Практические аспекты сетевой безопасности

Уровень приложений

Протоколы уровня приложений

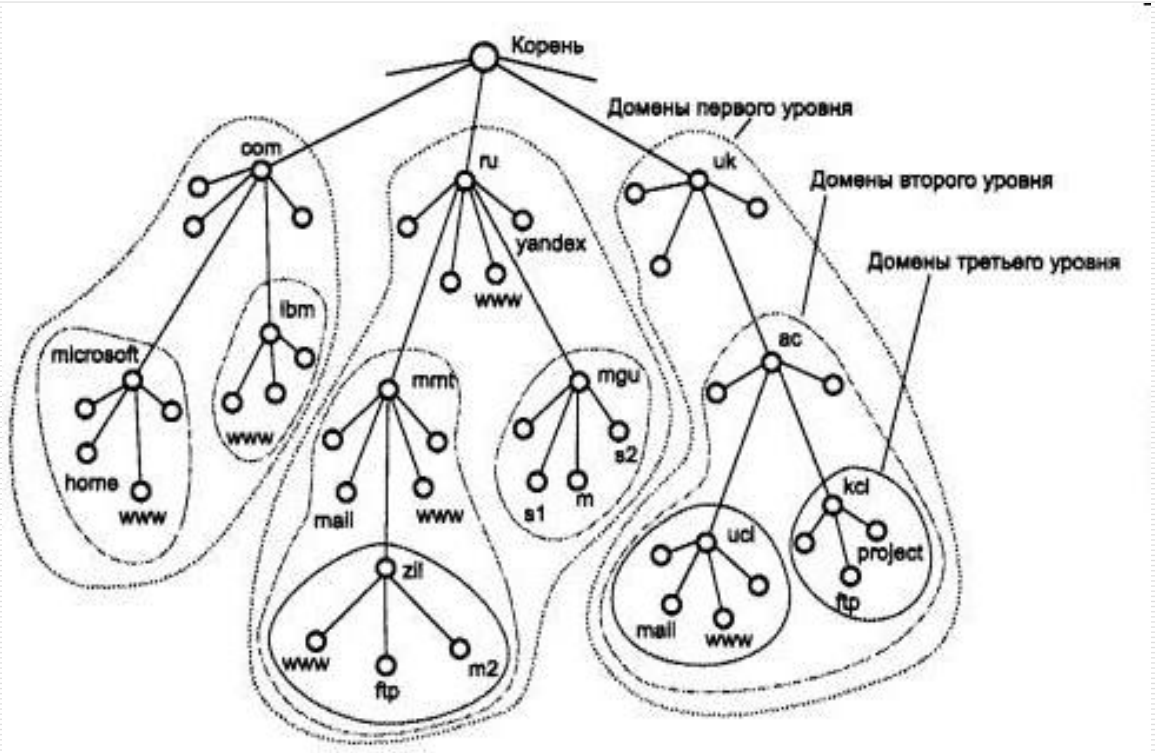
- Условно «сервисные»
  - DNS
  - Whois
- Условно «контентные»
  - HTTP
  - SMTP
  - P2P
    - Bittorrent
- ASCII
  - Telnet
  - HTTP
  - SMTP
- Бинарные
  - Corba

Domain Name System

- *DNS* – это распределенная база данных, поддерживающая иерархическую систему имен для идентификации узлов в Интернете
- Почтовый индекс vs IP адрес в сети
- Структура региональной системы имен

Доменные имена

- Глобальная иерархия имён



.com
.net .org
.co.uk
.org.uk
.us .eu
.biz .info
.me.uk .name
et al.

Доменные имена - 2

- lvk.cs.msu.su
- LVK.CS.MSU.SU
- Lvk.Cs.Msu.Su
- ...

lvk.cs.msu.su.

