Zabezpečení wi-fi

- Útočník může chtít jenom využít připojení k Internetu, které ale platíte vy
  - Také se může dopouštět nezákonných aktivit a správní orgány se pak budou zajímat i o vás, protože data šla přes váš router
  - Údajně se stal i případ, že se policie začala zajímat o komunitu hráčů on-line her
    - Protože si vyměňovali názory, jak někoho zastřelí brokovnicí, kde získají AK-47, vypálí něčí sídlo, kde nastraží C-4, atd.

http://www.computer.org/portal/site/computer/menuitem.5d61c1d591162e4b0ef1bd108bcd45f3/index.jsp?&pName=computer_level1_article&TheCat=1005&path=computer/homepage/0905&file=perspectives.xml&xsl=article.xsl

- Anebo se útočník chce dostat do vašeho počítače
  - Což je také reálné nebezpečí, které vám hrozí s notebookem např. v kavárně s veřejnou wi-fi sítí
    - Nebo s mobilem/PDA, které mají wi-fi

- V domácí síti
  - Možností by bylo omezit šíření signálu z routeru
  - Nebo router správně nakonfigurovat
  - Rozhraní, na kterém lze router nakonfigurovat, je buď přístupné z vnitřní sítě, nebo z venku
    - Rozhraní je u levnějších typů jen webové
      - Tj. router se chová jako webový server
        - Poslouchá na nějaké předdefinované adrese
          - Např. 192.168.2.1

    - Pokud umožníte přístup ke konfiguračnímu rozhraní zvenčí, zvyšujete pravděpodobnost, že někde prolomí příslušné zabezpečení
      - Routery mají defaultně nastaveno nějaké administrátorské jméno a heslo, které se lidé většinou ani neobtěžují měnit
        - Pro útočníka jsou to dveře otevřené dokořán
        - Např. ke starším počítačům existovala možnost je „zabezpečit“ heslem na úrovni BIOSu
          - Ale také existovaly univerzální hesla => úroveň zabezpečení 0

- Jestliže dovolíte přístup ke konfiguračnímu rozhraní routeru jenom z vnitřní sítě, ještě stále se k němu může útočník dostat
  - Protože jde o wi-fi, nepotřebuje k tomu žádné kabely – stačí mu být v dosahu signálu
    - Např. byt pod vámi?

  - Řešením je povolit přístup ke konfiguračnímu rozhraní pouze a jedině přes fyzicky připojený kabel – např. RJ45
    - Pokud se útočník nedostane fyzicky k vám do bytu, konfiguraci nezmění

- Zatím máme vyřešeno zabezpečení konfigurace routeru
  - Zbývá ještě vyřešit, aby útočník vůbec neměl přístup do naší sítě

- Jde-li o připojení kabelem, typicky Ethernet s RJ45, kontrolujeme ho tím, komu povolíme kabel připojit
  - Nicméně, router lze nakonfigurovat jako DHCP server, který bude přidělovat ARP adresy jenom těm počítačům, pro jejichž MAC adresy to povolíme
    - Stále je možný ARP Poisoning a IP Hijack
      - Doma po kabelu ale nehrozí

  - Výhodou DHCP je, že případného útočníka objevíte v záznamech včetně jeho MAC adresy
    - Lze ji pak porovnat s konkrétním hw
      - Pokud si ji ovšem nezměnil

- Stejným způsobem lze omezit přístup zařízení přistupující k routeru pomocí wi-fi
- Povolíme MAC adresy jenom těch zařízení, jejichž provozovatelům důvěřujeme

- Nicméně, síť stále ještě není zabezpečena
  - Je možný např. ARP Poisoning
  - Vysíláme nezašifrované informace, které může kdokoliv v dosahu signálu odposlouchávat a podvrhnout

- Dalším krokem je proto zašifrování komunikace
  - Útočník nebude moci data odposlouchávat, aniž by byl schopný prolomit používanou šifru
  - A zároveň tak nebude schopen namluvit routeru, že mu má věřit, protože mu nedokáže poslat správně zašifrovanou zprávu

- Bohužel, všechny použité operační systémy a samotný router nemusejí vždy podporovat to nejlepší šifrovací schéma
  - Jestliže mají komunikovat všichni, není jiného východiska, než použít to nejslabší
  - Někdy za to mohou i ovladače síťové karty

- WEP
  - Rozšířený, lze snadno prolomit
    - Zastaví jen amatéra, který neví, co dělá
    - *Runtime decoding of WEP packets for known networks – kismetwireless.net*

- WAP – TKIP – z WAP variant nejméně bezpečné, zato více rozšířené než ostatní varianty
- WAP2 – AES – bezpečnější než WAP – TKIP
- WAP Radius – ověření oproti serveru

- Bezpečné šifrovací schéma znamená, že použijeme nějaké heslo, které musíme fyzicky zadat na zařízení, kterému chceme umožnit využívat naše wi-fi připojení
  - Heslo bude silné a necháme si ho pro sebe

- Dále je možné využít firewall, který routery mají, a omezit provoz na síti podle dalších pravidel

- Mimo domácí síť
  - Např. smartphone se Symbianem, patřičným sw a wi-fi lze používat jako hotspot
    - Tj. není nutné kupovat wi-fi router
      - Ale zaplatí se to operátorovi – např. GPRS

    - Ale to musíme dobrovolně spustit příslušný software, k čemuž nás skrytý útočník nedonutí
      - Navíc tomu nepřejí ani cenové tarify

  - Reálný útok je možný, když využijeme volně dostupnou wi-fi síť, abychom si vybrali poštu, nebo zavolali přes Skype
    - Skype navíc dělá ze silných uzlů tranzitní
      - Tj. přes takový uzel jdou i cizí hovory

  - Jediným funkčním řešením je vytvoření zašifrovaného VPN spojení pomocí asymetrické šifry na důvěryhodný server
    - V otevřené síti je jinak možné data pohodlně odposlouchávat
    - Nebo prolomit dohodnutí klíče pomocí útoku Man in the Middle za pomoci ARP Poisoning
      - Viz vztah Diffie-Hellman a HTTPS
    - Bohužel to není pro každého a vždy možné, takže se nakonec lidé musejí spolehnout na pravděpodobnost, že zrovna jim se nic nestane

- Zabezpečení wi-fi se nevyplatí podcenit
  - Když se vám nepovede, routery poskytují možnost zrušit provedené změny v nastavení, aniž by jste k nim byli fyzicky připojeni, a zkusit to znovu

