

# BadTunnel: How Do I Get Big Brother Power ?

Yang Yu @ Tencent's Xuanwu Lab

# Who am I?

Yang Yu, @tombkeeper

- From Beijing, China
- Director of Tencent's Xuanwu Lab
- The guy who make the most money from Microsoft Bounty Programs 😊
- Working in information security industry since 2002

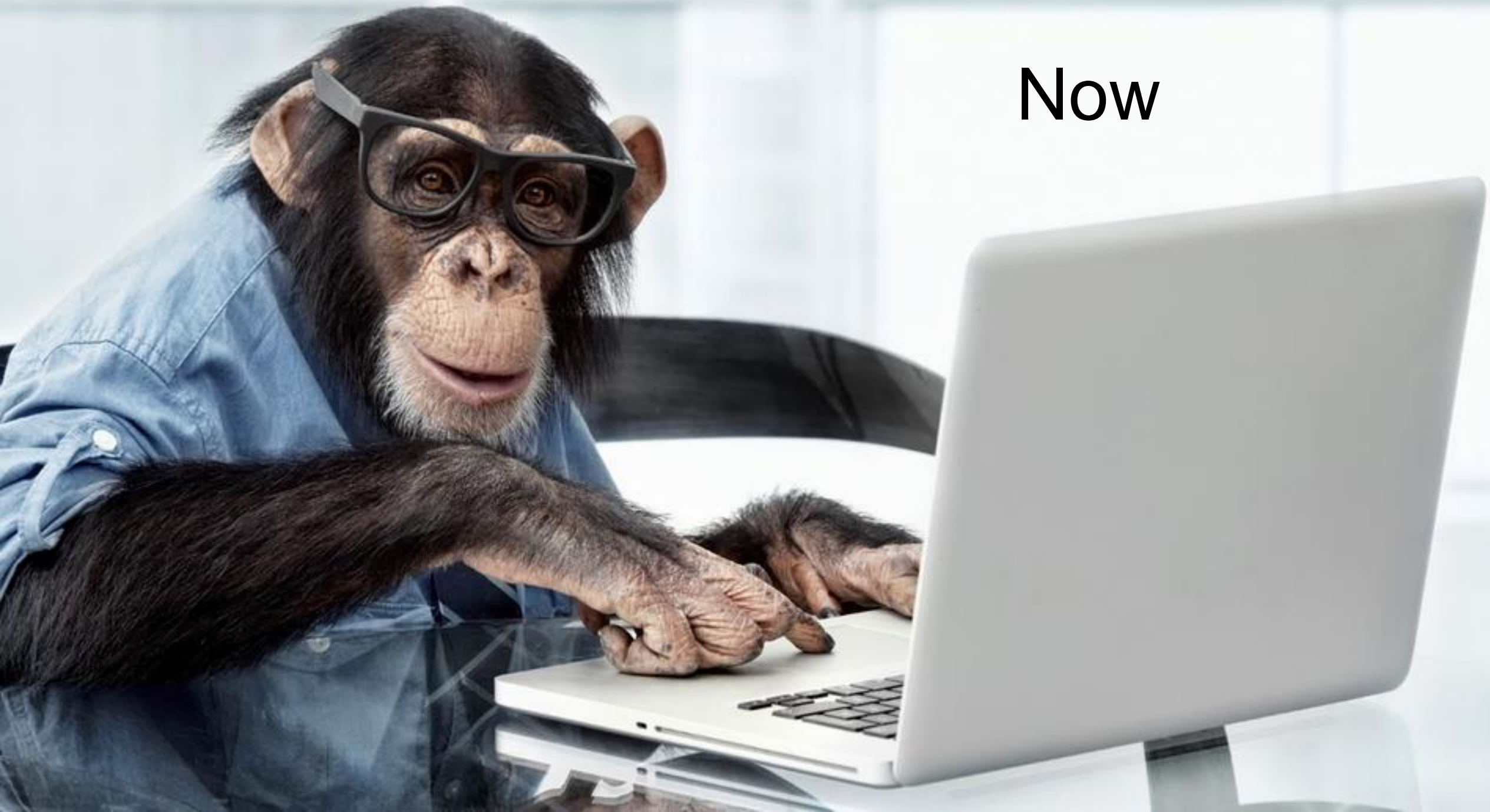


# Before 2002





# Now



# Agenda

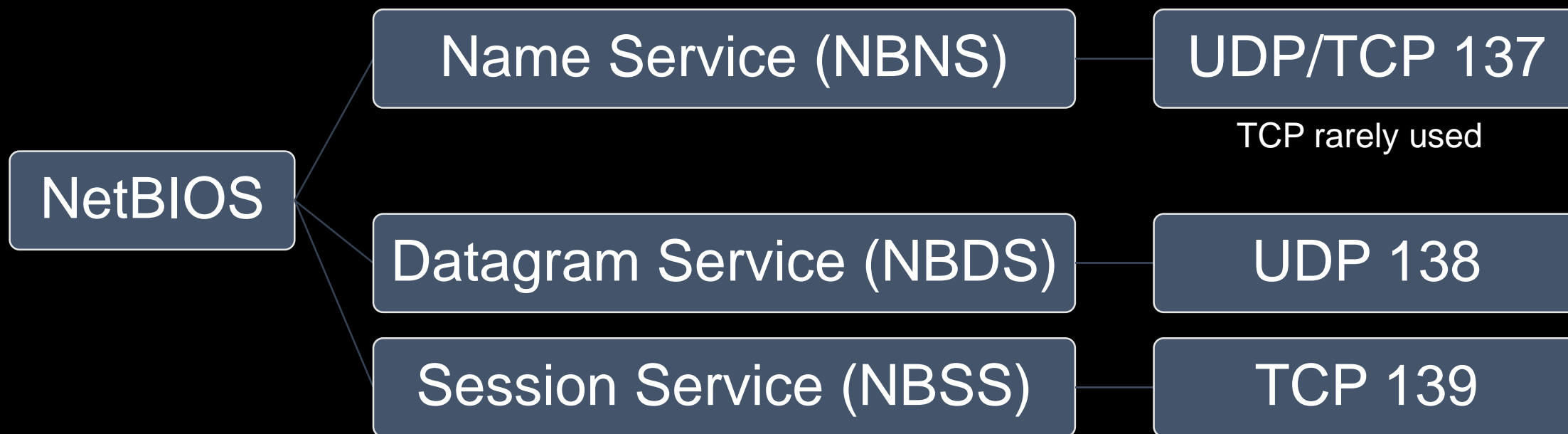
- Background knowledge
- How to create a BadTunnel
- What BadTunnel could do
- How to defend against BadTunnel attacks



# Background Knowledge



# Ancient NetBIOS Protocol



How ancient is NetBIOS? If you study on the research history of NetBIOS security, your will see the name *Cult of the Dead Cow*.

# NetBIOS Name Service (NBNS)

- NBNS provides a name resolution service, like DNS
- The packet formats of the NBNS are identical to DNS
  - “DNS running on port 137”
- Transaction ID of NBNS is **not** random but incremental
- NBNS use UDP packets sent **from and to** port 137
- The security of DNS protocol is completely dependent on the randomness of source port and Transaction ID. But NBNS abandoned this in design
  - However, this is understandable, considering NBNS is designed for exclusive use in the local area network. Name resolving is done using UDP broadcast, which can be received by all hosts in the same network. So it seems unnecessary to randomize the source port and Transaction ID.



# Two Types of NBNS Query

- NB query, for name resolving, can work both in broadcast mode or unicast mode
  - NB query be used to resolve names (e.g. "tencent"), but it can also be used to resolve FQDN (e.g. "www.tencent.com")
  - For FQDN resolving, NB query is only used when there is no DNS results.
- NBSTAT query, for diagnostics, unicast
  - NBSTAT query is usually send by diagnostic tools such as nbtstat.exe the system also sent it after failing to access network share path such as \\10.10.10.10\BadTunnel
- NB query and NBSTAT query shares the same Transaction ID counter

```
C:\Users\tk>ping -n 1 WINXP
```

```
Pinging WINXP [192.168.152.129] with 32 bytes of data:
Reply from 192.168.152.129: bytes=32 time=1ms TTL=128
```

```
Ping statistics for 192.168.152.129:
```

```
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

