.B. Küche) nicht (siehe 22:47)
  - Sensible Dokumente nicht schreddern
  - Sticker mit Passwörtern am Montior hängen lassen
- Tactics of Physical Pen Testers[2]
  - Schlösser „lockpicken“
  - Die Angeln von Türen entfernen und anschließend die Türe herausheben.

  - Bei „Crash Bar“ Türen mit einem Gegenstand durch den Türschlitz durchfahren, die „Crash Bars“ treffen und somit die Türe öffnen
  - Bei „Thumb Turn Locks“ mit einem „Thumb Turn Flipper“ durch den Türspalt durchfahren und das Schloss aufdrehen.
  - „Request-to-Exit“ Sensoren mit Rauch aktivieren.
  - Mit einem entsprechen Werkzeug unter/über der Tür durchfahren und den Türgriff von innen nach unten drücken
  - Offen herumliegende Schlüssel stehlen
  - Einen frei verfügbaren Universalschlüssel verwenden
  - Zutrittschips klonen
  - Mit Verkleidungen und guten Geschichten Leute glauben lassen, dass was man macht legitim ist
- Path of Least Resistance: Red Team Stories[3]
  - Nachdem jemand mit entsprechenden Privilegien die Türe geöffnet hat durchgehen bevor sie sich wieder schließt
  - Herumliegende Zugangsdaten (wie Wi-Fi Passwörter) stehlen
  - RFID Karten klonen
  - Mit einem entsprechenden Werkzeug unter der Türe hindurchfahren und sie öffnen
- The ULTIMATE Physical Penetration Test[4]
  - Die Zugangskarte eines Mitarbeiters stehlen
  - Wichtige Dokumente die nicht geschreddert wurden aus dem Müll fischen
- Using Food to Bypass Security: Red Team Stories[5]
  - Mit Social Engineering Tricks Wachleute glauben lassen dass man ein autorisierter Mitarbeiter ist
- I Broke Into The International Security Convention[6]
  - Ein Badge fälschen

Kategorien:

- Social Engineering
- Türen umgehen
  - Schließmechanismus manipulieren/ausnutzen
  - Öffnungsmechanismus (mit Werkzeug) betätigen
  - Aus den Angeln heben
- Schlösser umgehen
  - Lockpicking
  - Universalschlüssel
  - Schlüssel stehlen
  - PIN Brute-Force
- Zutrittsnachweis beschaffen
  - Klonen
  - Fälschen
  - Stehlen

- Informationsbeschaffung
  - Frei herumliegende Informationen
  - Unsachgemäß vernichtete Informationen
- Erpressung

2 Weiteres Video suchen

2.1 Aufgabe

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.

2.2 Prozess

Datum	Uhrzeit	Eintrag
21.01.2024	14:00	Link zu dem Video[7] das mir ein Freund vor einiger Zeit geschickt hat herausgesucht.
21.01.2024	14:05	Das Video erneut angesehen.
21.01.2024	14:20	Zusammenfassung und Kategorisierung ausgearbeitet.

2.3 Ergebnis

Suche

Da mir ein Freund ein entsprechendes Video vor einiger Zeit geschickt hat gestaltete sich die Suche recht einfach, ich musste nur die entsprechende Nachricht in unserem Chat finden.

Zusammenfassung

Der YouTuber „Zac Alsop“ kleidet einen vorher gecasteten älteren Herrn in Billigklamotten und Accessoires von Wish ein und gibt ihn bei der „Fashion Week“ als Modell aus. Das funktioniert erstaunlich gut und er schleicht sich mit dem Fake Modell erfolgreich auf verschiedene Veranstaltungen inklusive der exklusiven After Party ein.

Kategorisierung

Der erfolgreiche Zutritt zu den Veranstaltungen wurde mittels *Social Engineering* erreicht.

3 TU Sicherheitsprobleme

3.1 Aufgabe

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

3.2 Prozess

Datum	Uhrzeit	Eintrag
25.01.2024	16:10	Probleme für Kategorie „Studenten“ ausgearbeitet.
25.01.2024	16:20	Probleme für Kategorie „Mitarbeiter“ ausgearbeitet.
25.01.2024	16:25	Probleme für Kategorie „Administation“ ausgearbeitet.
25.01.2024	16:30	Probleme für Kategorie „Sicherheitspersonal“ ausgearbeitet.
25.01.2024	16:40	Kurze Pause gemacht
25.01.2024	16:50	Probleme für Kategorie „Nichtwissenschaftliches Personal“ ausgearbeitet.
25.01.2024	17:00	Probleme für Kategorie „Forscher“ ausgearbeitet.