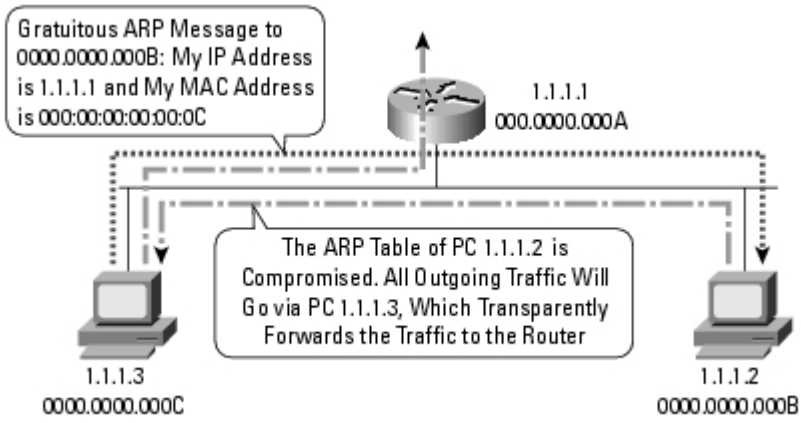
- Jakýkoliv router je jenom počítač, na kterém běží některý z operačních systémů
  - Je přístupný útokům stejně jako normální počítač
  - Viz dále
  - http://www.indiana.edu/~phishing/papers/warkit.pdf

ARP Poisoning

- Aby bylo možné provést útok Man in the Middle, prostředník musí být buď fyzicky zapojen mezi oběma uzly
- Anebo je musí zmást tak, aby posílaly svá data přes něj
- ARP Poisoning je jedna z možností, použitelná na lokálním segmentu

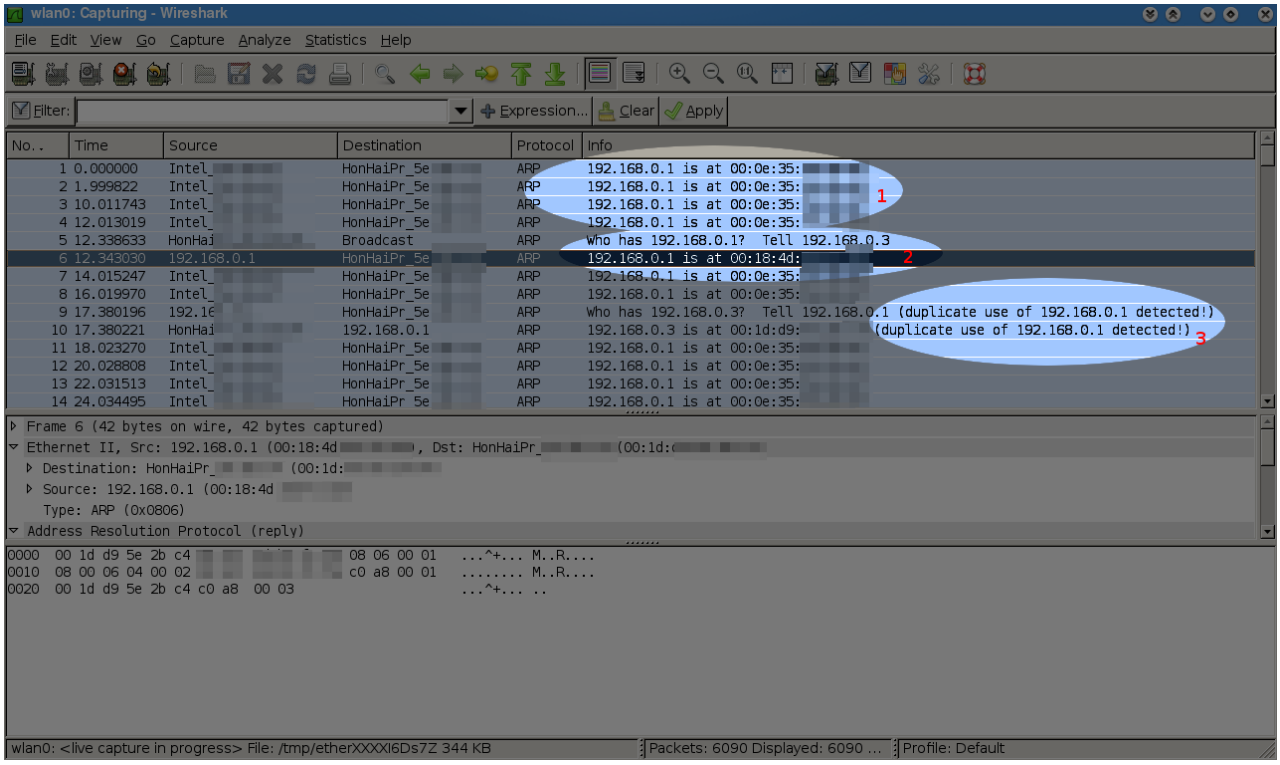
- Aby bylo možné používat IP protokol, je třeba asociovat IP adresu s fyzickou adresou zařízení
  - Např. MAC u Ethernetu

- ARP protokol nemá žádný bezpečnostní mechanismus, jak ověřit, či zamezit falšování zprávy
- Stačí jenom poslat falešnou odpověď, ve které bude napadená IP adresa asociována s MAC adresou útočníka
- Příjemce této zprávy si upraví záznamy o IP a MAC adresách
  - A až bude příště něco posílat na tuto IP adresu, rámec, který ponese pro ni určený IP paket, bude doručen na MAC adresu útočníka



http://www.cisco.com/warp/public/cc/pd/si/casi/ca6000/prodlit/vlnwp_wp.htm

- Obrana v IPv4
  - Použití statického přiřazení IP adres k MAC adresám
    - Což je na velkých sítích neúnosné



http://linux-tipps.blogspot.com/2008/06/detect-and-counter-arp-poisoning-under.html

  - Použije se speciálně vybavený uzel, který se vždy podívá do ARP rámce a v případě detekce útoku ho zahodí
    - Ale v kolika sítích se to doopravdy dělá?
    - Pokud vám takové riziko reálně hrozí, je možné si nainstalovat potřebný sw přímo u sebe
      - Např. ArpON

  - Mnohem běžnější opatření je, že administrátor sítě sebere uživateli práva nutná k provozování takového softwaru
    - V kolik případech však jde o opatření, který si admin ani neuvědomil, protože sledoval jiné cíle?

    - V některých případech však nejde o útok, ale např. o maskování výpadku důležitého serveru
        - V rámci redundance mohou v síti běžet dva

