positive hack camp

pt

Network reconnaissance and compromise of Windows machines

positive education

CyberED

Set up for class

In today's class, we're moving on to the last major phase: Attacking on the company's local area network

As part of this phase, we will familiarize ourselves the following topics:

- Network reconnaissance and compromise of Windows machines
- Privilege escalation on Windows machines
- Capturing a domain controller

Lesson plan

- Search for Windows machines on the local network
- Primary access attacks on Windows machines:
  - Exploits (MS17-010, MSSQL, Samba (cve-2017-7494))
  - Brute-force attacks and password spraying
  - Traffic interception and MiTM attacks on Windows machines (NTLM / NetNTLM hash capture, SMB Relay)
- Horizontal movement (PassTheHash attack)

positive hack camp

pt

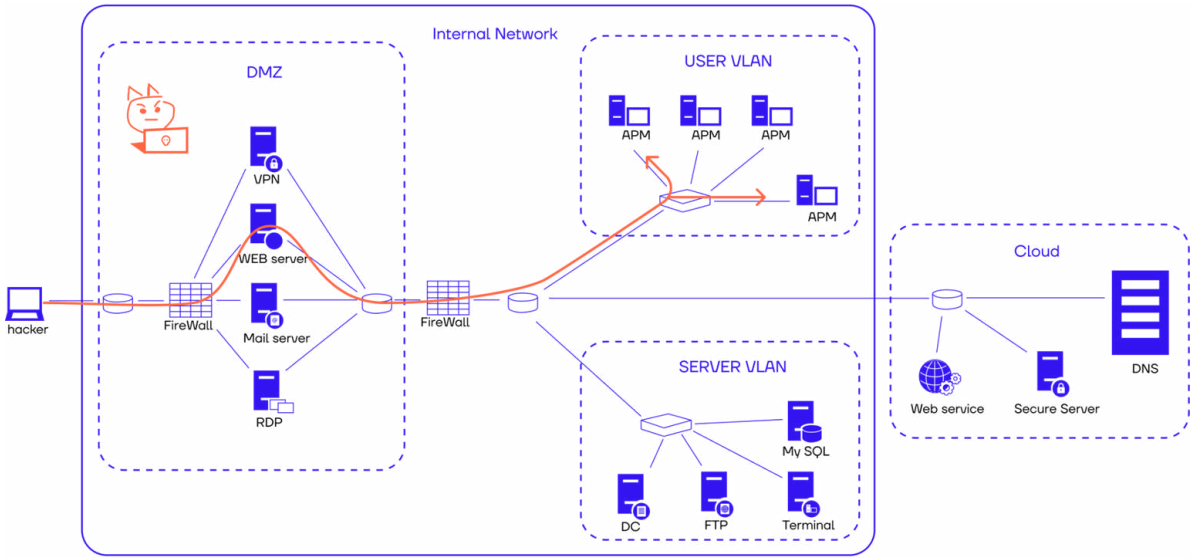
In this class, you will:

- Familiarize yourself with the weaknesses of Windows machines on your network
- You'll learn about popular attacks on Windows machines
- Learn how to search for Windows machines on a local network

positive education

CyberED

Our network position



Basic Concepts

Man-in-the-middle attack

MITM- a type of computer security attack in which an attacker covertly relays and, if necessary, alters communication between two parties who believe they are communicating directly with each other.

NBT (NetBIOS over TCP/IP)

Legacy protocol, disabled in Win11 22H2+, that is used for mapping NetBIOS requests to TCP/IP.

NetBIOS Name Service (NBT-NS)

Windows protocol that is used to translate NetBIOS names to IP addresses on a local network.

LLMNR, Link-Local Multicast Name Resolution

A TCP/IP stack protocol, based on the DNS data packet format, that allows computers to perform host name resolution on a local network.

MS17-010

A security update that addresses vulnerabilities in Microsoft Windows. The most serious of the vulnerabilities could allow remote code execution if an attacker sends specially crafted messages to a Microsoft Server Message Block 1.0 (SMBv1) server.

