Unterrichtsablauf

01 Unterrichtsblock

Ziele

- S erkennen die dünne Grenze zwischen Legalität und Illegalität.
- S kennen die Rechtssituation im Bezug auf Computerkriminalität im Überblick und können Beispiele aus dem Alltag nennen
- S erhalten einen Überblick über die Entwicklung der Computerkriminalität.

Zeit	Inhalt	Material
	Begrüssung	
10‘	Start mit Auftrag: 1. Suchen Sie das Computec Online Adventure (COA) unter http://www.computec.ch/projekte/coa/ auf und beginnen Sie das Spiel. 2. Versuchen Sie die Passwort-Abfrage des DoD (Departement of Defense) zu umgehen (erste Aufgabe). Allenfalls Hinweis geben: Das Durchsuchen des HTML-Quelltexts wird am schnellsten zum Ziel führen. 3. Wie lautete das Passwort und wo kann es gefunden werden? Motivator	 S.2
5‘	Besprechen und Abschluss des Vertrages: „Die Schülerinnen und Schüler verpflichten sich, das erworbene Wissen nicht zu missbrauchen oder leichtfertig weiterzugeben.“	 Vertrag
5‘	Überblick über das gesamte Projekt	S.3
17‘	**Geschichte der Computerkriminalität** • Der Geschichtsteil kann weggelassen werden, falls die Zeit zu knapp ist. • Der Geschichtsteil wird als Motivation für die Behandlung der Gesetze betrachtet. Es soll gezeigt werden, dass sich die Computerkriminalität von einem Kavaliersdelikt zu einem Schwerverbrechen, bei dem es um viel Geld geht, gewandelt hat. • Ein kurzer Überblick vom Phone Hacking bis in die Neuzeit	S.6
5‘	**Computerkriminalität und Rechtssystem:** • Überblick • http://de.wikipedia.org/wiki/Computerkriminalit%C3%A4t	S.11
3‘	**Auftrag Hausaufgaben** Informationsblatt «00_Praxisbeispiele Recht».	

Hausaufgaben

Informationsblatt «00_Praxisbeispiele Recht» lesen. Evtl. auftauchende Fragen aufschreiben. (Rechtsfragen sind für die Lehrperson sehr schwierig zu beantworten – auch die Juristen scheuen sich konkreter Aussagen.)

02 Unterrichtsblock

Ziele

- S wissen, was eine IP ist und verstehen deren Funktion.
- S kennen IPv4.Sie wissen, dass IPv6 der Nachfolger ist.
- S können die IP-Adresse am eigenen Gerät bestimmen.
- S kennen die grundlegenden Shell-Befehle (ipconfig /all, ping) und können sie anwenden.
- S. wissen was Mapping (ICMP-Request) ist und wozu es dient.

Zeit	Inhalt	Material
3‘	Begrüssung/Ziele	
7‘	**Grundlagen Netzwerke** Bevor wir echte Angriffe durchspielen können, müssen wir gewisse Grundlagen erarbeiten: Wie kommunizieren zwei PCs miteinander? • IP o Analogie zu Telefon o Ipconfig - Netzwerkkonfiguration o Ping – Was ist das?	S.13
20‘	• Am PC mit «01_Arbeitsblatt IP» Aufgaben 1-8 lösen. o Ipconfig ausprobieren o Welche Funktion hat die IP-Adresse o Grundlegender Unterschied IPv4 und IPv6 o ping 127.0.0.1 resp. die eigene Adresse o ping der Nachbarn – Problem? (Ist ein «Ping» strafbar? Nein – in Deutschland, wenn das Gesetz streng ausgelegt würde) •	PDF 
	Besprechung AB IP	
15‘	**Mapping** Erklären von Mapping, ICMP und auf das Problem mit Firewall hinweisen An dieser Stelle wird bewusst noch nicht weiter auf die Firewall eingegangen, da dieses Thema zu einer anderen Netzwerkschicht gehört. Wir beheben nur die Probleme. o S bestimmen ihre IP -Adresse und tragen sie auf einer Liste auf Google-Spreadsheets ein. o **ICMP in Firewall aktivieren?** o Aufgabe 9 vom Arbeitsblatt«01_Arbeitsblatt IP» lösen. o Was bringen die Ergebnisse?	S.19
5‘	IP-Netze: Aufgabe der Subnetzmaske • A-C Netz • Private Bereich In was für einem Netz sind wir hier an der Schule? (privates B-Netz, in dem nur 255 Adressen vergeben werden können)	S.27