3.3 Ergebnis

Potentielle Probleme:

- Studenten:
  - Diebstahl von Eigentum
  - Identitätsdiebstahl
  - Installation von Schadsoftware auf unzureichend gesichertem Gerät
  - Ausspähen von Zugangsdaten mit einem bösartigen WiFi Netzwerk und RADIUS Server
- Mitarbeiter:
  - Racheaktionen wegen schlechter Note
  - Einbruch ins Kabinett um an Zugangs- und andere Daten zu gelangen
- Administration:
  - Mit Social Engineering zu bösartigen Taten überredet werden
  - Bestechung
  - Erpressung
  - Mit Malware infiziert werden
- Sicherheitspersonal:
  - Diebstahl von Schlüsseln
  - Kopieren von Zutrittskarten
- Nichtwissenschaftliches Personal:
  - Erpressung
  - Bestechung
  - Sabotage (um zu bewirken, dass die betreffende Person entlassen wird, etc)
- Forscher:

- Manipulation der Forschungsapparaturen
- Diebstahl von Ideen durch Konkurrenz
- Diebstahl von Equipment

4 TU Sicherheitsprobleme Dokumentation

4.1 Aufgabe

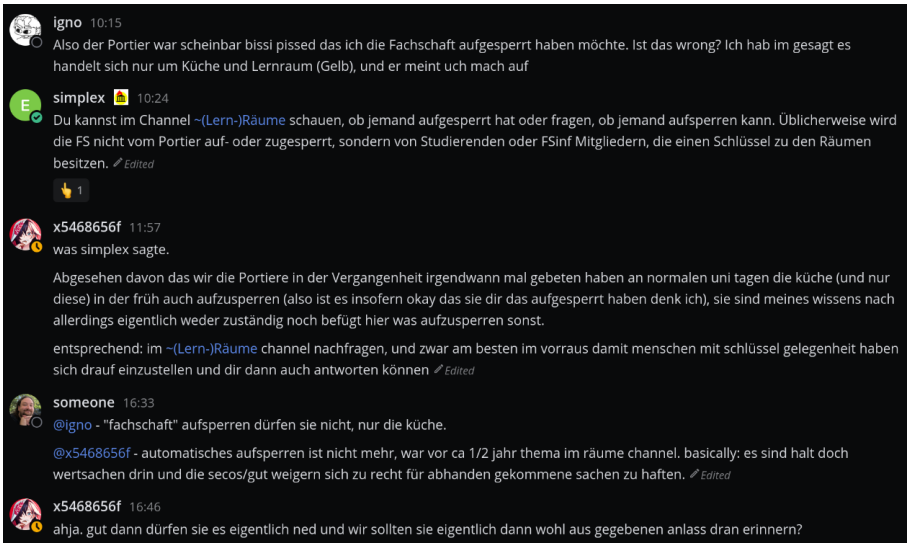
Beobachten Sie sich selbst eine Tag lang, den Sie an der TU verbringen, und machen Sie Fotos von Dingen, die Sie als problematisch für die Sicherheit, in Bezug auf die oben erstellte Liste, einschätzen.

4.2 Prozess

Datum	Uhrzeit	Eintrag
26.01.2024	12:00	Auf der TU angekommen.
26.01.2024	12:05	Angefangen an diversen Uni-Aufgaben zu arbeiten.
26.01.2024	17:00	Herumgegangen und diverse Sicherheitsprobleme dokumentiert.
26.01.2024	18:00	Entschieden, dass ich genug Material gesammelt habe, daher wieder in den Lernraum zurückgekehrt und angefangen die Bilder auszuwerten und in das Dokument einzufügen.
26.01.2024	18:05	Mich an einen Mattermost Thread erinnert in dem ein Sicherheitsproblem erläutert wurde: Ein Student bittet einen Security die Fachschaft aufzusperren. Obwohl dieser das eigentlich nicht darf kommt er der bitte vom Studenten nach. Ich bin mir nicht ganz sicher ob das als „Foto von problematischen Dingen“ durchgeht, habe mich aber dennoch entschieden es einzufügen, da es sehr passend ist.

4.3 Ergebnis

Unrechtmäßiges Aufsperren von Räumlichkeiten



Szenario: Security sperrt auf bitte einer Person die Fachschaft auf, diese entwendet anschließend herumliegende Wertsachen.