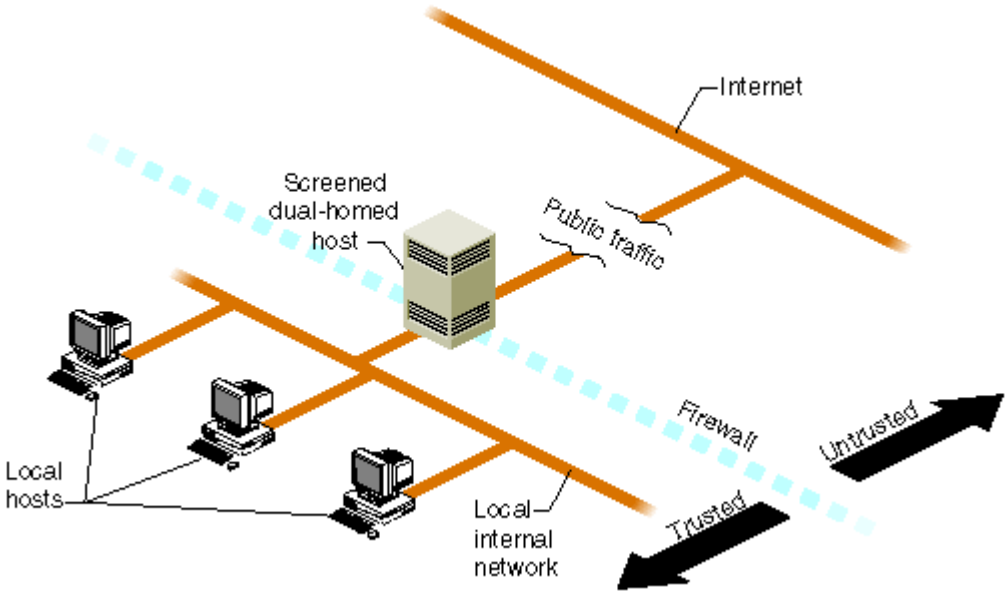
    - Spolehlivým řešením je pokládat celý komunikační kanál za nezabezpečený a důsledně používat možnosti šifrování

- Pro IPv6 se používá jiný protokol
    - Neighbor Discovery Protocol

Firewall

- Jak se vnějšímu světu prokazujete svou IP adresou, některý nekalý živel pojme za svou takovou myšlenku, že se vám naboura do počítače
    - Nemusí to být přímo on fyzicky, ale může se jednat o útočící vir
    - Ale také se může jednat např. o spyware, který už běží na vašem počítači a chce odeslat o vás získaná data

- Firewall může být nasazen jak na úrovni celé sítě,
- Tak by měl být nasazen přímo ve vašem počítači
    - V některých sítích je doba do zahájení útoku otázkou desítek sekund
        - Např. kavárna s veřejně dostupnou Wi-Fi



http://freon.chem.swin.edu.au/library/SGI_bookshelves/SGI_Admin/books/IA_BakSecAcc/sgi_html/ch05.html

- Firewall představuje množinu pravidel, která říkají, které pakety síťové úrovně propustit, a které naopak zahodit
  - Tj. např. IP a ICMP pakety

- Prakticky každý počítač v síti naslouchá příchozím spojením na nějakém portu
- Každý software obsahuje nějakou chybu
- Pokud útočník pošle správně vytvořenou zprávu na správný port, může donutit program na napadeném počítači provést akce, kterou nikdo nepředpokládal
  - Např. spustit útočníkův vlastní kód
- Firewall tomu umožňuje zabránit už tím, že komunikaci nepovolí

- Dále je to užitečné, ale mimo rozsah KIV/ZPS

- První možností je zakázat komunikaci podle vzdálené síťové adresy (např. IP adresy)
  - Tj. bez ohledu na to, který program by chtěl pakety posílat

- Další možností je vytvořit seznam programů, které smějí komunikovat
  - Tj. pro všechny ostatní programy bude síť nepřístupná
  - U dobrého firewallu lze nastavit
    - Vzdálená, popř. lokální, IP adresa kterou je možné použít
    - Na kterých portech smí program poslouchat na příchozí pakety
    - Ze kterých portů mohou pakety přicházet
    - Typ protokolu
      - ICMP, IGMP, TCP, UDP
    - Konkrétní program jedinečně určený cestou ke svému spustitelnému souboru
      - Co kdyby se některý vir rozhodl pojmenovat např. iexplorer.exe?

  - S dostatečnými oprávněními, nebo starším OS, je možné, aby jeden program „propašoval“ svůj kód do jiného už spuštěného program a tam tento kód spustil
    - Např. fce WinAPI CreateRemoteThread
      - Technik, jak to udělat, je více
    - Od Vista výše to však lze udělat jenom s administrátorskými právy
      - Pokud to ovšem někdo s nimi ochranu nevypnul, protože ho to pořád obtěžovalo s nějakou hláškou:-)

        - Např. spyware by tak mohl použít spuštěný prohlížeč a schovat svou komunikaci do něj
        - Některé firewally umožňují ošetřit i tohle

- Nejsofistikovanější z uvedených metod je možnost provádět analýzu datového toku
    - A buď paket zahodit
    - Nebo upravit jeho obsah

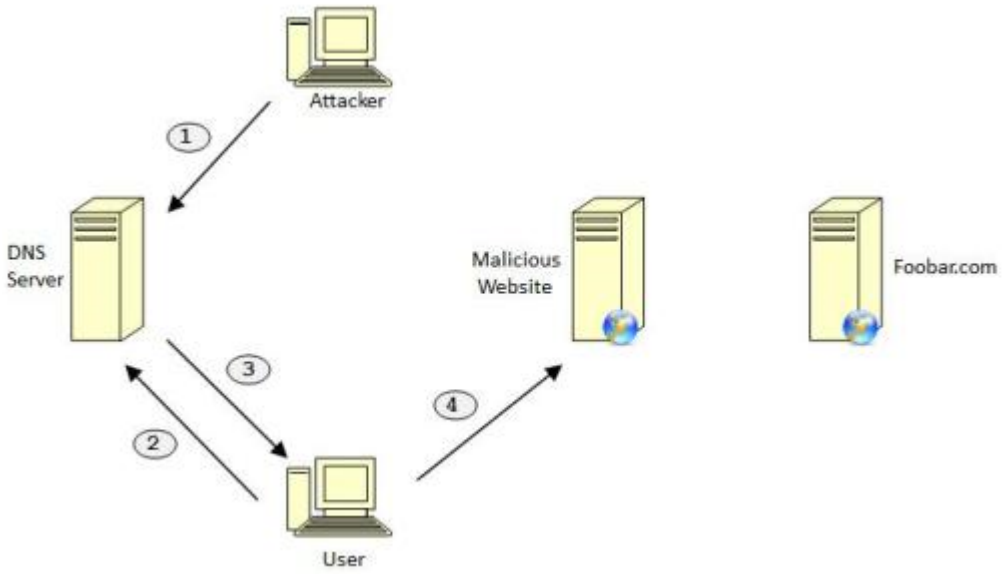
DNS Cache Poisoning

- Další možnost, jak realizovat útok Man in the Middle
- Chce-li např. oběť navštívit stránky své banky, kde se přihlašuje jménem a heslem, její počítač musí nejprve získat IP adresu stránek banky

- Pokud se útočníkovi podaří oběti doručit DNS záznam, kde bude jeho IP adresa, má vyhráno
    - Útočník na vrácené IP adrese spustí webový server s identickým rozhraním, jako má banka
    - Oběť ukolébaná podobou zadá své údaje
    - Útočník napíše „omlouváme se za momentální výpadek, prosím zkuste to za 15min“
        - A mezitím se sám přihlásí na skutečné stránky banky, na konto oběti, která mu právě ochotně sdělila své údaje na útočníkovo IP adrese