```
C:\Users\tk>nbtstat -A 192.168.152.129
```

```
Local Area Connection:
```

```
Node IpAddress: [192.168.152.128] Scope Id: []
```

### NetBIOS Remote Machine Name Table

Name	Type	Status
WINXP	<00> UNIQUE	Registered
WINXP	<20> UNIQUE	Registered
WORKGROUP	<00> GROUP	Registered
WORKGROUP	<1E> GROUP	Registered
WORKGROUP	<1D> UNIQUE	Registered
..__MSBROWSE__.	<01> GROUP	Registered

```
MAC Address = 00-0C-29-DA-28-A8
```

Capturing from VMnet1 Host (port 137) [Wireshark 1.10.5 (SV...)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression...

Protocol	Length	Info
NBNS	92	Name query NB WINXP<00>
NBNS	104	Name query response NB 192.168.152.129
NBNS	92	Name query NBSTAT *<00><00><00><00><00><00><00><00><00>
NBNS	271	Name query response NBSTAT

Transaction ID: 0xdff6

- Flags: 0x0110 (Name query)
  - 0... .. = Response: Message is a query
  - .000 0... .. = Opcode: Name query (0)
  - .... ..0. .... = Truncated: Message is not truncated
  - .... ...1 .... = Recursion desired: Do query recursively
  - .... .... ...1 .... = Broadcast: Broadcast packet
- Questions: 1
- Answer RRs: 0
- Authority RRs: 0

Hex dump: ff ff ff ff ff ff 00 0c 29 49 06 e4 08 00 45 00 ... )I....

The NBNS Transaction ID is incremental.  
NB query and NBSTAT query shared the same counter.

Capturing from VMnet1 Host (port 137) [Wireshark 1.10.5 (SV...)]

Filter: Expression...

Protocol	Length	Info