Unversperrter Laptop

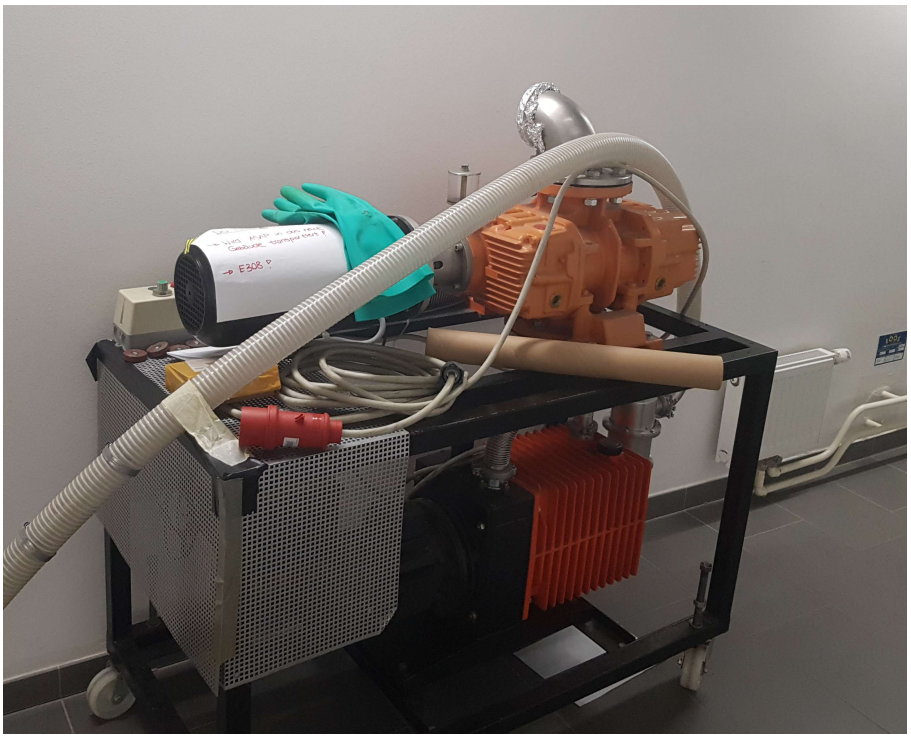
Szenario: Person lässt Laptop unversperrt und unbeaufsichtigt stehen. Jemand nutzt diese Situation aus und installiert Schadsoftware auf dem Gerät.

Breiter Türschlitz und mit Plastikkarte zurückschiebbarer Türriegel

Das Foto ist leider nicht gut gelungen und wird daher hier näher erläutert. Es stellt den Türschlitz mit dem gut erkennbaren Türriegel dar. Dieser lässt sich mit einer Plastikkarte zurückschieben und die Türe somit öffnen (wurde getestet).

Szenario: Unbefugter verschafft sich indem er den Riegel zurückschiebt Zutritt zu dem Labor eines Forschers und manipuliert dessen Equipment.

Am Gang stehendes Equipment



Szenario: Jemand böswilliges sabotiert das in einem frei zugänglichen Gang stehende Equipment.

RFID Karte klonen

Szenario: Eine böswillige Person versteckt ein entsprechendes Gerät in dem RFID-Scanner und klont damit die Zutrittskarten von Securitys oder anderen Personen die hier ihre Karte verwenden. Dies ist nur möglich unter der Voraussetzung, dass die TU Wien RFID-Karten verwendet, welche sich klonen lassen, was jedoch recht geläufig ist.

Unversperrte Türe

Szenario: Jemand böswilliges nutzt die unversperrte Türe aus um sich Zutritt zu einem eingeschränkten Bereich zu verschaffen. Dort findet er das Büro eines Administrators vor und installiert eine RAT[8] auf seinem PC.

Breiter Türspalt

Szenario: Ein Konkurrent verschafft sich Zutritt zu dem Büro eines Forschers, indem er ein entsprechendes Werkzeug unter der Türe durchschiebt um sie von innen zu öffnen. Dort stiehlt er die Arbeit seines Konkurrenten. Zusätzlich löscht er auch alle seine Dateien, um ihn auszubremsen um die gestohlenen Daten besser für seine eigene Arbeit verwerten zu können.