Hausaufgaben

- IP der Geräte Zuhause bestimmen, und wie lautet die Subnetzmaske, was für ein Netz ist es (A, B, C)
  Antworten in Forum der Gruppe EFI schreiben
- Text zu «02_Hackerparagraf - Auch die Aufpasser müssen aufpassen» lesen und die Kontrollfragen beantworten.

03 Unterrichtsblock

Ziele

- S kennen neben der IP-Adresse auch die MAC-Adresse und können diese am eigenen Gerät bestimmen.
- S wissen, was eine MAC-Adresse ist und kennen deren Funktion.
- S verstehen, warum es beide Adressen braucht.
- S wissen. was die Aufgabe der ARP-Tabelle ist und können sie mit «arp –a» anzeigen.
- S können den Protokollablauf des ARP nachvollziehen.

Vorbereitungen

- Wiki einrichten
- Google Spreadsheet einrichten für MAC-, IP-Adressensammlung
  Link dazu auf Netzlaufwerk ablegen

Zeit	Inhalt	Material
2‘	Begrüssung/Ziele	
10'	Besprechung der HA: • IP der Geräte Zuhause bestimmen, und wie lautet die Subnetzmaske, was für ein Netz ist es (A, B, C) Antworten in Forum der Gruppe EFI schreiben • Text zu «02_Hackerparagraf - Auch die Aufpasser müssen aufpassen» lesen und die Kontrollfragen beantworten.	
15‘	**MAC↔ARP↔IP** • «ipconfig/all» : Es gibt eine weitere Adresse: **MAC** – was ist das? • S bestimmen ihre IP und ihre MAC-Adresse und tragen sie auf einer Liste auf Google-Spreadsheets ein. Auswertung: Was zeichnet die IP-Adressen aus? Was zeichnet die MAC-Adressen aus? • MAC-Adresse (Media-Access-Control-Adresse) • Wozu braucht es eine MAC-Adresse? Problem der Eindeutigkeit. • Wozu braucht es IP-Adresse, wenn es bereits die MAC-Adresse gibt. • Übersetzungsdienst zwischen IP und MAC mit ARP. • Betrachten der ARP-Tabelle mit «arp –a» • Veranschaulichung der Funktionsweise mit interaktiver Animation	 

28‘	**Wireshark – Demonstration und Übung** • Sichtbarmachen des ARP-Ablaufes • Übung «03_Arbeitsblatt ARP untersuchen mit Wireshark» • Benutzung von Wireshark ist in CH erlaubt. Der Missbrauch von mitgeschnittener Information ist strafbar. • In Deutschland ist bereits das Installieren von Wireshark strafbar!!!! • Letzte Aufgabe des Arbeitsblattes: S schreiben ihre Darstellung des Protokollablaufes in ein Wiki. Dann können die Lernenden alle direkt die anderen Versionen lesen und beurteilen. Sollte die Zeit nicht reichen, dann kann dieser Auftrag als Hausaufgabe abgearbeitet werden. • Besprechung des Arbeitsblattes.	

Reserve/Hausaufgaben

- Arbeitsblatt «04_Mit ARP den ARP-Cache manipulieren»

04 Unterrichtsblock

Hinweis

Dieser Unterrichtsblock benötigt sicher mehr als eine Lektion!