NBNS	92	Name query NB WINXP<00>
NBNS	104	Name query response NB 192.168.152.129
NBNS	92	Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00>
NBNS	271	Name query response NBSTAT

Frame 1: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface 0

Ethernet II, Src: Vmware\_49:06:e4 (00:0c:29:49:06:e4), Dst: Broadcast

Internet Protocol Version 4, Src: 192.168.152.128 (192.168.152.128), Dst: 192.168.152.129

User Datagram Protocol, Src Port: netbios-ns (137), Dst Port: netbios-ns (137)

NetBIOS Name Service

Transaction ID: 0xdff6

Flags: 0x0110 (Name query)

0020 98 ff 00 89 00 89 00 3a 10 2f df f6 01 10 00 01 .....:..^

0030 00 00 00 00 00 00 20 46 48 45 4a 45 4f 46 49 46 .....:..^

0040 41 43 41 43 41 43 41 43 41 43 41 43 41 43 41 43 ACACACAC /

0050 41 43 41 43 41 41 41 00 00 20 00 01 ACACAAA. .v

Identification of transaction (nbns.id), 2 ... Profile: Default

Capturing from VMnet1 Host (port 137) [Wireshark 1.10.5 (SV...)]

Filter: Expression...

Protocol	Length	Info
NBNS	92	Name query NB WINXP<00>
NBNS	104	Name query response NB 192.168.152.129
NBNS	92	Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00>
NBNS	271	Name query response NBSTAT

Frame 3: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface 0

Ethernet II, Src: Vmware\_49:06:e4 (00:0c:29:49:06:e4), Dst: Vmware\_49:06:e4 (00:0c:29:49:06:e4)

Internet Protocol Version 4, Src: 192.168.152.128 (192.168.152.128), Dst: 192.168.152.129

