2021 金盾獎初賽

R09921A10 鄭翔予
Team: AAAAAA

Review

It's my second time participating in this competition. The last time was two years ago when I was still a college student. This time there are only two members in our team, me and R10922056, which means each of us needs to memorize and research more in the realm of cyber security. Fortunately, the competition cancels the skills test and reserves only academic test, which consists of 80 multiple-choice questions, and thus having general concepts is enough for answering most questions. The main characteristic of this contest is that the partitioners cannot connect to the Internet.

The test covers 5 main subjects: Reverse, Web, Pwn, Crypto, and Misc, while it indicates that almost every security knowledge is covered, there are some common questions that have been asked over the past few years. More specifically, for Web, each kind of DDoS, OSI model, TCP/IP model, common protocols (HTTP(s), SSH, SSL/TLS), common protocol numbers, common port numbers, MITM, Wi-Fi, VPN, IPSec, and Firewall. For Crypto, common hash functions (MD5, SHA, RIPEMD), common cryptography algorithm (RC4, DES, AES, RSA, Elgamal, ECC, Rabin), common traditional cryptography (Caesar, Vigenere, Playfair, Rail fence, Enigma), common padding scheme (OAEP, PKCS#1, PKCS#7), Data integrity (MDC, MAC, HMAC), common digital signature (RSA, DSA, ECDSA), and operation mode. Others like Cloud computing, OS, SQL injection, and XSS are also popular questions. Moreover, knowing some security-related commands are useful such as nmap, iptables, attrib, net, etc.

At least half of the questions in this year are covered in the above mentioned topics. Although there isn't any skills test, such challenges are transformed into multiple-choice question. For example, it'll give you some information and multiple payloads as options and ask you which one can achieve the goal or it'll give you the situation and payload then ask what kind of attack it's performing. Additionally, many tools are mentioned and require knowledge of how and when to use them, including Wireshark, x64dbg/x32dbg, CFF explorer, etc. Surprisingly, there aren't many questions about security laws, which is criticized by contestants every year, this kind of questions should be taken care of in real-world but in my opinion, reciting these laws aren't suitable for competition that is network-disconnected, knowing which laws are suitable for which attacking scenarios are more important.

Problem Analysis

- WPA2
  - PSK (Personal) vs. Enterprise
    - PSK
      - The owner can set a PassPhrase as a password
      - All clients use the same wi-fi password
      - WPA2 will generate the Preshared Key (PSK) according to the client's input password
        - PSK is also known as Pairwise Master Key (PMK)
        - PMK = PBKDF2(PassPhrase, ssid, ssidLength, 4096, 256)
        - PSK is not used for encryption/decryption
      - Pairwise Transient Key (PTK) is the key that is used for encryption/decryption
        - PTK = PRF(PMK, AP_MAC, STA_MAC, SNonce, ANonce)
    - Enterprise
      - The authentication protocol is 802.1X
        - Enable authentication via username and password, or a security certificate
      - There exists an AAA server (RADIUS) that provides centralized authentication and user management
      - Station and AAA server can authenticate each other and exchange keys through Extensible Authentication Protocol (EAP). Then, the AAA server generates PMK from the Master Key and send it to AP
    - Main difference
      - WPA2-PSK uses a shared password
      - WPA2-Enterprise has an AAA server that is responsible for authentication and management, and every client has their own password
  - AES vs. TKIP
    - AES
      - A block cipher used by the protocol CCMP
    - TKIP
      - It uses the RC4 cipher
      - A wrapper rather than encryption
      - Increase the length of IV from 24 bits to 48 bits
      - Increase the key length to 128 bits

        - Each packet has a unique 48-bit serial number
        - Mixing a base key, the MAC address of an Access Point (AP), and a packet serial number
    - Main difference
        - AES is more seucre than TKIP
        - AES is faster than TKIP
- ssdeep
    - A program for computing context triggered piecewise hashes (CTPH)
        - Also known as fuzzy hashes
    - CTPH can match inputs that have homologies
        - Such inputs have sequences of identical bytes in the same order, although bytes in between these sequences may be different in both content and length
    - CTPH is based on using a rolling hash
        - The hash has a sliding window and a state
        - The state maintains the hash of the last few bytes of the data that are in the current window
        - The final CTPH consists of the saved parts (state) of the traditional hash
    - CTPH comparison
        - Compared by using Bloom filters and Hamming distance
        - Bloom filter
            - A space-efficient probabilistic data structure
            - It is used to test whether an element is a member of a set
        - Hamming distance
            - Gives a weighting value based on the difference of two strings
- Windows Event ID
    - Execution Related
        - 4688
            - A new process has been created
        - 4104
            - Execute a Remote Command
            - Powershell
        - 106
            - the user registered the Task Scheduler task
        - 200
            - This event is logged when the task Scheduler launched the action in the instance of the task

- Logon Related
  - 4648
    - A logon attempt was made with explicit credentials
  - 4624
    - Successful account log on
  - 4625
    - Failed account log on
  - 4771
    - Kerberos pre-authentication failed
    - Windows logs other instances of event ID 4768 when a computer in the domain needs to authenticate to the DC typically when a workstation boots up or a server restarts
  - 4768
    - Authentication ticket granted
- Account Related
  - 4720
    - A user account was created
  - 4732
    - A user was added to a privileged global group

- Access Control List (ACL)
  - ACL refers to the permissions attached to an object that specifies which users are granted access to that object and the operations it is allowed to perform
  - ACL is a list of access control entries (ACE)
  - Each ACE in an ACL identifies a trustee and specifies the access rights allowed, denied, or audited for that trustee
  - The security descriptor for a securable object can contain two types of ACLs: a DACL and a SACL
  - Discretionary Access Control List (DACL)
    - Identifies the trustees that are allowed or denied access to a securable object
  - System Access Control List (SACL)
    - Enables administrators to log attempts to access a secured object
- Conditional jump instructions
  - JZ, JE
    - Jump if zero, jump if equal
    - ZF = 1
  - JNZ, JNE