Ziele

- S. wissen was Dienste, Protokolle und Ports sind.
- Sie kennen den Zusammenhang dieser drei Begriffe und können diesen anhand eines einfachen Schichtenmodells erklären.
- S. können gängige Dienste aufzählen und wissen, welche Protokolle und welche Ports dazugehören.
- S. wissen wie das Hybridschichtenmodell in seinen Grundzügen funktioniert.
- S. können die Aufgaben der einzelnen Schichten erklären.

Zeit	Inhalt	Material
1‘	Begrüssung	
2‘	Ziele: • Festigung MAC/IP ARP • **Was ist ein Dienst** • **Was ist ein Protokoll** • **Was ist ein Port**	S.40
5‘	Studium des ARP-WIKI-Eintrages: Jeder liest den Eintrag des nächsten und gibt ihm dazu ein Feedback. Wir schauen uns 3 Einträge gemeinsam an: Was meint ihr dazu? Wozu braucht es überhaupt diese MAC-Adresse?	
10‘	Besprechung Arbeitsblatt «04_Mit ARP den ARP Cache manipulieren» Ergänzungen zur Aufgabe 9 Die Versuche zeigen, dass sich grundsätzlich die Zuweisung von MAC- und IP-Adresse beliebig manipulieren lässt. Um eine Manipulation der ARP-Tabelle eines fremden Computers durchzuführen, wird von Angreifer aus eine gefälschte ARP-Antwort (auf die nie eine Anfrage stattgefunden hat) an das Opfer gesendet. Das Opfer nimmt die neuen Angaben in seine Tabelle auf. In der Unterrichtseinheit mit Cain & Abel wird genau das ausgenutzt, um den Netzwerkverkehr eines anderen Computers über den Angreifer-PC umzuleiten und dort alles mitzulesen	

Doppellektion

15‘	**Dienste, Protokolle und Ports** 1. Dienste • Was sind Dienste? Im Netzwerk und innerhalb des PCs 2. Protokoll	S.41

	• Was ist ein Protokoll? • Beispiel «smtp» 3. Dienste-Protokolle-Schichten • Erster abstrakter Zusammenhang über das Schichtenmodell • Betrachten der laufenden Dienste mit «msconfig» 4. Ports • Was sind Ports • Analogie mit Büro • Well-known Ports	
20‘	• Dienste ausprobieren mit Telnet: «05_Arbeitsblatt PortsDiensteProtokolle» Dienste werden angeboten und in Anspruch genommen. Dies ist ganz legal!	

Doppellektion

5'	**Rückblick HA:** 05_Arbeitsblatt PortsDiensteProtokolle **Was ist das Sicherheitsproblem beim Mailen mit Telnet?** Die Übung zeigt, dass das Fälschen von Mails sehr einfach ist und Phishing sehr gut möglich. Rückfrage: Bei wem hat das Versenden des Mails funktioniert??	
30‘	**Das Netzwerkschichtenmodell: Hybridmodell** **Ergänzung: OSI-Modell** 1. Anwendungsschicht • Mailprogramm, Browser greifen auf die Dienste der Transportschicht zu, um ihre Daten zu versenden. (smtp, http,…) 2. Transportschicht • Segmentierung der Daten. • Nummerierung und Beschriftung der Pakete → TCP & UDP 3. Netzwerkschicht • Korrekte Weiterleitung • IP-Adresse des Ziels 4. Data Link-Schicht • Fehlerfreie Übertragung • Prüfziffern →ARP 5. Physikalische Schicht • Übertragung der Daten auf die physikalische Leitung (Wireless, LAN, Bluetooth)	
30‘	Übung «06_Arbeitsblatt Schichtenmodell» durchführen Besprechung der Ergebnisse	
10'	Installation des Netzwerkes 1. Anmeldung in Public WLAN-EAP 2. Zugriff auf Netzwerkdateien über Educanet2 3. Wenn bereits möglich, dann Zugriff über WebDAV	
30'	DDoS Attaken	

Nun haben wir das Rüstzeug, um eine DDoS-Attacke durchzuführen:

Davor will ich aber von euch die Unterschrift, dass ihr das Wissen, das ihr hier erwerbt nie missbraucht.

