

ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА»
(СПбГУТ)

Факультет Инфокоммуникационных сетей и систем

Кафедра Защищенных систем связи

Лабораторная работа №1

Изучение протоколов сетевой аутентификации в сетях ОС Windows

Выполнили студенты группы ИКТЗ-83:

Громов А.А., Миколаени М.С.

(Ф.И.О., № группы)

(подпись)

Проверил:

Цветков А.Ю.

(уч. степень, уч. звание, Ф.И.О.)

(подпись)

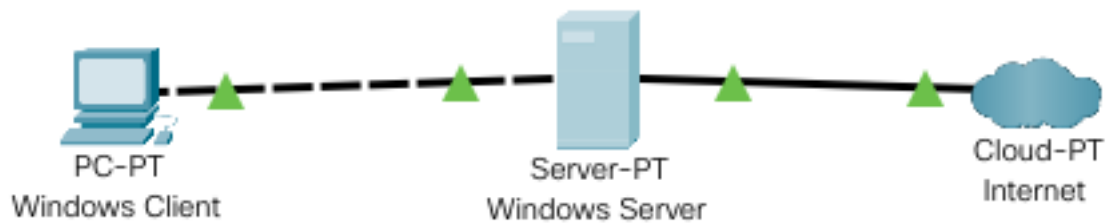
Санкт-Петербург

2020

Цель лабораторной работы:

1. Познакомиться с интерфейсом управления ролей Windows Server.
2. Познакомиться со структурой контроллера домена.
3. Изучить процесс аутентификации по протоколу NTLMv2 и Kerberos.

Схема сети:



Пункт 9:

[illegible]

Пункт 24:

AS-REQ:

The image shows a Wireshark capture of a Kerberos AS-REQ packet. The packet list shows a single packet of 292 bytes from 192.168.1.5 to 192.168.1.1. The packet details pane shows the following structure:

- Record Mark: 292 bytes
- as-req (5)
 - msg-type: krb-as-req (10)
 - padata: 2 items
 - PA-DATA PA-ENC-TIMESTAMP
 - padata-type: KRBS-PADATA-ENC-TIMESTAMP (2)
 - padata-value: 3041a003020112a23a043061ef427cbf3256e5dec2205e2f...
 - PA-DATA PA-PAC-REQUEST
 - padata-type: KRBS-PADATA-PA-PAC-REQUEST (128)
 - padata-value: 3005a0030101ff
 - include-pac: True
 - req-body
 - padding: 0
 - kdc-options: 40810010 (forwardable, renewable, canonicalize, renewable-ok)
 - cname
 - name-type: KRBS-NT-PRINCIPAL (1)
 - cname-string: 1 item
 - CNameString: User
 - realm: domain
 - sname
 - name-type: KRBS-NT-SRV-INST (2)
 - sname-string: 2 items
 - rttl: 2037-09-13 02:40:05 (UTC)
 - rttime: 2037-09-13 02:40:05 (UTC)
 - nonce: 1129186890
 - etype: 6 items

AS-REP:

The image shows a Wireshark capture of a Kerberos AS-REP packet. The packet list shows a single packet of 1573 bytes from 192.168.1.1 to 192.168.1.5. The packet details pane shows the following structure:

- Record Mark: 1515 bytes
- as-rep (5)
 - msg-type: krb-as-rep (11)
 - padata: 1 item
 - PA-DATA PA-ENCTYPE-INFO2
 - padata-type: KRBS-PADATA-ETYPE-INFO2 (19)
 - padata-value: 301b3019a003020112a1121b1044f4d41494e2e4c4f4341...
 - crealm: DOMAIN.LOCAL
 - cname
 - name-type: KRBS-NT-PRINCIPAL (1)
 - cname-string: 1 item
 - CNameString: User
 - ticket
 - tkl-vno: 5
 - realm: DOMAIN.LOCAL
 - sname
 - name-type: KRBS-NT-SRV-INST (2)
 - sname-string: 2 items
 - etype: ETYPE-AES256-CTS-HMAC-SHA1-96 (18)
 - kvno: 2
 - enc-part
 - cipher: 96e6edf82e9908eab4ed41fe5158b2ef1177be5640cb...

