eJPT Certification

Section: Network Attacks

10/1/2020

Learning Objectives

* Attack remote authentication
* How to approach a remote windows machine
* ARP spoofing and network layer 2 attacks

Types of Attacks

* Authentication cracking, window shares, null sessions, ARP poisoning, Metasploit, meterpreter.

**Authentication Cracking**

* Prue brute force attacks over network is impractical because of the time needed to run each probe.
* During a network authentication attack there are several factors involved:
  + Network latency- the time needed to transmit data from the pentesters machine to the target server and vice versa.
  + Delays on attacked service- some services wait some seconds during authentication routines with the scope of making authentication attacks slower.
  + Processing time on the attacked server- The target server must encrypt and check the credentials.
* Authentication cracking relies almost entirely on dictionary -based attacks.

**Authentication Cracking Tools**

* Hydra: fast, parallelized, network authentication cracker that supports different protocols.
  + Can attacks nearly 50 different service types, including:
    - Cisco auth
    - FTP
    - HTTP
    - IMAP
    - RDP
    - SMB
    - SSH
    - Telent

**Window Shares**

* Window Shares can be used on clients and server to provide authentication, file sharing, printer management and other features.
* **NetBIOS (Network Basic Input Output System)**
  + Used by servers and clients when viewing network shares on the LAN
  + NetBIOS supplys information about the computer’s hostname, NetBIOS name, Domain, Network Shares.
  + The NetBIOS layer sits between the application layer and the IP layer

**Diagram

Description automatically generated**

* **UDP** is used to perform NetBIOS name resolution and to carry other one-to-many datagram-based communications.
  + by using NetBIOS datagrams, a host can send small messages to many other hosts.
* For heavy data traffic such as a file copy, NetBIOS will use TCP by using NetBIOS Sessions
* Ports:
  + TCP port 139- NetBIOS sessions
  + UDP port 138- NetBIOS datagrams
  + UDP port 137- NetBIOS names
* When a window machine browses a network, it uses NetBIOS:
  + Datagrams is used to list the shares and the machines.
  + Names to find workgroups
  + Sessions to transmit data to and from a windows share.

**Shares**

* Shares allow windows machine users to share resources on a local area network. This also includes remote users.
* Shares can be extremely useful for the obvious: enables greater work efficiency by allowing workers to share resources such as files, documents, printers, etc., but can also be very dangerous.
  + If a network shares is misconfigured it can be a great threat.
* Generally speaking, it’s quite easy to create a network share in a Windows environment. All the user typically needs to do is turn on the *file and printer sharing service* and then they can start choosing directories or files to share.
  + Users can set permissions on a share, choosing who can perform operations such as reading, writing and modifying permissions.
* Shares in Windows Vista
  + Users can choose to share a single file or use a Public directory. When sharing a single file, they can choose local or remote users to share the file.
  + Using Publics directories, they can choose which users can access the files on the share, but they can only allow everyone or no one in the network to access the share.
* Authorized users can access shares by using Universal Naming Convention paths (UNC paths)



* Administrative Shares
* There are default administrative shares which are used by system admins and windows itself:
  + [**\\ComputerName\C$**](file://ComputerName/C$)lets an admin access a volume on the local machine. Every volume has a share (C$, D$, E$, etc.)
  + [**\\ComputerName\admin$**](file://ComputerName/admin$)points to the windows installation directory
  + [**\\Computername\ipc$**](file://Computername/ipc$)is used for inter-process communication. You cannot browse it via Windows Explorer.
* Badly Configured Shares
  + Accessing a share means having access to the resources of the computer hosting it. So, badly configured shares exploitation can lead to:
    - Information disclosure
    - unauthorized file access
    - Information leakage used to mount a targeted attack.

**Null Sessions**

* Null session attacks can be used to steal information about passwords, system users, system groups, and running system processes.
* Null sessions are remotely exploitable; this means that attackers can use their computers to attack a vulnerable windows machine.
  + Can call remote APIs and remote procedure calls.
* **NOTE- windows is configured to be immune from this kind of attack. However, legacy hosts can still be vulnerable.**
* Null session attacks exploit an authentication vulnerability for Windows Admin Shares; this lets an attacker connect to a local or remote share without authentication.
* **Enumerating Windows Shares** 
  + **Nbtstat is for windows**
  + In windows, the most common command to use when enumerating windows shares is *nbtstat*.
    - *NbtStat*

***Text

Description automatically generated***

* The most common command is “nbtstat -A <IP address>”
  + This displays information about the target.

**Nmblookup**

* You can also perform window Shares enumeration from Linux using the Samba Suite.
* To perform the same operations of nbtstat, you can use nmblookup with the same command line switch:

****

You can look up the manual for help:

Graphical user interface, text, application

Description automatically generated

* Smbclient
  + Smbclient is an FTP-like client to access Windows shares; this tool can, among other things, enumerate the shares provided by a host:

Graphical user interface, text, application

Description automatically generated

Here is a breakdown of the following commands from the prevous screen screenshot

Graphical user interface, text

Description automatically generated

Now we are going to analyze the results shown in the first screen shot on the previous page:

* Shows us admin shares that are hidden when using Windows standard tools (nbtstat)

Table

Description automatically generated

**Exploiting Null Sessions with Enum**

* A command line utility that can retrieve information from a system vulnerable to null sessions attacks.
* The *– S* parameter lets you enumerate the shares of machine. For example:

**Text

Description automatically generated**

* -U enumerates the users:

**Graphical user interface, text

Description automatically generated**

* To get information on password policies you can use the -P parameter:

**Graphical user interface, text, application

Description automatically generated**

* Gathering information on password policies helps build strong password authentication attacks:
  + Prevent accounts locking
  + Prevent false positives
  + Choose your dictionary or your bruteforce configuration.
* **Exploiting Null Sessions with Winfo**
  + Another command line utility that can be used to automate null session exploitation.
  + To use it you have to use the -n command to tell the tool to use null sessions.



* Winfo command line tool can be download from [packetstorm](https://packetstormsecurity.com/search/?q=winfo&s=files)
* Exploiting Null Sessions with Enum4Linux
  + Enum4linux is a PERL script that can perform the same operations as enum and Winfo.
    - Uses the same command line options as enum, but has additional options.
  + By default, it performs:
    - User enumeration
    - Share enumeration
    - Group and member enumeration
    - Password policy extraction
    - OS information detection
    - A nmblookup run
    - Printer information extraction
* You can get a list of enum4linux options by typing into the command line *enum4linux.*

Graphical user interface, text, application

Description automatically generated

**ARP Poisoning**