Network protocols attacks and countermeasure

Thuya

Manager – IT Security (Ananda)

Hacktilizer Team (Founder)

Agenda!

- Who am I?
- Layer 2 Protocols attacks and defenses
- Layer 3 Protocols attacks and defenses
- IPv6 attacks and defenses
- Tools
- Demos
- Q&A

Who am I?

IT-Security team Manager @ Ananda Livemore

Founder @ Hacktilizer Cybersecurity Research Team.

Around 10 years in IT-Security Domain.

CISCO CYBER OPS, CEH, ENSA, Fortinet NSE4, MCTS, MCNP, ITPEC,Cyber seagame CTF Player

The opinions expressed in this presentation are those of the speaker and do not reflect those of past, present or future employers, partners or customers.
Attacking and breaking network without permission is illegal and should not be performed. This presentation does not approve hacking/breaking network/attacking network in any way shape or form.

Background

- Nobody talks about these vulnerabilities
- Hacker focus on web apps, mobile apps, IOT hacking.
- Old protocols but still used widely.
- If you can own the network, literally you can own the IT system.
- Network admin should need to aware.
- Hardware upgrade, protocols aren’t
- Most small and mid-size company vulnerable to these attacks

No more network vulnerabilities

- Are you sure ?
- Heardbleed <CVE-2014-0160> (2014-2015).
- Microsoft EthernalBlue <MS17-010> (2017).
- CVE-2019-1967 (NTP vulnerability)
- CVE-2019-1963 (SNMP vulnerability in cisco devices)
- CVE-2019-1326 (Microsoft Windows Remote Desktop Protocol, Denial of Service Vulnerability)

The Threat Surface

- Access to a live network port
- or Wifi (including “guest” network)
- OR even VPN network.
- Think about your perimeter ??????

Let’s go to layer 2 protocols

ARP

- Address Resolution protocol
- Essential layer 2 protocol
- IP to MAC address mapping
- Mac to IP : Reverse ARP (RARP)
- ARP cache
- **### No authentication ###**

ARP Attacks

- ARP spoofing
  - Pretending to be something else
- ARP Poisoning
  - Messing with ARP caches
- Mac flooding
  - Filling up CAM tables
- Very well known attacks…..

ARP Defense

- Port security and 802.1x
  - Prevents MiTM attacks
- Dynamic ARP Inspection (DAI)
  - Verifies MAC to IP mapping
  - Rate limits ARP packets
- Static ARP entries
  - Can be tough to manage
  - Good idea for sensitive systems
- ARP defense tools and IDS

CDP

- Cisco Discovery Protocol
- Multicast.
- Advertises device capabilities.
  - Router, switch, voice, etc.
- Voice VLAN determination.
- **### No authentication ###**

CDP Attacks

- DOS: flood the CDP table
  - very effective
- Troll: add non-existent device.
- Pwn: jump onto other VLANs
  - Access to VOIP subnets

CDP Defense

- Turn of the CDP
  - No cdp run (cisco command)
- Port security and 802.1x

- *** if you have any idea to defense this protocol, let the Cisco know, I think they'll pay you ☺

DHCP

- Dynamic Host Configuration Protocol
  - IP address and other necessary add leasing
  - DNS
  - Default gateway
  - For TFTP services (voice, thin clients, PXE)
- Wireless controllers
- Broadcast across a given subnets
- **### No authentication ###**

DHCP Attacks

- DOS : eating the entire address pool
- DOS : send clients fake addresses
- Pwn : Rouge DHCP server and gateway
  - miTM attack
  - DNS spoofing
  - Boot from attacker firmware/OS
  - Boot from attacker WiFi controller

DHCP Defense

- Port security and 802.1x
- DHCP snooping
  - Cisco commands
- IPS/IDS

DTP

- Dynamic Trunking Protocol
- Cisco proprietary
- For trunking VLANs between switches
- Default auto-negotiate on all ports
- ### No authentication ###

DTP Attacks

- DOS: Trunk VLANs out too far
- Pwn : Trunk VLANs to attacker box
  - VLANs are available on target switch

DTP Defense

- Disable it
  - Switchport nonegotiate (Cisco command)
- Port security and 802.1x

(R)STP

- (Rapid) Spanning Tree Protocol
- Csico proprietary: PVST & PVST+
- Prevents network loop using Bridge Protocol Data Unit
- Elets a root "bridge" (Switch)
- ### No authentication ###

(R)STP Attacks

- DOS : random BPDUs
  - Create loops instead of preventing them... ((+_+))
- Pwn: become the root bridge
  - Not your standard MiTM
  - Little/no impact to users (if done correctly)
  - Potentially wide scope

(R)STP Defense

- Stop using it. Please
- LACP + switch stack & virtualization = no more STP
- But since that costs big $$
- Disable STP on non-trunk ports
- Enable BPDU Guard (circa 2005)
- Enable Root Guard
- Hope for no more bugs
- Stay patched