User Datagram Protocol, Src Port: netbios-ns (137), Dst Port: netbios-ns (137)

NetBIOS Name Service

Transaction ID: 0xdff7

Flags: 0x0000 (Name query)

0020 98 81 00 89 00 89 00 3a 2d e4 df f7 00 00 00 01 .....:..^

0030 00 00 00 00 00 00 20 43 4b 41 41 41 41 41 41 41 .....:..^

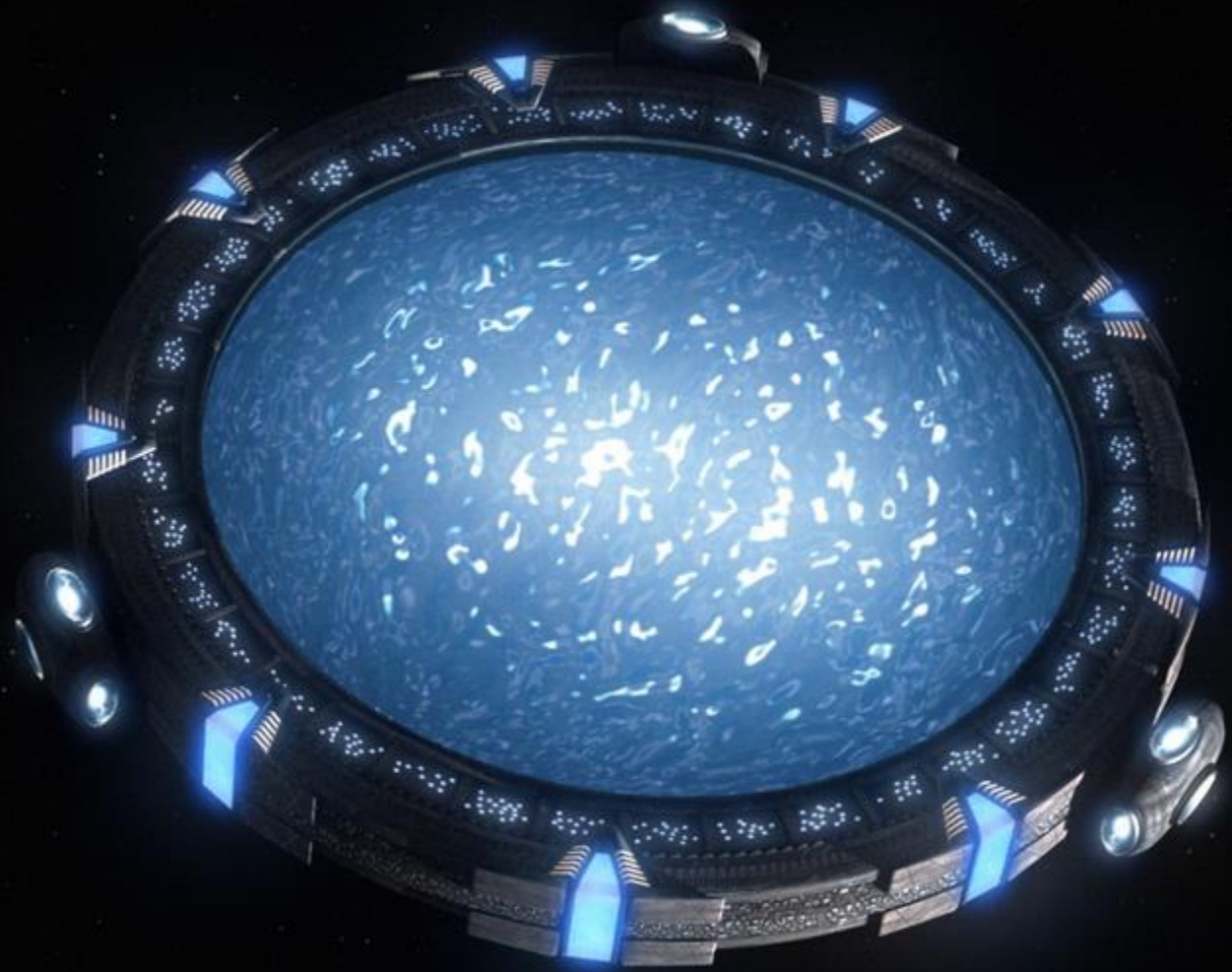
0040 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAA /

0050 41 41 41 41 41 41 41 00 00 21 00 01 AAAAAAA. .v

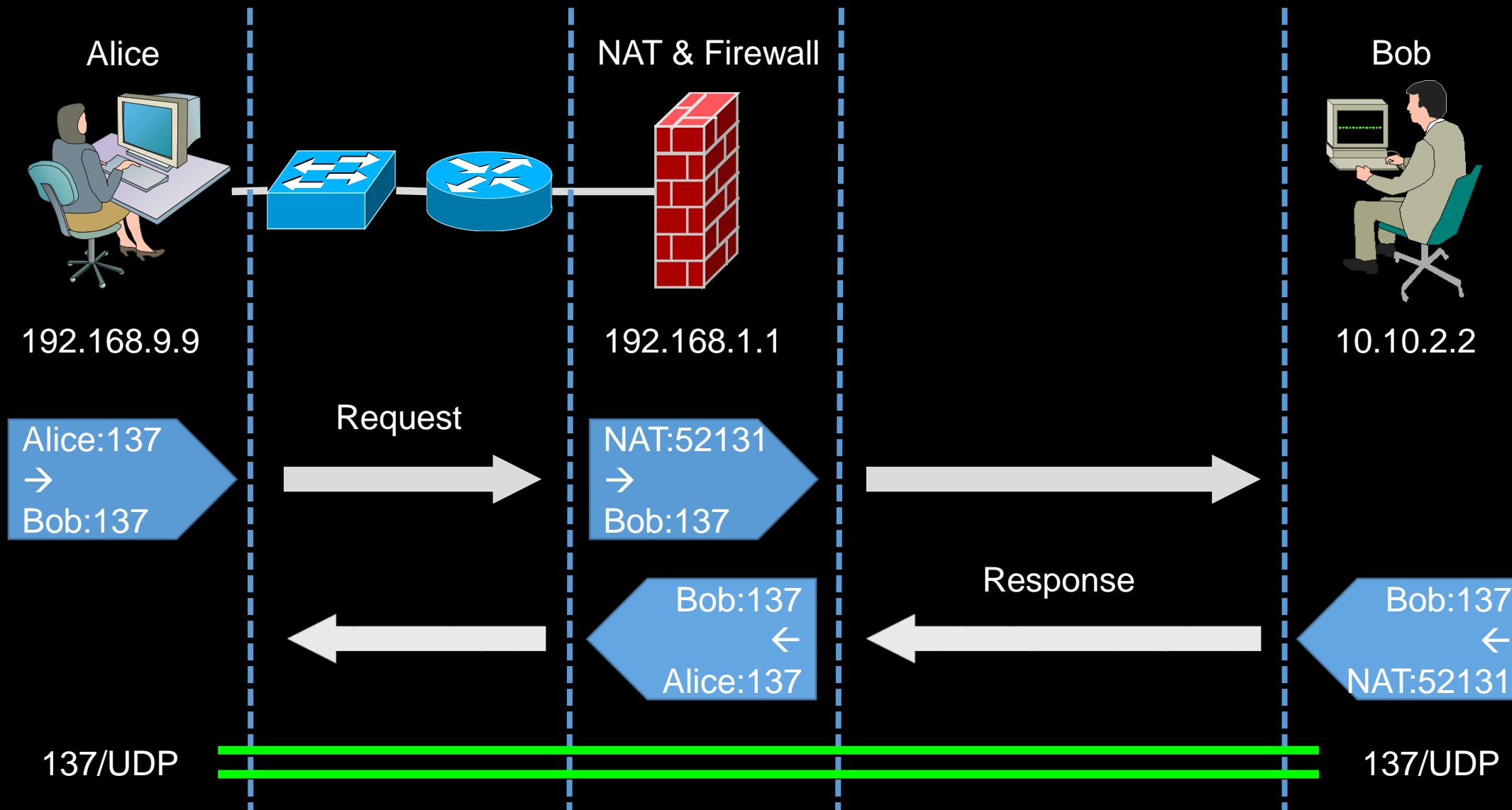
Identification of transaction (nbns.id), 2 ... Profile: Default



# Create BadTunnel



# If Alice send a NBSTAT query to Bob:



As mentioned previously, NBNS use UDP packets sent **from and to** port 137.

Host firewalls, network firewalls, NAT devices and any other network devices cannot distinguish which session the UDP packet belongs to, so if they allow a UDP traffic, they must allow the UDP packet on both directions.

So, the client can become the server, the server can become a client.

Now, the only question is: how to make Alice send a NBSTAT query to Bob?



When Windows is trying to access an UNC path with IP address, if the 139 and 445 port of the target is inaccessible – either timed out or been reset – the system will send a NBNS NBSTAT query to the target IP address.

There are numerous ways to make a system access a UNC path.

To web browser:

