Education in Network Security
- Username Ryan
  - Research and Development Assistant at DePaul University
  - B.S Information Assurance & Security Engineering from DePaul University
  - Participated in over 25 security challenges over my collegiate career

Source: username Ryan password 70838435B040C1603100E1C162F3F3031313A3016031E1609
What is the most commonly used exterior routing protocol?

- BGP
- OSPG
- EIGRP
- RIP
show run | b NationalCyberLeague

- Jeopardy style CTF
- Categories include:
  - Log analysis
  - Reverse Engineering
  - Exploitation
  - Forensics
  - OSINT
  - Network Traffic Analysis

Source: http://www.nationalcyberleague.org/index.shtml
show int f0/2

Custom Protocol

The hackers have created their own custom protocol for private communication. Luckily, police officers have managed to obtain the documentation describing the protocol. Use it to fill out this report.

Overview

The communication between the client and server will contain three types of messages: Initialization, Encrypt Request, and Encrypt Response. A connection is started with the client sending an Initialization message, which contains the number of Encrypt Requests that the client wishes to make. Then, the server will send the length of its response. Then, the client sends their Encrypt Requests to the server. After all of the Encrypt Requests have been received, the server will finish sending a single Encrypt Response which contains hashes of all of the data that was sent by the client.

Initialization (Client -> Server)

1. N - A 4-byte integer in network byte order that represents the number of Encrypt Requests that will be sent.

Encrypt Request (Client -> Server)

1. Check - A fixed 2-byte integer in network byte order that verifies the integrity of the message.
2. Len - A 4-byte integer in network byte order that represents the length of the data in bytes.
3. Data - The data that will be encrypted.

Encrypt Response (Server -> Client)

1. Count - The length of the data, in bytes, that follows.
2. Hashes - The encrypted hashes requested by the client. Each hash is in the form of a fixed-length chunk. These hashes are in the same order that the requests were made.
Frame 5518: 72 bytes on wire (576 bits), 72 bytes captured (576 bits)

Internet Protocol, Src: 10.1.0.217 (10.1.0.217), Dst: 10.1.0.20 (10.1.0.20)
Transmission Control Protocol, Src Port: 42455 (42455), Dst Port: 60123 (60123), Seq: 1, Ack: 1, Len: 4

Destination port: 60123 (60123)

[Stream Index: 116]

Sequence number: 1 (relative sequence number)
[Next sequence number: 5 (relative sequence number)]
Acknowledgement number: 1 (relative ack number)
Header length: 32 bytes
Flags: 0x18 (Psh, Ack)
Window size: 29312 (scaled)
Checksum: 0x1519 [validation disabled]
Options: (12 bytes)
[IP/ICMP analysis]
[Timestamps]
Data (4 bytes)

Data: 00000005

[Length: 4]
show run | inc CCDC

- Collegiate Cyber Defense Competition
  - Red versus Blue
  - Strictly defensive
  - Teams of 8 students
  - Includes business injects

Source: http://www.nationalccdc.org/
show int e0/3

interface FastEthernet0/3
  description *** ADS Port ***
  switchport access vlan 999
  switchport trunk native vlan 999
  switchport trunk allowed vlan none
  switchport mode access
  switchport nonegotiate
  switchport port-security
  switchport port-security aging time 10
  switchport port-security aging type inactivity
  switchport port-security mac-address sticky
  ip access-group ip-device-list in
  shutdown
  mls qos cos override
  storm-control broadcast level 0.00
  storm-control multicast level 0.00
  storm-control unicast level 0.00
  no cdp enable
  spanning-tree portfast
  spanning-tree bpdufilter enable
  --More--
show int fa0/3

scheduler allocate 20000 1000
event manager applet config
  event cli pattern "show* (run*|star*|conf*)" sync yes
  action 1.0 cli command "show running-config | exclude ^snmp-server"
  action 2.0 puts "$_cli_result"
  action 3.0 set $_exit_status "0"
event manager applet flash
  event cli pattern "show* flash*" sync yes
  action 1.0 cli command "show flash: | exclude .tcl"
  action 2.0 puts "$_cli_result"
  action 3.0 set $_exit_status "0"
event manager applet users
  event cli pattern "show* users*" sync yes
  action 1.0 cli command "show users | exclude .vty"
  action 2.0 puts "$_cli_result"
  action 3.0 set $_exit_status "0"
event manager applet system
  event timer cron name system cron-entry "*/15 * * * *"
  action 1 cli command "enable"
  action 2 cli command "tclsh flash:sem.tcl"
!
end
show int g0/3

Firewall Configuration

- How do you defend against an enemy that has root access to your firewall???
delete flash:

- Twitter: @r_haley
- LinkedIn: linkedin.com/in/ryanhaley