HSRP/VRRP

- Hot Standby Router Protocol
  - Cisco proprietary
- Virtual Router Redundancy Protocol
  - Used by other vendor as well as Cisco
- Layer 3 redundancy protocol
- Shared MAC and IP address
- Clear text authentication by default
  - Can sniff and same as no authentication ☺

HSRP/VRRP Attacks

- DOS: Send client to nowhere
- Pwn : become primary router
  - Act as MiTM for entire subnet
  - Easier than any other method
  - No need to brute force the password
  - Little/no impact to users (if done right)

HSRP/VRRP Defense

- MD5 for authentication string
  - Broken, but better than nothing
  - Log failovers & treat as potential security events
  - Need to add more security from developer
- Get a better redundancy protocol
  - Common Address Redundancy Protocol (CARP)
  - From OpenBSD
  - Uses SHA-1 & protects virtual IP

Routing protocol attacks

- Interior gateway protocols
- OSPF, IGRP, EIGRP, RIP
- Vulnerable when no authentication (default)
- Can guess and brute force the password (cisco)
- Send crafted packet to the router and own the network.

Routing protocol defense

- Listen only where you have to
  - Passive interface command in cisco
- Put Strong Authentication
- Control Plane Policing (Cisco)
  - Allows you to rate limit all matching traffic across the entire device

BGP attacks and defenses

- Send crafted packet to the router and own the network.

- Defenses
- Require authentication
  - Coordination with ISP
- TTL security check
  - Restrict to routers x hops away
- Access control lists
- Set max prefixes (if possible)
- Filter inbound prefixes
- Limit AS path length
- Control Plane Policing

Let’s talk about IPv6

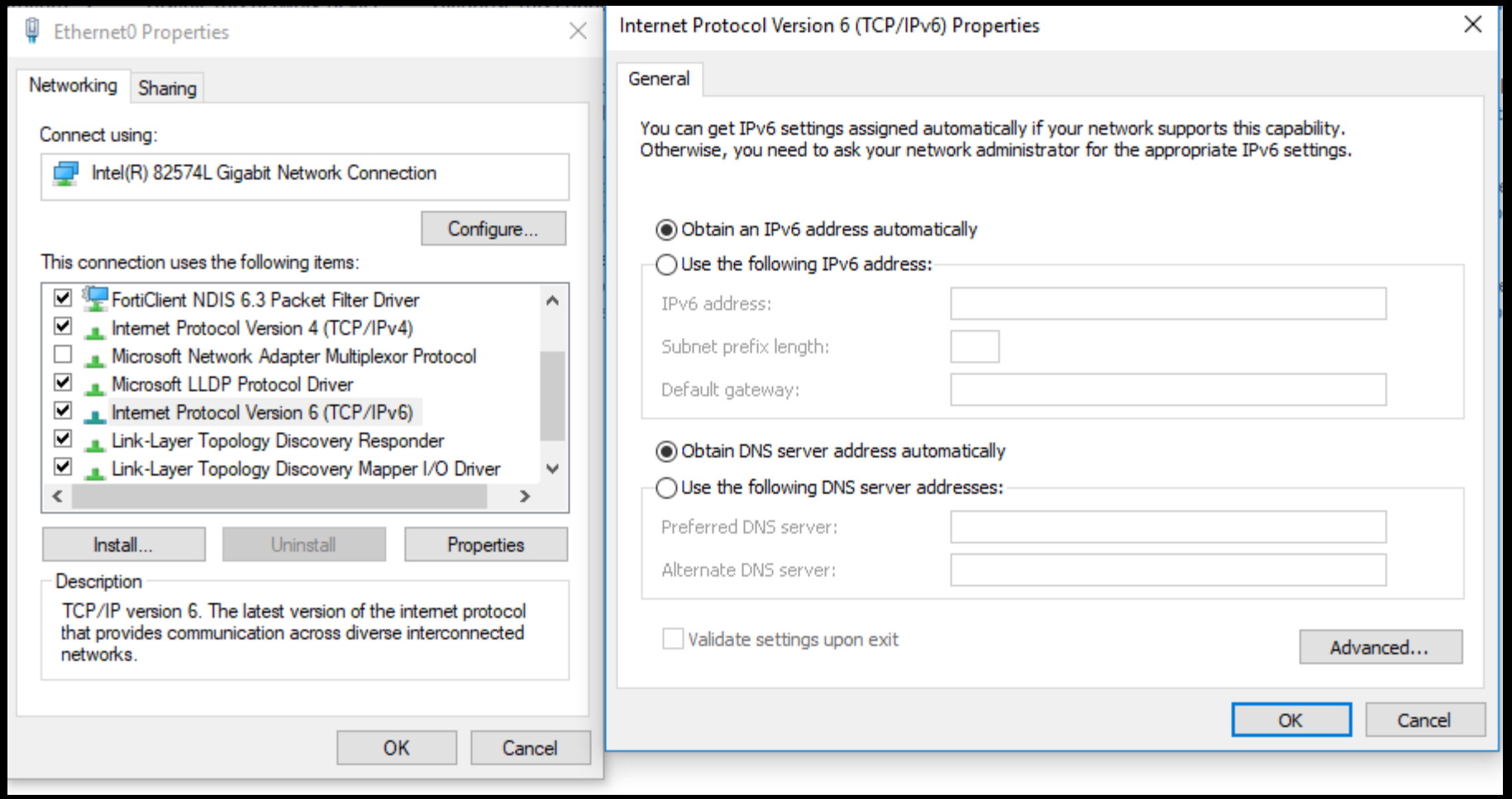
- Many vulnerabilities to be aware
  - NA Spoofing
  - SLACC attack
  - WPAD attack
  - Many more !!
- IPv6 defense ?