Формат базы DNS

Каждый домен описывают в виде множества ресурсов:

Domain_name Time_to_live Class Type Value

```
$ORIGIN .
$TTL 3600      ; 1 hour
cs.msu.su           IN SOA  ns.cs.msu.su. root.cs.msu.su. (
                            2010052274 ; serial
                            10800      ; refresh (3 hours)
                            1800       ; retry (30 minutes)
                            3600000    ; expire (5 weeks 6 days 16 hours)
                            3600       ; minimum (1 hour)
                            )
                    NS      ns.cs.msu.su.
                    NS      ns.radio-msu.net.
                    NS      ns1.radio-msu.net.
                    NS      ns2.radio-msu.net.
                    A       158.250.10.250
                    MX      10 mailhost.cs.msu.su.
                    MX      15 imap.cmc.msu.ru.
                    TXT     “BMK Zone"
$ORIGIN cs.msu.su.
academy             CNAME   educert.cmc.msu.ru.
adler               CNAME   farm
al                  A       212.192.248.21
                    MX      10 imap
$ORIGIN al.cs.msu.su.
www                 CNAME   al.cs.msu.su.
```

Резолвер

- Встроен в операционную систему
- UNIX/Linux:
  - /etc/nsswitch.conf

    ```
    ~> grep dns /etc/nsswitch.conf
    hosts:      files dns
    ```
  - /etc/resolv.conf

    ```
    ~> cat /etc/resolv.conf
    search lvknet lvk.cs.msu.su
    nameserver 158.250.17.1
    ```

Утилиты

- dig

```
~> dig mx lvk.cs.msu.su
; <<>> DiG 9.7.2-P3 <<>> mx lvk.cs.msu.su
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34349
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3

;; QUESTION SECTION:
;lvk.cs.msu.su.                 IN      MX

;; ANSWER SECTION:
lvk.cs.msu.su.          259200  IN      MX      10 mail.lvk.cs.msu.su.

;; AUTHORITY SECTION:
lvk.cs.msu.su.          259200  IN      NS      ns.cs.msu.su.
lvk.cs.msu.su.          259200  IN      NS      ns.lvk.cs.msu.su.

;; ADDITIONAL SECTION:
mail.lvk.cs.msu.su.     259200  IN      A       158.250.17.1
ns.cs.msu.su.           3160    IN      A       158.250.10.1
ns.lvk.cs.msu.su.       259200  IN      A       158.250.17.1
```

- host

```
~> host -t mx lvk.cs.msu.su
lvk.cs.msu.su mail is handled by 10 mail.lvk.cs.msu.su.
```

Атаки?

- DNS Cache Poisoning

  Запрос:

  www.yandex.ru. IN A

  Ответ:

  Answer:

  (no response)

  Authority section:

  attacker.ru. 3600 IN NS ns.yandex.ru.

  Additional section:

  ns.yandex.ru. IN A 4.4.4.4

Защита DNS

- Рандомизация номеров портов для запросов
- Дополнительная проверка полей ответа
- DNSSEC
  - В 2010 году реализован на корневых серверах DNS
  - В мае 2010 года криптоалгоритмы ГОСТ стандартизованы в IETF

Электронная почта

- Формат сообщений – RFC 822
- SMTP
  - TCP port 25
  - RFC 821
- IMAP4/POP3
- MIME

WWW

- Основа – протокол HTTP
  - Протокол без состояний
  - Использует «методы» - HEAD, GET, POST и т.д.
- Служебные протоколы для веб-приложений – WebDAV, SOAP, XMLRPC используют HTTP как транспорт
- Форматы данных – HTML, JSON, XML

XML/JSON

```
{
    "firstName": "Иван",
    "lastName": "Иванов",

    "address": {
        "streetAddress":
    "Московское ш., 101, кв.101",
        "city": "Ленинград",
        "postalCode": 101101
    },

    "phoneNumbers": [
        "812 123-1234",
        "916 123-4567" ]
}
```

```
<person>
  <firstName>Иван</firstName>
  <lastName>Иванов</lastName>
  <address>
     <streetAddress>Московское ш., 101,
     кв.101</streetAddress>
     <city>Ленинград</city>
     <postalCode>101101</postalCode>
   </address>
    <phoneNumbers>
       <phoneNumber>812 123-
     1234</phoneNumber>
       <phoneNumber>916 123-
     4567</phoneNumber>
   </phoneNumbers>
</person>
```

SSH

- Secure Shell
- SSHv2 – современная версия протокола