Search for Windows machines on the local network

We have already learned about the various aspects of scanning the local network and external network scanning. Let's reiterate the important one:

- You should scan the network, starting by looking for nodes.
- Once the nodes are discovered, you can get busy scanning the services on them.
- You should only look for services that you know what to do with.

positive hack camp

pt

When you have discovered existing hosts on the network and you want to identify Windows hosts among them, you shouLd start with:

→ Scanning ports belonging to Windows machines

→ Examining the traffic of broadcast requests that initiate Windows machines

positive education

CyberED

Scanning ports belonging to Windows machines

Services belonging to Windows machines that can assist in targeting or compromising a system:

88 - kerberos
(Kerberos Key Distribution Center)

The presence of this port helps to identify the domain controller on the network

135 - MSRPC (Microsoft RPC[6])

is used in Microsoft client-server applications (e.g. Exchange), allows you to perform various OS operations when credentials are available

137 - NETBIOS-NS
(NetBIOS Name Service)

allows you to find out the domain name of the machine and its MAC address

389 - LDAP
(Lightweight Directory Access Protocol)

This port can provide various opportunities for both credential selection, and to gain access to LDAP through exploitation of vulnerabilities (Example)

Scanning ports belonging to Windows machines

445 - SMB
(Server Message Blocks over IP)

The SMB protocol has a number of vulnerabilities and flaws in various versions, that can lead to code execution, user session hijacking, accessing data on file servers.

1433 - MSSQL (Microsoft SQL Server)

The MSSQL service allows us to access database management and, more importantly, execute arbitrary code on a Windows machine if we have an account to access the database.

3389 - RDP
(Remote Desktop Protocol)

The remote desktop service also had a history of various vulnerabilities BlueKeep and is susceptible to MiTM attacks that allow access to the service on behalf of the victim.

In fact, there are many more public services

positive hack camp

pt

consoLe command

```
nmap -Pn -n -sT -p 88,135,137,389,445,1433,3389 -sV -sC --open -iL list-of-machines.txt
```

positive education

CyberED

Examining the traffic of broadcast requests that initiate Windows machines

Windows machines are actively using WPAD, LLMNR, NBT-NS protocols, which allow us to determine that it is highly likely that Windows machines have used this protocol.

→ Web Proxy Auto-Discovery Protocol (WPAD) is a method used by clients to determine whether a Web proxy

Proxy Auto-Discovery Protocol (WPAD) is a method used by clients to determine the location (URL) of a configuration file using DHCP and/or DNS technologies.

→ NetBIOS Name Service (NBT-NS) is a Windows protocol that is used to translate NetBIOS names to IP addresses on a local network.

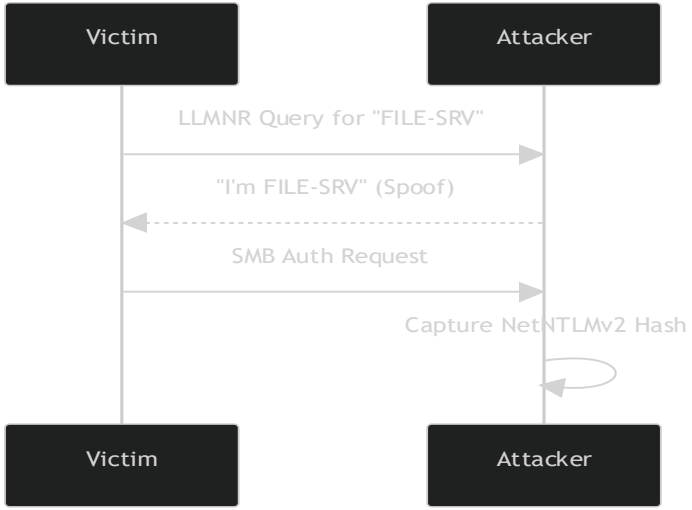
→ Link-Local Multicast Name Resolution (LLMNR)

A TCP/IP stack protocol based on the DNS data packet format that allows computers to perform host name resolution on a local network.