```

```

To MS Office:

```
Set TargetMode to "External" and Target to "file://10.10.10.10/A/A.png"
```

To shortcut:

```
Set IconFile to "file://10.10.10.10/A"
```

To web server:

```
http://web.server/reader.aspx?ID="//10.10.10.10/BadTunnel
```

...

What BadTunnel could do

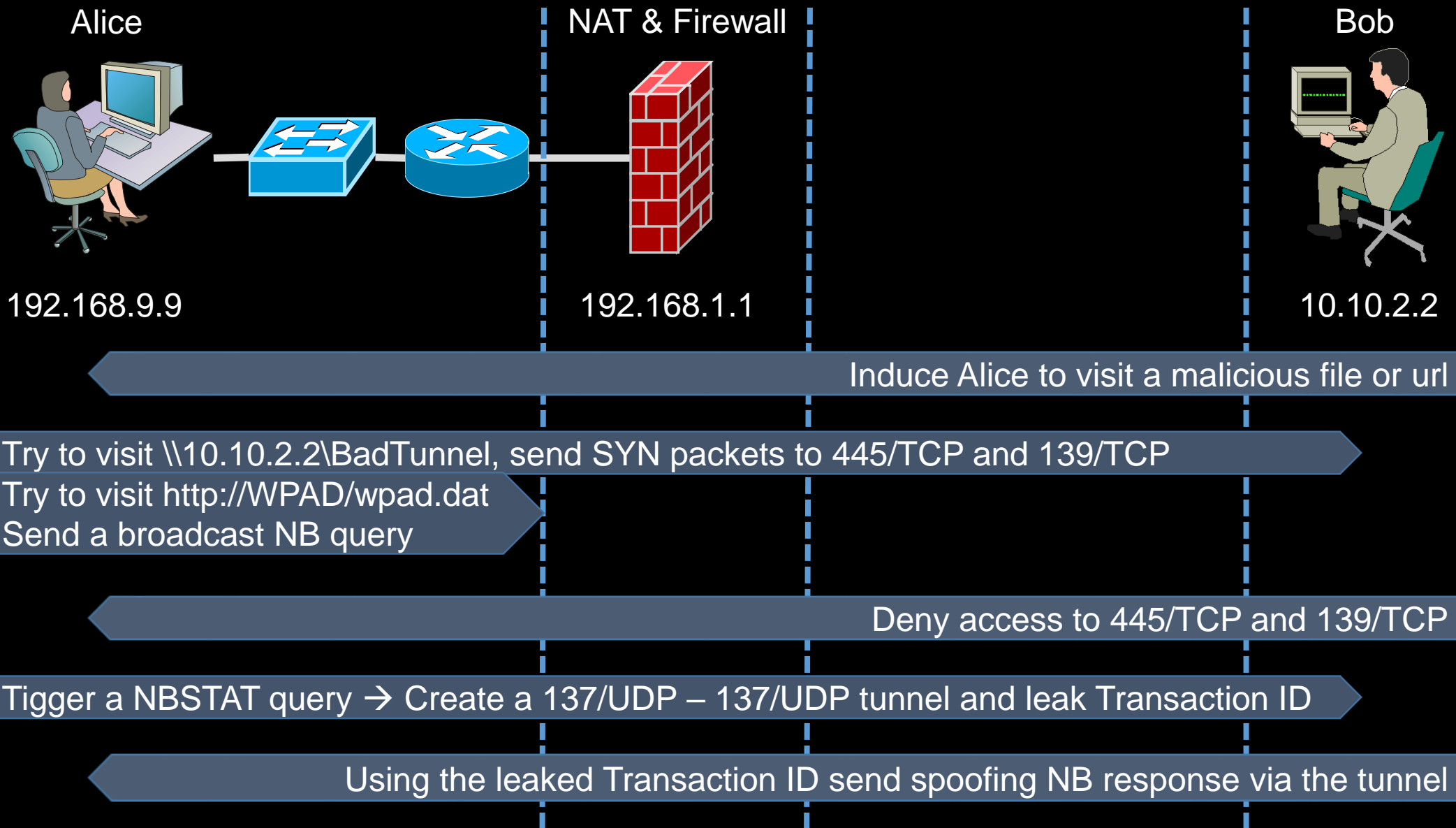


# What BadTunnel Could Do?

- Hijack "WPAD"
  - The Web Proxy Auto-Discovery Protocol
  - Windows system use `http://WPAD/wpad.dat` to configure proxy settings
  - Hijacking WPAD + Evilgrade  $\approx$  Execute any program
  - Hijacking WPAD = Bypass IE Sandbox