- V rámci bezpečnosti je třeba používat šifrované spojení HTTPS
- Slušný prohlížeč varuje, že s použitým certifikátem serveru něco není v pořádku
  - Většina uživatelů ale podobné zprávy „bezduše vyOuKuje“ a prohlížeči tak řekne, že je to v pořádku
    - Prohlížeč by totiž akci jinak zastavil a bylo by po útoku
      - Za blbost se platí

- Slušný firewall si pamatuje asociace IP adres a doménových jmen
  - Pokud nesedí, zobrazí varování
    - A uživatel zase udělá OK…
  - Občas to nesedí, protože mohli změnit ISP a tím i používaný rozsah IP adres
    - Legální důvod, o kterým by slušná banka informovala
    - IP rozsah je možné ověřit v databázi RIPE
      - Kolik uživatelů to udělá?



http://blogs.technet.com/mmpc/archive/2008/08/28/a-normal-day-at-the-office.aspx

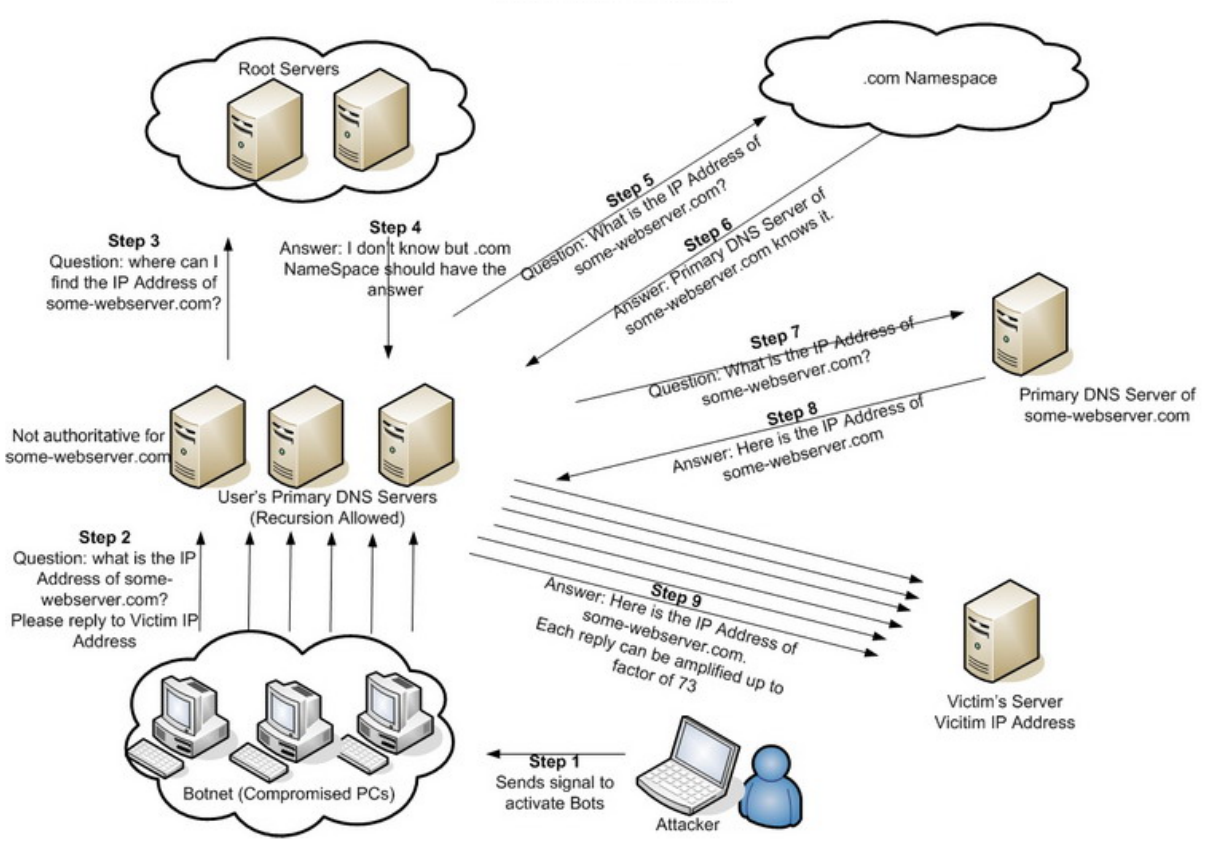
- Jednou z možností realizace útoku je poslat falešnou zprávu s aktuálními informacemi DNS serveru
  - Ala ARP Poisoning
  - DNS server si aktualizuje data podle falešné zprávy
  - A podvrhnutá data vrací obětem
  - Existuje DNSSec, který přijímá aktualizace pouze od důvěryhodných zdrojů
    - Ostatní jsou ignorovány
    - Kolik adminů už si to nastavilo?
      - Namátkovou kontrolou v databázi CZ.NIC nebyl v době psaní přednášky objeven ani jeden takto zabezpečený DNS server

- Další možností je kombinace s ARP poisoning
  - K IP adrese lokálního DNS serveru se podvrhne MAC adresa útočníka
    - Požadavek na IP adresu doménového jména banky útočník zachytí, ale už nepošle DNS serveru
    - Místo toho, pošle zpět DNS odpověď se svou IP adresou

- Operační systém má svou vlastní cache doménových jmen a IP adres
  - Soubor hosts
  - Stačí, když ji např. nějaký malware přepíše se svými hodnotami

  - `127.0.0.1 www.banka.cz`
    - Ať už doména banka.cz používá jakýkoliv rozsah, v tomto případě by se požadavek vždy poslal na adresu 127.0.0.1

- Další možností útoku je např. DNS Forgery

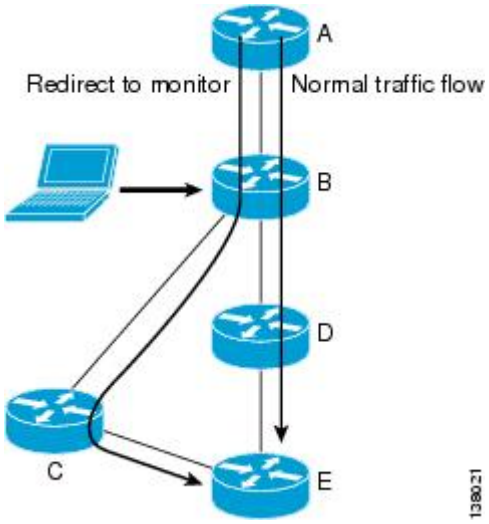


http://www.nirlog.com/2006/03/28/dns-amplification-attack/

Útok směrovacím protokolem

- Co když oběť není na našem segmentu a tak nelze použít ARP Poisoning?
- A co když přistupuje přímo podle IP adresy, takže nelze použít ani DNS Cache Poisoning?
- Je-li cílový počítač mimo síť oběti, pakety musí projít alespoň jedním routerem

- Útočník routeru podvrhne popis optimální cesty k uzlu, kam se chce oběť dostat
- Protože cesta je optimální, router ji přijme a začne používat
  - Navíc ji začne šířit i ostatním routerům
- Oběť pošle svá data routeru, jako vždy, ale ten už je pošle po právě instalované „optimální“ cestě
  - Ta optimální být nemusí, ale vede přes uzel, který je pod kontrolou útočníka