DoS:
Als Denial of Service (kurz DoS, englisch für: Dienstverweigerung) wird in der digitalen Datenverarbeitung die Nichtverfügbarkeit eines Dienstes bezeichnet, der eigentlich verfügbar sein sollte. Obwohl es verschiedene Gründe für die Nichtverfügbarkeit geben kann, spricht man von DoS in der Regel als die Folge einer Überlastung von Infrastruktursystemen. Dies kann durch unbeabsichtigte Überlastungen verursacht werden oder durch einen mutwilligen Angriff auf einen Server, einen Rechner oder sonstige Komponenten in einem Datennetz.

Wir spielen nun so eine Attacke durch
Zuerst ganz simpel: mit ping auf meinen Rechner

1. Schauen, dass alle im Public-Netz per WLan verbunden sind
2. Ich gebe meine IP bekannt und zeige euch meinen Netzwerktraffic
3. Ihr schiesst eure PINGs auf mich los und wir beobachten die Netzlast auf meinem Rechner

Nun nehmen wir ein Tool zur Hilfe
LOIC -Low Orbit Ion Cannon (fiktive Massenvernichtungswaffe aus einem Spiel) und machen das gleiche damit.

1. Ich starte XAMPP und lasse die Lernenden die Webseite meines XAMPP besuchen.
2. Wir beobachten den Netzwerkverkehr?
3. Wir starten LOIC
4. Wir beobachten den Netzwerkverkehr
5. Wir versuchen erneut die Webseite zu besuchen
6. Ich deaktiviere die Firewall
7. Wir versuchen erneut die Webseite zu besuchen
8. Wir beobachten den Netzwerkverkehr

Wo liegt jetzt noch der Unterschied zum Angriff auf öffentliche Server?
Wir müssen die IPs der Webserver wissen.
Mit nslookup ist das aber keine Sache

Nehmen wir als Beispiel den Angriff als Protestaktion von Anonymus bei der Sperrung der Konti von Wikileaks

nslookup liefert bei der Suche nach www.postfinance.ch194.41.166.33
Gibt man diese IP ein, dann landet man tatsächlich auf der Seite der Postfinance.

Und schon könnte es losgehen.

05 Unterrichtsblock

Ziele:

- S können einen Portscan durchführen.
- S kennen verschiedene Ports und deren Bedeutung.
- S erkennen die zentrale Funktion der Firewall.
- S vertiefen die bisher erlernten Konzepte.

Zeit	Inhalt	Material
30‘	«07_Arbeitsblatt Portscan» Portscan des eigenen Computers mit netstat. Portscans durchführen mit Nmap • Wichtigste Einstellung:Quick Scan (durchsucht nur die wichtigsten Ports und die Timeoutzeit wird optimiert.) Bei Scan von Teilnetzen: z.B. 192.168.1.0/24 Das bedeutet, dass die ersten drei Byte (3x8bit=24bit) das Netzwerksegment (hier also 192.168.1.1-192.168.1.255) festlegen. 1. Nmap starten und eigenes System Scannen Welche Ports sind offen, welche Dienste werden angeboten? 2. Firewall deaktivieren und nochmals einen Scan ausführen Was hat sich verändert? Warum? Mache dich exemplarisch über dir unbekannte Dienste schlau. Nutze dazu das Internet. 3. Nachbarn Scannen in Zweiergruppen Dabei sollen die Gruppenmitglieder jeweils die Netzwerkart von Heim- auf öffentlich ändern und dabei die Veränderungen studieren und analysieren. (Windows 7) Portscans werden von Administratoren dazu verwendet, ihr Netzwerk auf Schwachstellen und Schädlinge zu überprüfen. Sind zum Beispiel gewissen Ports im Netzwerk geöffnet, so können sie auf aktive Schädlinge hinweisen. Andererseits wird ein Portscanner genau dazu eingesetzt, Schwachstellen im System ausfindig zu machen und auszunutzen. In Deutschland ist somit bereits die Installation von Nmap strafbar. (s. Hackerparagraph) Besprechung des Arbeitsblattes Mit netstat -ano wird auch die Prozess-ID angezeigt. Mit dem Taskmanager kann damit überprüft werden, was hinter dem Port läuft.	