Examining the traffic of broadcast requests that initiate Windows machines

Protocol	Purpose	Port	Attack Method
WPAD	Automatic proxy config discovery via DHCP/DNS	80/HTTP	Spoof wpad.dat → Credential theft
LLMNR	Hostname resolution when DNS fails	5355/UDP	Poisoning → NetNTLMv2 hash capture
NBT-NS	NetBIOS name → IP resolution	137/UDP	Spoofing → SMB relay attacks

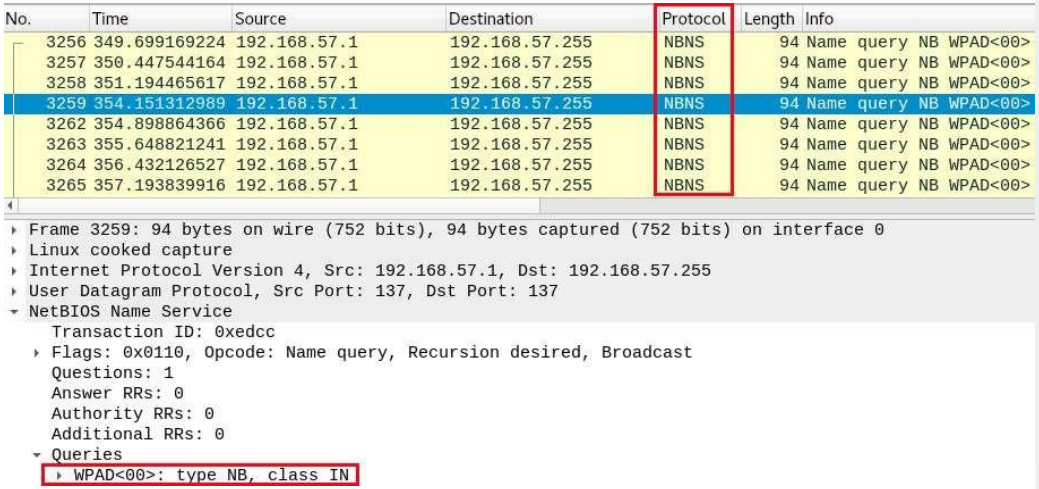
Examining the traffic of broadcast requests that initiate Windows machines



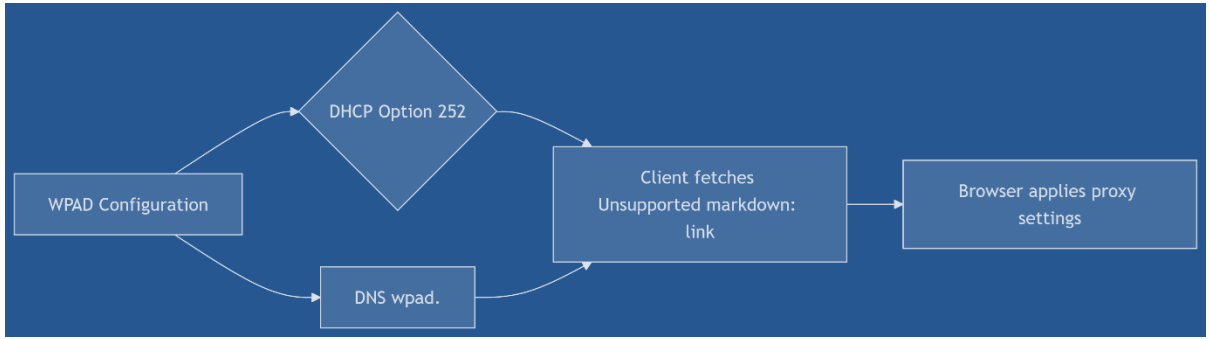
Broadcast requests NBNS, LLMNR on the example of work with Web Proxy Auto-Discovery Protocol

The WPAD protocol is needed to automatically configure all browsers in an organization without manually configuring each one.