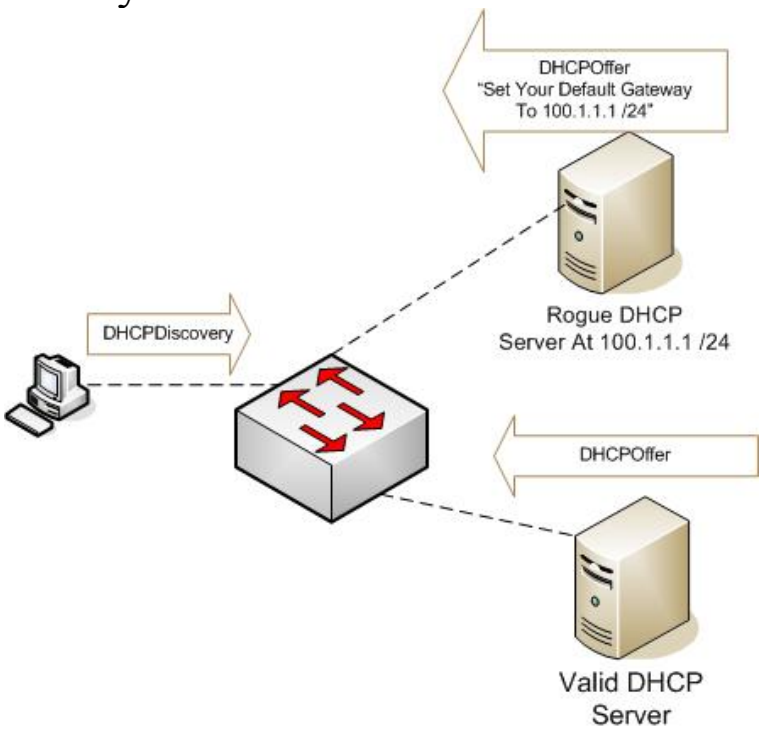


http://www.cisco.com/en/US/docs/ios_xr_sw/iosxr_r3.3/security/design/guide/sg33ddos.html

- Řešením na straně uživatele je používat šifrovanou komunikaci a neumožnit útok Man in the Middle pomocí dvou kanálů

- Řešením na straně správce sítě/Autonomní oblasti je umožnit přijímat aktualizační zprávy jenom z autorizovaných routerů

- Jsou-li oba uzly na stejné sítě, je možné modifikovat směrovací tabulku přímo na počítači oběti
- Buď pomocí malwaru, nebo útokem na DHCP server oběti
- DHCP server kromě přidělování IP adresy také
  - Posílá informace o výchozí bráně
  - A adresy DNS serverů



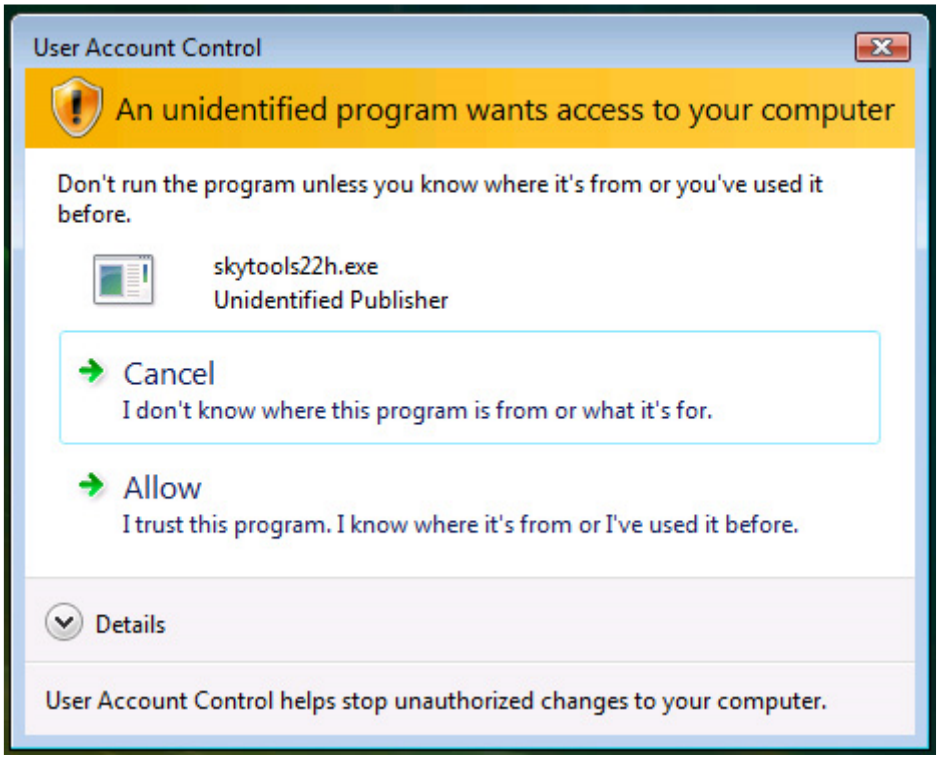
http://www.thebryantadvantage.com/BCMSNCiscoCCNPExamTutorialDHCPSnooping.htm

  - Útočníkovi je stačí podvrhnout serveru a všichni na síti si je z DHCP serveru načtou
  - Je-li to možné, pak se lze bránit statickým nastavením DNS serverů a výchozí brány
    - A neumožnit je automaticky měnit
      - Což po vás bude chtít většina adminů větších sítí

Viry, adware, spyware, rootkity a další malware

- Rozsáhlé a vždy aktuální téma, nicméně daleko za rozsahem KIV/ZPS
- Obranou je specializovaný software a vhodný OS
  - Ale také využívání jeho možností
  - Např. ptá-li se vás OS, zda opravdu chce pokračovat, že program chce administrátorské práva…

