Bevezetés a kiberbiztonságba és biztonságtudatosság

Böngészés az interneten

Szarvák Anikó

2023. Tavasz

Böngésző

- Mi látható a képen?
- Mit jelképez a lakat szimbólum?
- Milyen gyakran gépelünk el webcímeket?
- Mi történik, ha egy hivatkozás fölé visszük az egeret a webböngészőben?
- Mik azok a web sütik (cookie)?
  Érdemes reklámblokkolót használni? Miért?
- Érdemes privát böngészési módot használni? Miért?

Webcímek

Uniform Resource Locator (URLs):

- Példa URL: https://en.wikipedia.org/wiki/URL
- Az RFC 1738 definiálja
- „feltaláló”: a világháló atyja (Tim Berners-Lee)

Általános formátum:

- scheme:[//[user[:password]@]host[:port]][/path][?query] [#fragment]

A domain

TLD – Top Level Domain:

- “.hu”, “.com”

Restricted / korlátozott domainek:

- “.mil”, “.gov”

Domain:

- “uni-obuda.hu”

Aldomain:

- neptun.uni-obuda.hu

Webcímek formátuma

Séma szerinti web url:

http://user:pass@example.tld:8080

Milyen problémák vannak egy ilyen típusú használattal?

Protokollok

Szokásos protokollok:

- http
- https

“szokásostól eltérő” protokollok használata:

- ftp
- gopher
- Stb.

Weboldalak felépítése

A weboldalak tartalmát hierarchiába lehet rendezni:

https://neptun.uni-obuda.hu/hallgato/login.aspx

“/” után:

- Könyvtár struktúrát vagy logikai struktúrát írhat le
- Hivatkozhat fájlra, egyéb állományokra.

Speciális karakterek dinamikus oldalak esetén:

- pl.: “?”, “&“, “#”

“Escape” karakter és használata:

- ASCII – UNIcode
- “%20”

Hol van a HTTP?

OSI (Open Source Interconnection) 7 Layer Model

Layer	Application/Example		Central Device/ Protocols		DOD4 Model
Application (7) Serves as the window for users and application processes to access the network services.	**End User layer** Program that opens what was sent or creates what is to be sent Resource sharing • Remote file access • Remote printer access • Directory services • Network management		**User Applications** SMTP	GATEWAY Can be used on all layers	Process
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	**Syntax layer** encrypt & decrypt (if needed) Character code translation • Data conversion • Data compression • Data encryption • **Character Set Translation**		JPEG/ASCII EBDIC/TIFF/GIF PICT		
Session (5) Allows session establishment between processes running on different stations.	**Synch & send to ports** (logical ports) Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.		**Logical Ports** RPC/SQL/NFS NetBIOS names		
Transport (4) Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.	**TCP** Host to Host, Flow Control Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing	PACKET FILTERING	TCP/SPX/UDP		Host to Host
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	**Packets** ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting		**Routers** IP/IPX/ICMP		Internet
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	**Frames** ("envelopes", contains MAC address) [NIC card — Switch — NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control		**Switch Bridge WAP** PPP/SLIP	Land Based Layers	Network
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	**Physical structure** Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts		**Hub**		

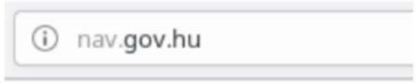
HTTPS

Az SSL/TLS legfontosabb szolgáltatásai:

- Felek azonosítása külső tanúsító szervezetek (Certifcate Authorities, CA) segítségével,
- Lehetőséget biztosít hibásan azonosított weboldalak automatikus tiltására – feltételezhető valamilyen rosszindulatú cselekmény,
- Adatok védelme erős titkosítás segítségével.

