Lab 06
Reflection

CIT 288

Chaz Davis

BCTC
Spring 2020

February 20, 2020

Reflection

i) What is the difference in a personal VPN and an enterprise VPN at a company?
Personal VPN's are limited as to the bandwidth they can provide, partially because they're dependent on the public internet for connectivity and also because you're sharing a connection to the service provider's server (which can only support so much bandwidth in or out). These services are also limited when it comes to more advanced network configuration options; again, that's likely by design since they're really designed as easy-to-use consumer products rather than IT tools.
A key difference with enterprise VPNs is that they support essentially any type of networking. You're not restricted to using the public internet, and while you can use it, you don't have to. The benefit with the resulting private networking is that it's far more secure. While voice and video services can work without a VPN, the result can frequently be much less than ideal. This is one situation in which you need an enterprise solution if you want your communications to sound like you're really in an enterprise.
ii) What is NAT and how does it affect VPN usage?
Network address translation or NAT is a method by which IP addresses are mapped from one group to another and the address translation is transparent to the end-users. VPN's come in two varieties, Remote Access VPN and Site-to-site VPN, remote access is based on point to pooint connections and is estabished between a user's computer and the organization's server. the site to site uses a gateway device to connect the entire network from one location to the other. in this case, the gateway handles the VPN connections, so end-node does not need VPN clients. Most of the site-to-site VPN's use IPsec. the can also use multiprotocol label switching or MPLS to create VPNs.
VPN tunnel cannot be established if both the destination network and the local network have the same subnets. so you have to create a VPN tunnel to overcome this on an end to end overlapping subnets.
iii) What has replaced PPTP in VPN technologies?
OpenVPN is the current secure protocol standard thats replaced pptp.
iv) What is IPsec?
IPSec is an IETF standard suite of protocols between 2 communication points accross an IP network. It can be used to encrypt application layer data, provide security for routers sending routing data accross the public internet, to provide authentication without encryption, and protect network data by setting up circuits using IPSec tunneling.
v) How well is the Windows Firewall doing its job at the beginning of the lab?
It is not doing a great job. after we redid the configurations and added the VPN, things were going greaat.
vi) What is a RADIUS server? Is it superior to single host authentication? Why or why not?
Communication between a NAS and a RADIUS server is based on the UDP

protocol. Generaly a RADIUS server, or Remote Authentication Dial-In User Service, is considered a connectionless service. radius is a client/server protocol. the radius client is typically a NAS and the radius server is usually a daemon process running on a UNIX machine. The client passes user info to designated radius servers and acts on the response that is returned.

vii) What does the ping switch -n do?

the number of pings to be sent.

viii) What is a safer alternative to TELNET? Why?

SSH, and a more recent version, is MOSH. which is a mobile shell, which allows roaming, supports intermittent connectivity, and provides intelligent local echo and line editing of user keystrokes. its more robust and responsive, especially over wifi, cellular and long distance links.

ix) What is a banner grab?

banner grabbing is a technique used to gain information about a computer system on a network and the services running on its open ports. Admins can use this to take inventory of the systems and services on their network.

x) How does ipconfig information change once you connect to a VPN?

Theoretically, your ip address should stay the same, because the IP address is set internally and pre VPN. its the end node of the VPN that is different. the way the browser and other computers view it.

xi) How can you initiate a permanent ping from a Windows CMD?

from Windows CMD you would issue ping with a -t flag. On linux, its runs on an endless loop already.

xii) what is the command used to map a drive?

We can map a drive to the network with net use drive: path

xiii) What wireshark filters shows VPN traffic?

follow UDP/TCP streams.