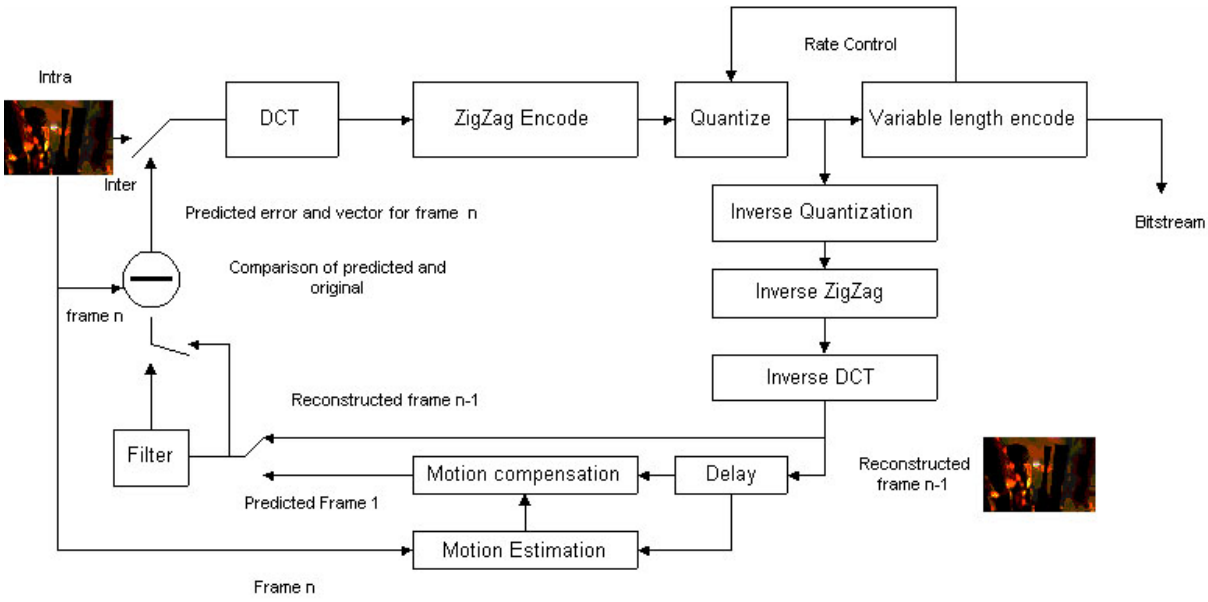
- Např. ve Windows
  - Některý malware je schopný si tlačítko „Pokračovat“ stisknout sám
    - Pošle zprávu WM_COMMAND



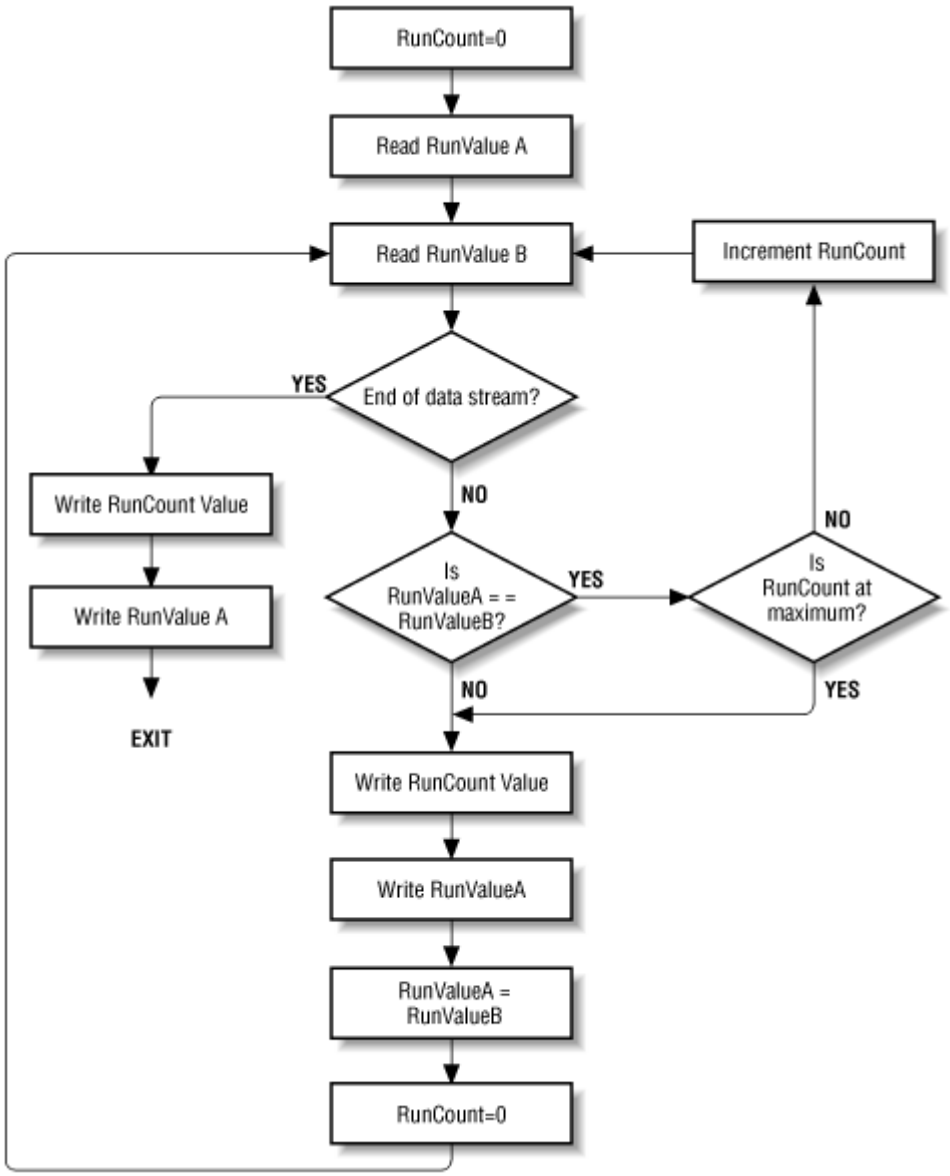
  - Ve Vistě to však nejde, protože pro potvrzovací okno se otevře nová plocha, kterou malware nevidí
  - Přesto se i tak najdou uživatelé, kteří si tuhle schopnost Vist vypnou, protože je obtěžuje v práci

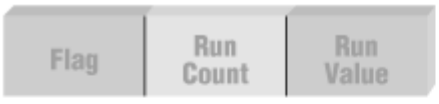
- Uvedený příklad šíření viru se stále ještě používá a např. umožňuje rychlou instalaci viru z webové stránky, aniž by byl uživatel „obtěžován“ podobným hlášením
  - I když ho má zapnuté

- Každý program obsahuje nějakou chybu, která se projeví v závislosti na tom, jaký mu poskytneme vstup
- Např. bude-li se jednat o prohlížeč obrázků/přehrávač videa a specifický kus sw, o kterém víme, že má jistou slabinu – tj. chybu
- Grafické a video formáty jako je jpg, png a mpeg používají kompresi obrazových dat
  - Tj. obsahují instrukce, co a s čím má program dělat, aby obrázek dekódoval a pak ho mohl zobrazit



http://ai3.asti.dost.gov.ph/h.323/video.htm

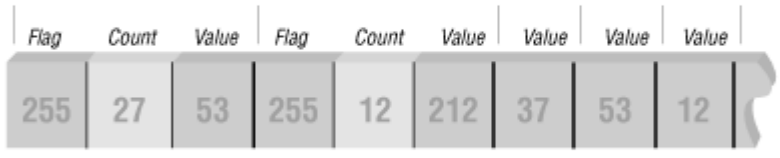


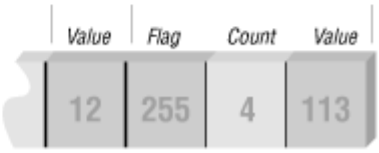


Flag = 255

Encoded line with the following runs:

28 pixels of value 53
13 pixels of value 212
1 pixel of value 37
1 pixel of value 53
1 pixel of value 12
1 pixel of value 12
4 pixels of value 113





http://enteos2.area.trieste.it/russo/LabInfoMM2006-2007/ProgrammaEMaterialeDidattico/daStudiare/010RLE.htm

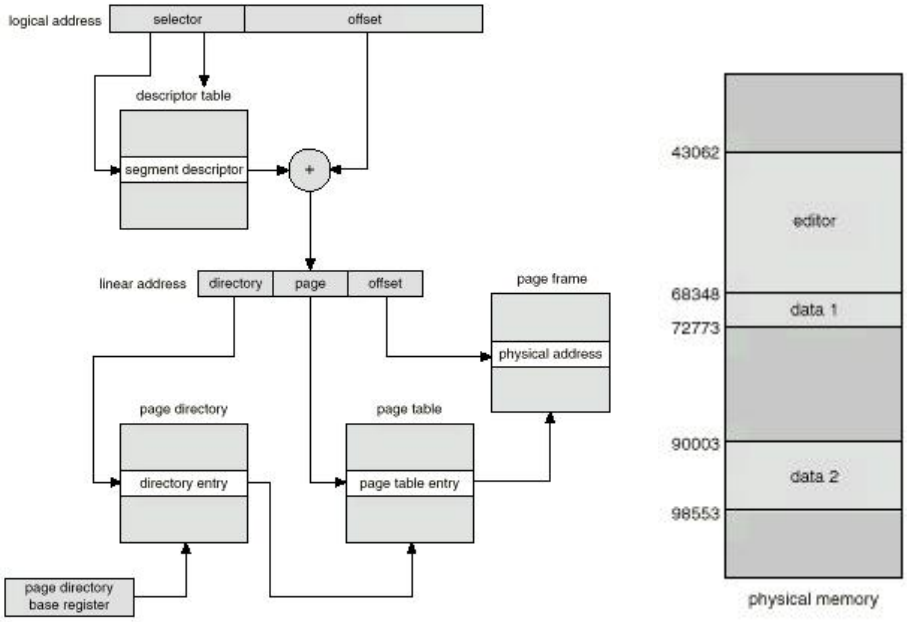
- Může se stát, že na určitou sekvenci dat program zareaguje chybou
- A data, která měl původně jenom dekódovat a zobrazit, ve skutečnosti spustí jako programový kód
- Který útočník vložil do souboru namísto skutečného obrázku

- Protože se obrázek ve skutečnosti neuloží na disk
- Ani se kvůli němu nespustí nový proces, spustí se to v rámci běžícího procesu – např. webového prohlížeče,
- Antivir nebude nic hlásit, protože ani o ničem neví

- Nemusí se jednat hned o video, ale např. o archív apod.

- Naštěstí, problém byl tak závažný, že je ochranu postaráno přímo na hw úrovni

- (Virtuální) Paměť počítače
  - RAM + odkládací soubor
  - a dělí se na bloky zvané segmenty (a ty na stránky)



http://data.uta.edu/~ramesh/cse3320/chap8.html

- Každý spuštěný program vlastní několik segmentů
  - V jednom má uložený programový kód
    - Tj. popis, co má program dělat
  - V ostatních data

- Každý segment má svůj popisovač
- A v něm bit, který říká, zda segment obsahuje spustitelný kód, či data, která se nemají spouštět
  - Útočníkův kód propašovaný v obrazovém formátu totiž vždy bude v datovém segmentu

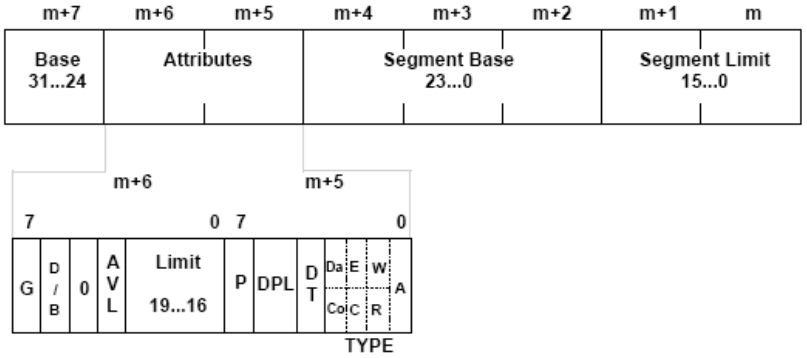


Figure 2. Segment Descriptor Layout

Bit Name	Bit Meaning
G	Granularity bit, used to determine if the limit is check on byte or 4KB page granularity.
D/B	Default/Big bit, for code segments represent the default operand size (16 or 32 bit). For expand down data segments it affects the operation of limit checking (this maintains compatibility with 286 protected mode expand down segments).
AVL	Available bit, this bit is available for use by the system designer.
P	Present bit, indicates that the specified segment is present in memory. Can be used to help with the implementation of virtual memory system.
DPL (2-bits)	Descriptor Privilege Level, Used by the protection mechanism.
DT	Descriptor Type, for systems descriptors DT=1 for segment descriptors DT=0.
Code/Data	Segment Type bit, indicates if the segment is a Code (=1) or Data (=0) segment. The setting of this bit effects the meaning of bits 1 and 2
E (Data)	If E=1 the data segment is an expand down data segment (typically used for stacks).
W (Data)	If W=1 the data segment is both read and write, else segment is read-only.
C (Code)	If C=1 then the code segment is a conforming code segment
R (Code)	If R=1 then the code segment is executable and readable, else it is execute-only.
A	Access bit, The processor automatically sets this bit whenever a descriptor is referenced. The bit is cleared by software.

Table 1. Segment Descriptor Attributes

ftp://download.intel.com/design/intarch/papers/exc_ia.pdf

  - Procesor: NX – No Execute
    - Obsahují ho všechny moderní procesory
  - Windows: DEP – Data Execution Prevention
    - Využití NX

- Když byla vyřazena přímá možnost, objevila se alternativa, která se používá dodnes
  - Úspěšně
  - A funguje na stejném principu

- Operační soubory umožňují spouštět dávkové soubory
  - .bat, .cmd, .sh
    - Anebo např. skripty/makra pro Office
- Dávkový soubor je sekvence instrukcí pro OS, co má udělat
  - Respektive, pro shell, který dávkový soubor interpretuje
- A protože je dávkový soubor vždy uložen v datovém segmentu, hw ochrana tu není nic platná

- Útočník si připraví potřebný dávkový soubor a ten prezentuje oběti jako např. neškodný obrázek
  - Např. pojmenováním souboru vhodnou příponou
  - A následně použije např. metodu POST protokolu HTTP, ve které uvede takové parametry, které dávkový soubor spustí

- Řešením je zakázat nebezpečné konstrukce a neakceptovat určité typy požadavků
  - Jejich seznam je znám
  - Takže i v případě spuštění, nedojde alespoň k rozsáhlým škodám