Hausaufgaben

Eventuell «Warriors oft he net» schauen.Arbeitsblatt «08_Arbeitsblatt Warriors of the net» bearbeiten.

06 Unterrichtsblock

Hinweis

Dieser Unterrichtsblock benötigt sicher mehr als eine Lektion!

Ziele:

- Swerden auf die Risiken und möglichen Auswirkungen ihres Handelns im Internet sensibilisiert.
- S vertiefen das Wissen Rund um das ARP.
- S erkennen Schutzmassnahmen, um das Risiko zu reduzieren.

Zeit	Inhalt	Material
2‘	Begrüssung/Ziele	
60‘	«09_Arbeitsblatt ARP Cache Poisoning - Man-in-the-middle-attack» S mit Anleitung die verschiedenen Szenarien nachbauen lassen. Fragen beantworten. Dieses Arbeitsblatt befähigt, sensible Daten wie Benutzernamen und Kennwörter im Netzwerk abzufangen. **Ohne Wissen und Billigung der betroffenen Person ist diese Handlung strafbar!** Es geht hier nicht darum, Lernende zu einem Cracker auszubilden! Vielmehr soll auf die möglichen Risiken und Nebenwirkungen im Umgang mit dem Internet sensibilisiert werden und Schutzmassnahmen erkannt werden. Die Anweisungen auf dieser Anleitung müssen strickte eingehalten werden. **Besprechung**	  
	Allenfalls Reserve: An Peer-to-Peer Netzwerk weiterbasteln.	
60	• Musikordner aus Netzlaufwerk auf Partition D des Laptops speichern. • Wir erstellen einen neuen Benutzer: BN: admin KW: Asdf1234 mit Adminrechten • Die Netzwerkumgebung – die einzelnen Arbeitsstationen – warum können wir uns sehen??? Windows 7: Windows-Explorer → Netzwerk Um jetzt aber auf die Geräte zugreifen zu können, muss die Netzwerkerkennung und die Dateifreigabe aktiviert werden. Der entsprechende Balken wird auch sofort eingeblendet. Danach kann sofort zugegriffen werden. Da aber noch nichts freigegeben ist, ist auch nichts sichtbar. • Freigabe des ganzen Laufwerkes: Rechtsklick – erweiterte Freigabe – freigeben Nun Freigabe über Netzlaufwerkverbinden \\pc_name\c einbinden • Freigaben erstellen	Mp3-Files auf WMI-Server

	Auf einem Client hat es einen Ordner mit Musikdateien (LW D) Ordner freigeben für „admin“ öffnen, abspielen kopieren auf HD eigenen Ordner erstellen und Musikdateien hineinkopieren Ordner freigeben Hälfte der Dateien löschen lassen • Rechtemanagement Rechte der Benutzer einschränken: über Freigabe und über Sicherheits-einstellungen • Reserve: • Das Gleiche oder sehr ähnlich würde das Einrichten einer Heimnetz-gruppe gehen. Die freigegebenen Ordner (gewisse, wie Musik, Bilder und Videos, werden bereits bei der Konfiguration der Heimnetzgruppe frei-gegeben. • Jeder Client kann dann der Heimnetzgruppe beitreten, indem er ein Kennwort einmalig eingibt.	

Ausblick:

kleine Prüfung über die Grundlagen der Netzwerktechnik.