- Jump if Not Zero, Jump if Not Equal
- ZF = 0

- JC
  - Jump if Carry
  - CF = 1
- JNC
  - Jump if No Carry
  - CF = 0
- JO
  - Jump if Overflow
  - OF = 1
- JNO
  - Jump if No Overflow
  - OF = 0
- JS
  - Jump if Signed (Negative)
  - SF = 1
- JNS
  - Jump if Not Signed
  - SF = 0
- JP, JPE
  - Jump if Parity, Jump if Parity is Even
  - PF = 1
- JNP, JPO
  - Jump if Not Parity, Jump if Parity is Odd
  - PF = 0
- JCXZ
  - Jump if CX = 0
- JECXZ
  - Jump if ECX = 0
- JG, JNLE
  - Jump if Greater, Jump if Not Less or Equal
  - ZF = 0 and SF = OF
- JGE, JNL
  - Jump if Greater or Equal, Jump if Not Less
  - SF = OF
- JL, JNGE
  - Jump if Less, Jump if Not Greater or Equal

        - SF != OF
    - JLE, JNG
        - Jump if Less or Equal, Jump if Not Greater
        - ZF = 1 or SF != OF
    - JA, JNBE
        - Jump if Above, Jump if Not Below or Equal
        - ZF = 0 and CF = 0
    - JAE, JNB
        - Jump if Above or Equal, Jump if Not Below
        - CF = 0
    - JB, JNAE
        - Jump if Below, Jump if Not Above or Equal
        - CF = 1
    - JBE, JNA
        - Jump if Below or Equal, Jump if Not Above
        - ZF = 1 or CF = 1
- FTK Imager
    - It is a data preview and imaging tool used to acquire data (evidence) in a forensically sound manner by creating copies of data without making changes to the original evidence
    - File Slack
        - OS can only address clusters, rather than sectors which hard drives can, it means that files are stored on a hard drive in units of clusters and not sectors
        - Thus a file has two different sizes
            - Logical file size
                - The actual size of the file
            - Physical file size
                - The size that is given to the file on the hard drive
        - File slack is the difference between the physical file size and logical file size
        - It's essentially old fragments of unallocated file space
            - It can contain anything
- NXNS attack
    - Create a massive DDoS attack
    - A vulnerability in the DNS
    - The attack happens during the DNS delegation and makes DNS resolvers generate a massive number of queries to authoritative servers

- Steps
  - The attacker owns the domain *random.attack.com* and sends the request to resolve his own domain name to a DNS Resolver.
  - The DNS Resolver contacts the attacker's own authoritative name server
  - The attacker's authoritative name server responds with fake records like *fake.victim.com*
    - This leads to a record that doesn't contain any IP address
  - The Resolver must connect to the victim's authoritative name server for *victim.com* to search for the fake records on all *subdomains* and *victim.com*
    - As the records are fake the server will reply with an error message
- Evil Twin Attack
  - Attacker set up a fake Wi-Fi access point, which has similar or identical SSID and password settings, to eavesdrop on wireless communications
- Virus
  - Macro virus
    - Utilizes the software's macro ability to design virus
  - BootStrap Sector Virus
    - Infects and hides in the boot sector of floppy disks or the Master Boot Record (MBR) of hard disks
    - It can be loaded into memory before OS is loaded during bootup
  - Multipartite Virus
    - It has properties of both BootStrap Sector Virus and File Infector Virus
    - Thus it is highly infectious
  - Stealth Virus
    - Also known as Interrupt Interceptors
    - It controls DOS' interrupt vector to make DOS and antivirus programs think all files are clean
  - Polymorphic/Mutation Virus
    - It can create modified versions of itself to avoid detection yet remain the same basic routines after every infection
- Shoulder Surfing
  - A type of social engineering technique
  - An unauthorized third party can view a screen and any confidential data displayed on an electronic device
- .LNK

- The LNK file is a shortcut file used by Microsoft Windows and is often a direct link to an executable file
- It can be leveraged as a living off the land style attack
- LNK file can trick users into opening it, which then lead to executing commands and scripts or downloading other malicious files

- nmap
  - -iflist
    - List interfaces and routes
  - -e
    - Use specified interface
  - -S
    - Spoof source address
  - -D
    - Clock a scan with decoys
    - ME
      - One of the decoys represents the position of the real IP address
  - -g
    - Spoof source port number
  - --ttl
    - Set IP time-to-live field
  - --spoof-mac
    - Spoof MAC address
  - -A
    - Aggressive scan options
    - This option enables additional advanced and aggressive options
      - -O
        - OS detection
      - -sV
        - Version scanning
      - -sC
        - Script scanning
      - --traceroute
      - …
  - -sS
    - TCP SYN scan
    - Default setting
    - Quick
    - Relatively unobtrusive and stealthy since it never completes TCP

connections

- -sT
  - TCP connect scan
- -sU
  - UDP scans
- -sY
  - SCTP INIT scan
- -sN
  - TCP NULL scan
  - Does not set any bits (TCP flag header is 0)
- -sF
  - TCP FIN scan
  - Sets just the TCP FIN bit
- -sX
  - TCP Xmas scan
  - Sets the FIN, PSH, and URG flags
- -sA
  - TCP ACK scan
  - It is used to map out firewall rulesets, determining whether they are stateful or not and which ports are filtered
- --scanflags
  - Custom TCP scans
- -T
  - Set a timing template
  - There are six levels (0-5)
  - The higher the level is, the faster the speed of the scan is
    - But easier to be blocked by firewall and IDS