    - If the `wpad.dat` returns "DIRECT" for a site, IE will runs at Medium IL, outside of EPM/AppContainer
- Hijack "ISATAP"
  - ISATAP: The Intra-Site Automatic Tunnel Addressing Protocol
  - Windows use hosts named "ISATAP" as ISATAP router.
- Hijack nonexistent domain name
  - Steal Cookies
- Send NBNS NBSTAT query to get LAN host name and MAC addresses



# Using BadTunnel to Hijack WPAD



With BadTunnel, you can hijack the network traffic of every version of the Microsoft Windows going back to Windows 95

This is Big Brother power

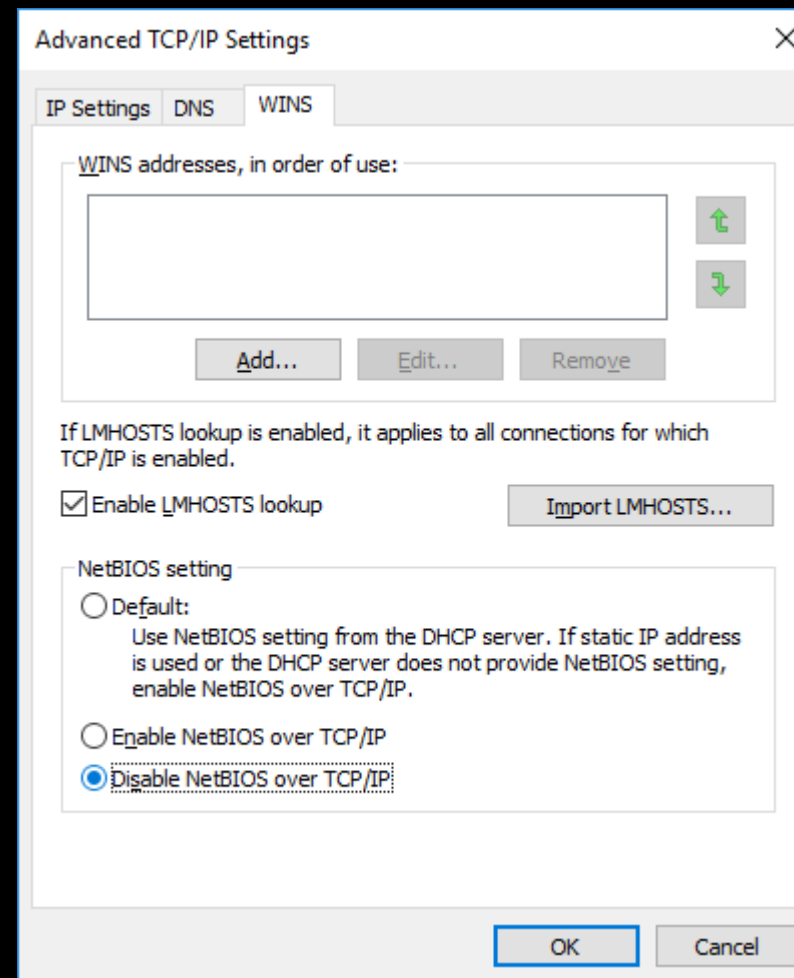