Türscharniere

Szenario: Ein Student ist mit seiner Note unzufrieden und will sich an seinem Professor rächen. Er bemerkt, dass die Türe zu seinem Büro Scharniere verwendet, die er mit einem einfachen Kreuzschraubenzieher entfernen kann. Er tut dies, hebt die Türe aus den Angeln und verschafft sich somit Zutritt zum Büro des verhassten Professors. Nun verwüstet er das Büro und löscht die Festplatte des Computers.

5 Sicherheitsguidelines

5.1 Aufgabe

Beschreiben Sie Maßnahmen für die unterschiedlichen Personengruppen, mit deren Einhaltung die dringlichsten Probleme vermieden werden könnten.

5.2 Prozess

Datum	Uhrzeit	Eintrag
26.01.2024	20:10	Die vorher dokumentieren Sicherheitsprobleme, sowie die potentiellen Probleme für die Personengruppen nochmal durchgegangen und angefangen darauf aufbauend Guidelines zu verfassen
26.01.2024	21:00	Nach einer kurzen Unterbrechung an der Fertigstellung der Guidelines gearbeitet

5.3 Ergebnis

Guidelines für Personengruppen

- Studenten:
  - Geräte immer versperren, wenn man sich von ihnen entfernt.
  - Auf seine Sachen aufpassen und sollte man sich von ihnen entfernen gegebenenfalls einen Freund bitten ein Auge darauf zu haben.
  - Am Gerät einstellen, dass das Zertifikat des RADIUS-Servers im *tunet* überprüft wird.
- Mitarbeiter:
  - Seine Türen mit Scharnieren versehen, die nicht einfach abmontiert werden können.
- Administration:
  - Schulungen die auf Social Engieering aufmerksam machen und dieses kontern in Anspruch nehmen.
  - Full-disk-encryption für alle digitalen Arbeitsgeräte einrichten, sodass man nicht bloß durch physischen Zugriff auf die Festpatte Schadsoftware installiert werden kann.
- Sicherheitspersonal:
  - Auf die Schlüssel aufpassen und diese unter keinen Umständen aus den Augen lassen.
  - Bevor man seine Karte an einen RFID-Scanner hält diesen auf Spuren von Manipulation oder versteckten Kartenklongeräten überprüfen.
- Nichtwissenschaftliches Personal:
  - Die Arbeits- und Büroräume immer korrekt verschließen.
- Forscher:
  - Wichtige Gerätschaften niemals am Gang stehen lassen.
  - Räume mit wichtigem Inhalt mit Sicherheitstüren sichern. Vorallem darauf achten, dass die Türe unten, oben und sonstwo keinen Spalt aufweist und dass der Riegel geschützt ist und nicht mit entsprechendem Werkzeug zurückgeschoben werden kann.

6 Fiktives Schreiben

6.1 Aufgabe

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.

6.2 Prozess

Datum	Uhrzeit	Eintrag
27.01.2024	20:20	Mit der Ausarbeitung des Schreibens begonnen.
27.01.2024	22:30	Das Schreiben fertiggestellt, das gesamte Dokument nochmals korrekturgelesen und eventuelle Fehler ausgebessert.

6.3 Ergebnis

Sehr geehrte TU Wien,

nach einem von mir durchgeführten Test der physischen Sicherheit Ihrer Infrastruktur sind mir leider einige Schwachstellen aufgefallen. Im folgenden werde ich Ihnen Maßnahmen und Guidelines erörtern, um Ihre physische Sicherheit zu verbessern.

Diese wären wie folgt:

1. Alle Personen sollten darauf achten ihre digitalen Gerätschaften zu versperren sollte man sich von Ihnen entfernen. Dies kann einfach durch drücken des Windows+L Shortcuts erreicht werden.

2. Alle Personen und insbesondere Studenten sollten auf ihre Sachen aufpassen um Diebstahl vorzubeugen. Muss man sich von seinen Wertsachen entfernen (beispielsweise um aufs Klo zu gehen) kann man einen Kollegen darum bitten ein Auge auf sie zu haben.

3. Jeder der das *tunet* WLAN Netzwerk verwendet, insbesondere Studenten und Mitarbeiter sollten das Zertifikat des entsprechenden RADIUS-Servers installieren um dem Diebstahl von Zugangsdaten vorzubeugen. Details hierzu, sowie das Zertifikat selbst können unter `https://colab.tuwien.ac.at/pages/viewpage.action?pageId=153387594` abgerufen werden.