The WPAD-standard describes two alternative methods of disseminating information configuration file location information to system administrators using the Dynamic Host Configuration Protocol (DHCP) or Domain Name System (DNS).



Broadcast requests NBNS, LLMNR on the example of work with Web Proxy Auto-Discovery Protocol



When DNS/DHCP misconfigured, clients broadcast LLMNR/NBNS requests for WPAD host → poisonable.

Broadcast requests NBNS, LLMNR on the example of work with Web Proxy Auto-Discovery Protocol

For autoconfiguration, the client attempts to discover a URL with a configuration file location pointing to a Proxy server

Before the first page is loaded, a browser on a Windows machine uses this technology to send a DHCPINFORM request to the local DHCP server and uses the resulting URL from the server's WPAD response option. If the DHCP server cannot provide the required information, DNS is used. If, for example, the computer's DNS name is pc-hostname.subname.local-domain-name.ru, the browser will attempt to refer to the following URLs to find the configuration file:

- wpad.subname.local-domain-name.ru/wpad.dat
- wpad.local-domain-name.ru/wpad.dat
- wpad.com/wpad.dat

Problems

Since some name does not really exist on the network, the client performs a DNS name lookup through the following steps:

- Checks the "hosts" file for system and configuration information
- Checks the local DNS cache
- Sends a request to DNS
- Sends LLMNR request
- Sends a request to NBT-NS
- Sends an MDNS request

If we can let the client know that the wpad.dat file is in our we can try to ask the client for authentication credentials, or we can give the client proxy settings with their host address and listen to all traffic that goes through our proxy server.

Conclusions

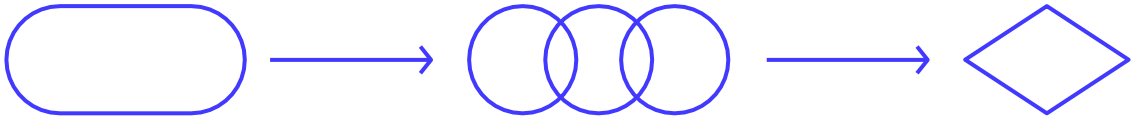
To search for Windows machines we can:

→ Scan the local network with the command:

```
nmap -Pn -n -sT -p 88,135,137,389,445,1433,3389 -sV -sC
--open -iL list-of-machines.txt
```

→ Examine traffic using Wireshark and a filter:

```
nbns && llmnr && mdns
```



Primary access attacks on Windows machines

Primary access attacks on Windows machines can be attempted once they are detected and utilize the following attack methods:

- Applying exploits to known vulnerabilities in Windows machines
- Using brute force attacks
- Traffic interception and MiTM attacks
- Let's look at the possibility of applying these methods in order

Use of exploits

We are already familiar with the ability to detect vulnerable software versions and apply exploits to them. Let's talk about typical vulnerabilities and exploits for Windows machines.

The most common vulnerabilities
Windows machines at different times were:

- CVE-2008-4250 (MS08-067)
- CVE-2017-0143 (MS17-010)
- CVE- 2019-0708 (BlueKeep).

More complete list

MS08-067

ms08_067_netapi is one of the most popular remote exploits against Microsoft Windows.
It is considered a trusted exploit and allows access as SYSTEM - Windows' highest privilege.
In modern penetration tests, this exploit is most likely to be used in an internal environment
and not as often in an external environment due to the likelihood of a firewall.

This exploit works against a vulnerable SMB service for the following Windows systems:

- Windows 2000
- Windows XP
- Windows 2003

Exploit:

Metasploit > exploits/windows/smb/msmb08_067_netapi

MS17-010

ms17_010_eternalblue is a remote exploit against Microsoft Windows, originally written by the Equation Group (NSA) and disclosed by Shadow Brokers (an unknown hacker organization). It is considered a robust exploit and allows access not only as SYSTEM, the highest privilege of Windows user mode, but also full control of the kernel in ring 0.

As far as remote kernel exploits go, this one is very reliable and safe to use.

The verification command is also very accurate, as Microsoft's patch inadvertently added disclosure with additional checks for vulnerable code paths.