# How to defend against BadTunnel attacks

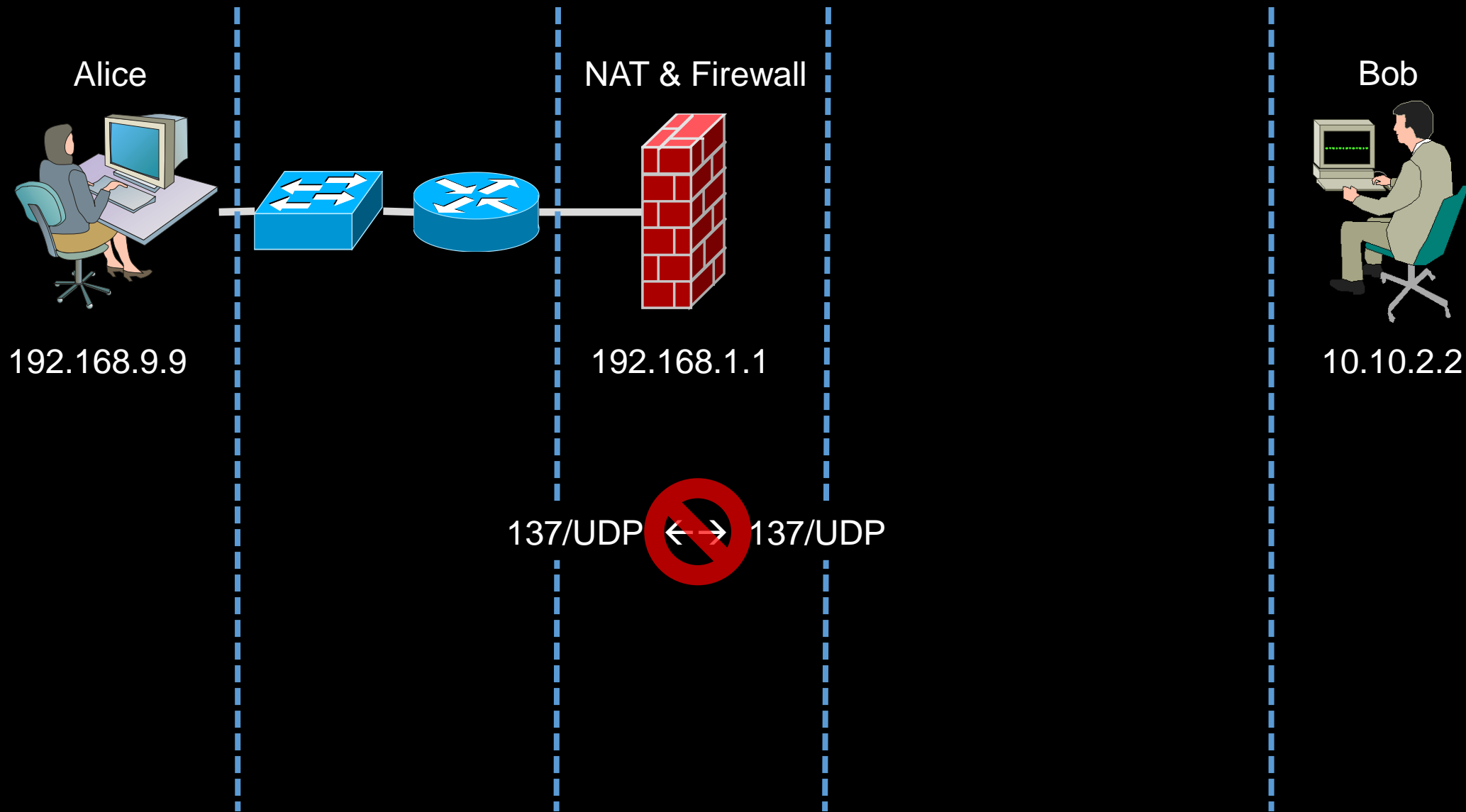
# Defend Against BadTunnel

- Microsoft has fixed the vulnerability in June 2016
  - No more NBNS NBSTAT query after failed UNC path access
  - No longer use NBNS to resolve WPAD name
- If you are still using unsupported versions such as Windows XP, or otherwise can not install the patch, you could consider disabling the NetBIOS over TCP/IP.





# Mitigate with Perimeter Firewall



Thank you for listening!



To explore strange attack surfaces  
To seek out new flaws and new weaknesses  
To boldly go where no hacker has gone before