   Zusätzlich empfiehlt es sich ein eigenes Passwort nur für das WLAN-Netzwerk zu setzen. Dies ist bei folgender URL möglich: `https://oase.it.tuwien.ac.at/ZID-Accounts.studentNetworkPassword`

4. Türen hinter denen sich wichtiges Equipment oder sonstige Sachen von Wert befinden sollten mit Scharnieren versehen werden die sich nicht einfach abmontieren lassen. Dies beugt unbefugtem Zutritt durch das simple aus-den-Angeln-heben der Tür vor.

   Weiters sollten solche Türen keinen Spalt, weder oben noch unten noch auf der Seite aufweisen. Dies hat den Grund, dass sonst Werkzeug hindurchgeschoben und die Tür von innen geöffnet werden könnte.

   Außerdem ist darauf zu achten, dass der Riegel geschützt ist und nicht mit entsprechendem Werkzeug zurückgeschoben werden kann.

5. Für Administratoren wird eine empfohlen eine Social Engineering Schulung anzubieten um diese auf das Problem aufmerksam zu machen.

6. Es wird empfohlen auf allen Arbeitsgeräten Full-Disk-Encryption einzurichten um die folgen eines physischen Zugriffs auf das entsprechende Gerät abzumildern. Unter Windows kann dies recht einfach mit dem quelloffenen Programm „VeraCrypt“ getan werden, siehe hierzu `https://veracrypt.fr/`. Alternativ dazu kann auch der in Windows eingebaute „BitLocker“ verwendet werden.

   Zusätzlich sollte diese Maßnahme auch allen Studenten und Forscher für private Laptops nahegelegt werden.

7. Sicherheitspersonal sollte geschult werden auf Schlüssel acht zu geben. Diese sind nicht aus den Augen zu lassen und sicher zu versperren.

8. Alle Besitzer von RFID-Zutrittskarten, inbesondere Sicherheitspersonal sollte vor Verwendung der Karte den Leser auf Spuren von Manipulation oder versteckten Klongeräten prüfen. Sollte sich hier ein Verdachtsmoment ergeben ist die Karte auf keinen Fall zu verwenden und jemand qualifiziertes zu informieren.

9. Alle Türen sind immer sachgemäß zu versperren. Dies sollte durch das Sicherheitspersonal durch entsprechende Rundgänge überprüft werden.

10. Forscher sollten wichtige Gerätschaften niemals offen beispielsweise im Gang stehen lassen sondern immer in einen versperrbaren Raum bringen.

Ich hoffe diese Guidelines können Ihnen helfen die Sicherheit Ihrer Einrichtung noch weiter auszubauen.

Mit freundlichen Grüßen
Max Muster

7 Literatur

[1] Jayson E Street. *Talk from DEFCON 19*. 28. Aug. 2011. URL: https://vimeo.com/28284322 (besucht am 20. 01. 2024).

[2] Devian Ollam. *Tactics of Physical Pen Testers*. 22. Sep. 2020. URL: https://www.youtube.com/watch?v=VJ4FDOw9NcI (besucht am 20. 01. 2024).

[3] TheNotSoCivilEngr. *[71] Path of Least Resistance: Red Team Stories*. 4. Apr. 2021. URL: https://www.youtube.com/watch?v=jcVIruSqI6w (besucht am 20. 01. 2024).

[4] Gary Ruddell. *The ULTIMATE Physical Penetration Test (from Better Call Saul)*. 26. Mai 2023. URL: https://www.youtube.com/watch?v=JketdMhzMz0 (besucht am 20. 01. 2024).

[5] TheNotSoCivilEngr. *[52] Using Food to Bypass Security: Red Team Stories*. 11. Sep. 2020. URL: https://www.youtube.com/watch?v=zgcP_mj9dJE (besucht am 20. 01. 2024).

[6] Max Fosh. *I Broke Into The International Security Convention*. 2. Nov. 2021. URL: https://www.youtube.com/watch?v=qM3imMiERdU (besucht am 20. 01. 2024).

[7] Zac Alsop. *I Faked My Grandpa To The Top of Fashion Week*. 22. März 2023. URL: https://www.youtube.com/watch?v=K_8_aO4iIsE (besucht am 20. 01. 2024).

[8] Proofpoint Inc. *What Is a Remote Access Trojan (RAT)?* URL: https://www.proofpoint.com/us/threat-reference/remote-access-trojan (besucht am 26. 01. 2024).