TGS-REQ:

The image shows a Wireshark capture of a TGS-REQ packet. The packet list on the left shows a sequence of packets: 310 (AS-REP), 319 (TGS-REQ), 321 (TGS-REP), and 329 (TGS-REQ). The selected packet 319 is expanded to show its structure. It is a Kerberos message of type 12 (TGS-REQ). The structure includes a padding field, a PA-DATA field (type 1), an ap-req field (type 14), a ticket field (type 1), and an authenticator field (type 18). The authenticator contains a cipher field (type 18) and a req-body field (type 0). The packet is captured on interface 0, source 192.168.1.1, and destination 192.168.1.5.

Frame 319: 1527 bytes on wire (12216 bits), 1527 bytes captured (12216 bits) on interface 0
Ethernet II, Src: VMware_a4:56:a4:12:63, Dst: VMware_a4:56:a4:12:63
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.5
Transmission Control Protocol, Src Port: 88, Dst Port: 49164, Seq: 1, Ack: 1532, Len: 1508
Kerberos
Record Mark: 1527 bytes
0... .. Reserved: Not set
0000 0000 0000 0000 0101 1111 0111 = Record Length: 1527
Type: 5
msg-type: krb-tgs-req (12)
padding: 1 item
padding-type: PA-DATA-TGS-REQ (1)
padding-value: 6e8204d8308204d4a003020105a10302010ea20703050000...
ap-req: 5
msg-type: krb-ap-req (14)
padding: 0
ap-options: 00000000
ticket: 1
real: DOMAIN.LOCAL
sname: krb5-NT-SRV-INST (2)
sname-string: 2 items
enc-part: 1
etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
kvno: 2
cipher: 96e0edfe2e9900eeab4e4d41fe5158bb2ef1177be5640cb...
authenticator: 1
etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
cipher: d1150c14fd10ed80ee94b7196afaf1b72a0b6da2e7aff4...
req-body: 0
padding: 0
kdc-options: 40010000 (forwardable, renewable, canonicalize)

TGS-REP:

The image shows a Wireshark capture of a TGS-REP packet. The packet list on the left shows a sequence of packets: 310 (AS-REP), 319 (TGS-REQ), 321 (TGS-REP), and 329 (TGS-REQ). The selected packet 321 is expanded to show its structure. It is a Kerberos message of type 13 (TGS-REP). The structure includes a padding field, a crealm field (type 1), a cname field (type 1), a ticket field (type 1), and an enc-part field (type 18). The enc-part contains a cipher field (type 18) and a req-body field (type 0). The packet is captured on interface 0, source 192.168.1.5, and destination 192.168.1.1.

Frame 321: 1562 bytes on wire (12496 bits), 1562 bytes captured (12496 bits) on interface 0
Ethernet II, Src: VMware_a4:56:a4:12:63, Dst: VMware_a4:56:a4:12:63
Internet Protocol Version 4, Src: 192.168.1.5, Dst: 192.168.1.1
Transmission Control Protocol, Src Port: 88, Dst Port: 49164, Seq: 1, Ack: 1532, Len: 1508
Kerberos
Record Mark: 1504 bytes
0... .. Reserved: Not set
0000 0000 0000 0000 0101 1110 0000 = Record Length: 1504
Type: 5
msg-type: krb-tgs-rep (13)
crealm: DOMAIN.LOCAL
cname: 1 item
cname-string: User
ticket: 1
real: DOMAIN.LOCAL
sname: krb5-NT-PRINCIPAL (1)
sname-string: 1 item
sname-string: User
enc-part: 1
etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
kvno: 3
cipher: 0a2224f877ae212c37ce5cc09ef355d603a04e3453090323e...
req-body: 0

Выводы

По итогам этой лабораторной работы, мы научились настраивать контрольный домен и давать защищенный доступ клиентам к серверу. С помощью программы Wireshark, мы разобрались в алгоритмах работы протоколов Kerberos и NTLMv2. На скриншотах данной программы видно, как компьютер-клиент безуспешно совершил 3 попытки отправки пакета аутентификации NTLMv2 со стандартными логин/паролем, прежде чем запросил у пользователя логин/пароль к серверу.