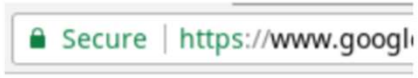
Tanúsítványok

- Nincs titkosítás

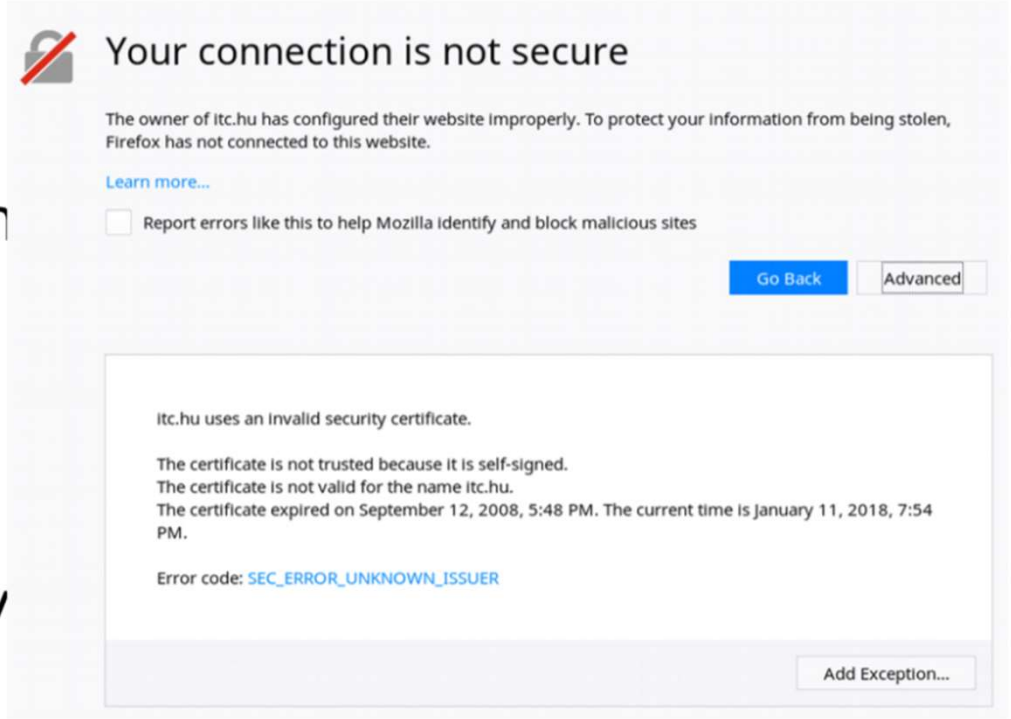


- Saját belső tanúsítván

- Domain tanúsítvány



- Kibővített tanúsítvány



Támadások

Adatgyűjtés tudatos hozzájárulás nélkül

Bizalmasság megsértése:

- Lehallgatás (snifng, wiretapping)
- Közbeékelődés (MitM)

Kérések eltérítése:

- Címhamisítás (DNS, DHCP, IP, ARP)
- Trükkös kódolás (URL kódolás, homoglyph támadás)

Támadások (folyt.)

Social engineering:

- Phishing (“A fiókod lejárt, újítsd meg itt”),
- Kattintásvadászat (“Sosem fogod kitalálni, hogy aztán mi történt…”),
- Rémisztgetés (“A számítógéped fertőzött, kattints a segítségért”).

Rendszer (böngésző) elleni támadások:

- Szkriptelés (CSRF, XSS),
- Puffer túlcsordulások, stb.

Támadások (folyt.)

A felhasználó megtévesztése kibővített unicode karakterek segítségével.

Például:

- http://google.com (vegyük észre a kis eltéréseket)

A valóság:

- http://g%u03BF%u043E%u0261%u217C%u0435.com
- http://xn--gl-jgb31l6qtb.com
- http://xn--g-s1a36hsnmb7023a.com

Zárókérdések

- Miért fontos a webes hivatkozásokat ellenőrizni a meglátogatásuk előtt?
- Hogy ellenőrizhetünk egy hivatkozást anélkül, hogy meglátogatnánk?
- Miért használjunk HTTPS protokollt azokon az oldalakon, ahol adatokat lehet rögzíteni?
- Ez a kereső űrlapokra is vonatkozik? Miért?
- Hogy győződhetünk meg arról, hogy valóban a bankunkkal kommunikálunk a weben?
- Mit jelent számunkra a domain birtoklás, vagy a kibővített tulajdonos ellenőrzés?