This exploit works against a vulnerable SMB service for the following Windows systems:

- Windows XP x86 (All Service Packs)
- Windows 2003 x86 (All Service Packs)
- Windows 7 x86 (All Service Packs)
- Windows 7 x64 (All Service Packs)
- Windows 2008 R2 x64 (All Service Packs)
- Windows 8.1 x64
- Windows Server 2012 R2 x64
- Windows 10 Pro x64 (< Version 1507)
- Windows 10 Enterprise Evaluation x64 (< Version 1507)

Exploit:

Metasploit > exploit/windows/smb/ms17_010_eternalblue

BlueKeep

A BlueKeep vulnerability was discovered in the implementation of the RDP protocol in some versions of the Windows operating systems in May 2019. BlueKeep has nothing to do with the protocol mechanism itself and only affects its implementation. In particular, the vulnerability affects a part of the code, The vulnerability affects the part of the code responsible for managing so-called virtual channels.

The vulnerability currently targets the following Windows systems:

- Windows 10
- Windows 7
- Windows 8.1
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

Exploit:

Metasploit > exploit/windows/rdp/cve_2019_0708_bluekeep_rce

positive hack camp

pt

Brute-force attacks

Brute force attacks are just as effective at attacking Windows machines. Why?

Each Windows machine has seveRaL protocoLs to impLement attacks on authentication mechanisms

A little understanding of what credentials and passwords to use for such attacks in a particular context can make this method much easier and extremely effective.

positive education

CyberED

positive hack camp

pt

What can be attacked in Windows

SMB | MSSQL | LDAP | RDP

Example of an attack:

```
hydra -L ~/wordlists/user.txt -P
~/wordlists/pass.txt 192.168.1.5 smb -V
```

positive education

CyberED

positive hack camp

pt

Preparation

- Before you can launch an attack by brute force, you need to answer the following questions:
- Is it possible to find out the logins for users in the domain?
- What kind of passwords do you use to use to find them?
- How do you not block users in a domain?

positive education

CyberED

positive hack camp

pt

Dictionary of logins

A dictionary of logins from a domain can be obtained either from the reconnaissance phase, from external systems.

from external systems (mail)
or by compromising a machine/account
(retrieve mail address book \ access LDAP)

Password dictionary

A dictionary of passwords can be prepared knowing the habits and mentality of the company's employees. The most popular passwords are: Winter2025, March2025, Company2025 and so on. I.e. using combinations of year, month, company name etc.

* Dictionaries should be chosen according to the context in which you use them.

positive education

CyberED

Bypassing blocking

To bypass the lockout, you can use Password Spraying attack, i.e. 1 attempt at password mining for all accounts on the list in a certain period of time.

The peculiarity of customizing Windows systems is that, is that administrators often customize policy of the number of password attempts.

Usually, the number of attempts in this policy is set from 3 to 10 times per hour. If the number of attempts is exceeded, the user's account is locked.

Traffic interception and MiTM attacks on Windows machines

Another feature of Windows machines is that they use LAN communication protocols by default, through which you can try to compromise the communication channels and gain access to session or data management.

We've talked before about the Windows machine running the algorithm for name resolution on the local network. Let's do it again:

Every time a Windows machine attempts to perform a domain name resolution domain name resolution, it performs the following actions:

- Checks the "hosts" file for system and configuration information
- Checks the local DNS cache
- Sends a query to DNS
- Sends LLMNR request
- Sends a request to NBT-NS
- Sends an MDNS request