  - Příklady za všechny jsou SSI a PHP
    - Např. s nezabezpečeným PHP lze vhodnou konstrukcí uživatelské stránky spustit programový kód získaný z jiného webu

Dynamické HTML a HTTP

- Je možné vytvářet dynamický kód, který bude zapisovat odkazy na podvodné stránky, ale přitom je prezentovat jako součást důvěryhodného webu – phishing
  - Např. uživatel uvidí www.banka.cz
  - Ale ve skutečnosti prohlížeč použije odkaz www.podvodnici.org

- Prohlížeč obvykle ve stavové liště zobrazuje URI odkazu
  - Např. JavaScript umí lištu přepsat
    - Tedy uměl, moderní prohlížeče to už neumožňují

- Existuje však celá řada sofistikovanějších technik
  - Cookie Poisoning
  - Cross-Site Scripting
  - Parameter Tampering
  - SQL Injection
  - A další

- Např. Session Hijacking umožňuje převzít kontrolu nad stávající relací – připojením k webu
  - Např. k bankovnímu účtu, nebo Internetovému obchodu
    - A zaplatit si z účtu oběti své věci
  - `<input type="hidden" name="sessionID" value="54321abcd">`
    - Skrytý formulář webové stránky s id relace
- Nezapomeňte, že i pěkně zobrazený e-mail je ve skutečnosti HTML kód
  - A že obrázky se často zobrazují rovnou
- Techniky mohou využívat dříve uvedených možností

Zombie a DDoS

- Útočník spojí své síly s příznivcem barona Soboty
- A kdyby se to ukázalo jako nedostatečné
    - První krok se často neuskuteční a rovnou se začne druhým krokem

- Pomocí některé z technik propašuje malware, konkrétně trojského koně, do počítače oběti
- Takový počítač pak čeká na příkazy útočníka, aby je mohl provést
    - => Zombie

- V okamžiku, kdy je jeho armáda „záhrobníků“ dostatečně velká, začnou posílat požadavky na jeden konkrétní uzel
- Každý požadavek stojí něco paměti, přenosové kapacity a výpočetního výkonu – tzv. zdroje (resources)
- Pod dostatečně velkým útokem oběti dojdou zdroje a přestane poskytovat služby legitimním uživatelům
    - => Distributed Denial of Service alias DDoS

- Jelikož je ale náš hypotetický útočník „dobrák od kosti“, pošle např. provozovateli Internetového kasina slušný, anonymní e-mail, že určitý, vhodným způsobem doručený, finanční obnos by ho od jeho další činnosti odradil

- Kolik asi uživatelů má doma zombii, aniž by vůbec kdy tušili, že právě jejich počítač opakovaně podniká útoky vyšetřované policií?

Google Hacking

- Není nutné se hned nabourávat do nějakého počítače
- Google periodicky prochází všechny známé stránky a kompletně celý adresový prostor IPv4
- Stačí jenom vhodně zformulovat dotaz a zcela legálně odeslat
    - A jestli už stránku někdo odstranil?
        - Třeba bude ještě stále uložená někde v archívu

- Viz cvičení

Porno, celebrity, keygeny a další

- Pro řadu uživatelů je zcela zbytečné, aby útočník vymýšlel sofistikovaný způsob, jak se dostat do jejich počítačů,
    - Když stačí spustitelný soubor jenom vhodně pojmenovat

- Chcete skvělý software, jenže stojí peníze a tak vám bude stačit kradená kopie?
    - Na kterou potřebujete crack, nebo keygen
    - Co takhle poslat zfalšovaný e-mail od kamaráda, který ho má dodat, se souborem „acadkeygen.exe“?
    - Nebo poslat kamarádovi nevyžádaný e-mail s odkazem na warezový server, že to tam je a on vám sám pošle „důvěryhodný“ soubor?
        - Ostatně, na warezových serverech už takhle čeká celá řada trojských koňů na stažení
        - Ne, že by se vám někdo nedostal do počítače už jenom návštěvou takové stránky

- A co když např. kamarádovi, fandovi Hvězdné brány, přijde e-mail od kamaráda, taky fandy SGA, e-mail s videem pojmenovaným „JewelStaiteNudeOnBeach.avi“?
  - Nejspíš si ho rovnou otevře

- Anebo když kamarádce, fanynce StarTreku, přijde ve stejném duchu video „NakedSpock.mpg“?

- Řada uživatelů má tendenci otevírat a spouštět vhodně pojmenované soubory, i kdyby jim antivir a další obranné prvky desetkrát říkali, že to špatně dopadne

- Takové útoky kombinují technické možnosti spolu se sociálním inženýrstvím

- Když pošlete e-mail s textem

Dobrý den,

bohužel jsme opakovaně zaznamenali neoprávněný pokus o přístup k vaší e-mailové schránce. Z bezpečnostních důvodů jsme zablokovali funkce a ponechali jen ty základní. Prosíme o zaslání hesla k vaší autorizaci, abychom ji mohli opět uvést do normálního provozu.

S přátelským pozdravem,
Administrátor

- Najdou se tací, kteří heslo skutečně pošlou a nebudou nic zkoumat, ani se nepodívají na adresu, ze které e-mail přišel

- Případně lze použít následující variantu

Chcete získat přístup k libovolné e-mailové schránce na freemailu? Stačí, když mi pošlete vaše heslo spolu s e-mailovou adresou schránky, která vás zajímá.

Lord Helma

- Nicméně i tady se útočník bude muset někdy prokázat svou IP adresou

- Všechny uvedené útoky jsou pochopitelně protizákonné
- A až do této chvíle, a ať vypadaly jakkoliv hrozivě, proti nim existuje možnost technické realizace obrany

- Čerstvě aktualizovaný antivir, spyware blocker, firewall, povolené UAC (Vista), globální detekce spamu (zachytila by poslední adminův dopis), čerstvě aktualizovaný seznam podvodných webů, který využívá prohlížeč, atd.

- A hlavně bezhlavě neodklikávat různé dialogy

- Internet však umožňuje i nebezpečnější útok, který primárně není veden technickými prostředky
    - Technické prostředky nejsou použity k (jednoznačně?) protizákonné činnosti
        - Ale např. k tvorbě webové prezentace s diskusním fórem

    - A jsou pak vlastní techniky útoku vždy klasifikovatelné jako protizákonné?

- Tyto útoky jsou vedeny pouze technikami sociálního inženýrství, kterým webové prezentace poskytly nové možnosti
  - Zejména možnost potlačit cenzurou nepohodlnou opozici

- Nikdy bezhlavě nevěřte čemukoliv, co vám kdokoliv předkládá jako pravdu, i kdyby měl sebelepší prezentaci
  - Zjistíte-li, že šlo o útok, raději předpokládejte, že i další aktivity útočníka jsou stejného záměru

- Jelikož je ale Internet „dvojsečná zbraň“, jeho „druhé ostří“ vám dává šanci dohledat fakta k danému tvrzení
  - A dokonce i konkrétní techniku, kterou na vás zkusili použít, včetně jejího popisu a vysvětlení