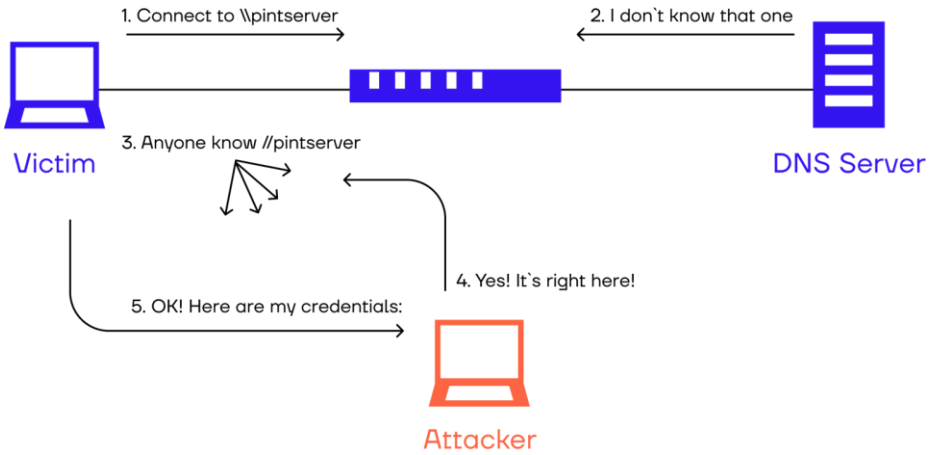
Traffic interception and MiTM attacks on Windows machines

And just when LLMNR, NBT-NS and MDNS protocols are being used, it becomes possible to spoof the response to such a request and attempt to lead the victim to its malicious resource, which will be able to: direct the victim to an authentication service and steal hash of the account password (and subsequently the password itself), conduct a Relay (session hijacking) attack, execute commands on behalf of the victim in the machine where the victim has been authenticated, etc.

This attack is called LLMNR / NBT-NS / MDNS Spoofing

How does NBT-NS and LLMNR Spoofing work?

The moment an LLMNR/NBT-NS request is received, an attacker can spoof the real source of name resolution in the victim's network by responding to traffic as if it knows the identity of the requested host, poisoning the service so that victims communicate with a system controlled by the attacker.



How does NBT-NS and LLMNR Spoofing?

- If the host to which the victim will be redirected victim will require an identification/authentication process, then the username and NTLMv2 hash will already be sent to the system controlled by the attacker. to a system controlled by the attacker.
- The adversary can then gather hash information using traffic-tracking tools and crack the hashes offline using a brute force method brute force to obtain the passwords in plaintext.
- To conduct such an attack, you can tools such as: NBNSpoof, Metasploit and Responder.

Responder

Let's take a closer look at performing an LLMNR/NBT-NS/MDNS Spoofing attack using Responder. Tool Reference.

Responder is a tool for performing a MiTM attack against Windows authentication methods. This program uses LLMNR, NBT-NS and MDNS poisoning through which it redirects traffic with authentication requests and hashes to a subordinate host.

The program also has built-in HTTP/SMB/MSSQL/FTP/LDAP authentication servers that support such authentication methods as NTLMv1/NTLMv2/LMv2, Extended Security NTLMSSP and basic HTTP authentication, for which Responder acts as a relay.

Responder

Let's use this tool to steal the victim's password hash and then recover her account password.

→ Let's run Responder:

```
sudo responder -I eth0
```

→ Having captured the NTLMv2 hashes, let's put them in the tickets.txt file and try recover the passwords of the accounts that sent us the hashes:

```
hashcat -a 0 -w 4 -m 5600 tickets.txt
/usr/share/wordlists/rockyou.txt
```

→ After obtaining the password, we will use the evil-winrm utility to get convenient access to the terminal shell of the server:

```
evil-winrm -i [ip] -u [username] -p [password]
```

Conclusions

We looked at how to probe the local network for Windows machines Windows machines and how to conduct initial attacks against Windows machines.

Let's summarize:

- Windows machines are quite visible on the LAN because of their behavior (use of multicast and broadcast requests), and because they use specific services located on ports published by the machines.
- Also, Windows machines in their default configuration can be vulnerable to many different attacks such as brute force attacks, man-in-the-middle attacks, and exploits to known vulnerabilities.

Supplementary materials

- Memo on MITM attacks
- Telegram channel of Magama Bazarov,
  an expert on network attacks
- Responder
- All about authentication attacks on Windows
- How the NTLM Relay attack works