Ipconfig (dangerous cli)

```
Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::ac1b:f830:fe24:ef91%4
   IPv4 Address. . . . . . . . . . . : 192.168.246.128
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.246.2
```

IPv6 is by default enable ☹



ICMPv6 (NDP)

- No ARP
  - No ARP Spoofing
  - Tools anti-ARP Spoofing are useless

- NeighbourDiscoveryProtocol uses ICPMv6
  - NS: NeighbourSolicitation
  - NA: NeighbourAdvertisement

And it works!: Neighbours

C:\WINDOWS\system32\cmd.exe

```
C:\Users\thuya>netsh interface ipv6 show neighbors

Interface 1: Loopback Pseudo-Interface 1


Internet Address                              Physical Address   Type
--------------------------------------------  -----------------  -----------
ff02::c                                                          Permanent
ff02::16                                                         Permanent
ff02::1:2                                                        Permanent

Interface 21: Local Area Connection* 2


Internet Address                              Physical Address   Type
--------------------------------------------  -----------------  -----------
ff02::16                                      33-33-00-00-00-16  Permanent
ff02::1:2                                     33-33-00-01-00-02  Permanent

Interface 7: VMware Network Adapter VMnet1


Internet Address                              Physical Address   Type
--------------------------------------------  -----------------  -----------
ff02::1                                       33-33-00-00-00-01  Permanent
ff02::2                                       33-33-00-00-00-02  Permanent
ff02::c                                       33-33-00-00-00-0c  Permanent
ff02::16                                      33-33-00-00-00-16  Permanent
ff02::fb                                      33-33-00-00-00-fb  Permanent
ff02::1:2                                     33-33-00-01-00-02  Permanent
ff02::1:3                                     33-33-00-01-00-03  Permanent
ff02::1:ff85:dcf3                             33-33-ff-85-dc-f3  Permanent
```

ICMPv6: SLAAC

- Stateless Address Auto Configuration
- Devices ask for routers
- Routers public their IPv6 Address
- Devices auto-configure IPv6 and Gateway
  - RS: RouterSolicitation
  - RA: RouterAdvertisement

WPAD attack in IPv6

- Web Proxy Auto Discovery
- Automatic configuration of Web Proxy Servers
- Web Browsers search for WPAD DNS record
- Connect to Server and download WPAD.pac
- Configure HTTP connections through Proxy

WPAD Attack

- Evil FOCA configures DNS Answers for WPAD
- Configures a Rogue Proxy Server listening in IPv6 network
- Re-route all HTTP (IPv6) connections to Internet (IPv4)

THC-IPv6 Attack Tool

- fake_router6 eth0 2001:db8:BAD::/64
- detect-new-ip6 eth0
- dos-new-ip6 eth0
- flood_router6 eth0
- flood_advertise6 eth0
- implementation6 eth0 2001::1
- smurf6 eth0 2001::1

IPv6 defenses

- IPv6 is on your box
  - Configure it or kill it (if possible)

- IPv6 is on your network
  - IPv4 security controls are not enough
  - Topera (port scanner over IPv6)
  - Slowloris over IPv6

Tools

Scapy

- Swiss army knife (packet creation/manipulation/sniffing)
- First released in 2005 by Philippe Biondi
- Many protocols supported
- Based in Python
- Lots of community support
- My tutorial on Youtube

Yersinia

- Layer 2 and 3 protocols attack toolkits
- Released in 2005 by David Barroso and Alfredo Andres at Black Hat EU
- GUI and CLI
- Easy to use

Evil Foca

- Test security in IPv4 and IPv6 data network.
  - MITM over IPv4 networks with ARP Spoofing and DHCP ACK Injection.
  - MITM on IPv6 networks with Neighbor Advertisement Spoofing, SLAAC attack, fake DHCPv6.
  - DoS (Denial of Service) on IPv4 networks with ARP Spoofing.
  - DoS (Denial of Service) on IPv6 networks with SLAAC DoS.
  - DNS Hijacking.
- 01/09/15. Version 0.1.3 (Open Source)

Other Tools

- Nping – released by Fyodar in 2010 with Nmap 5.30
- Hping3 – released in 2007 by Victor Forsyuk
  - Some of the function are the same with Scapy but limited
- Loki – Released in 2010 at Black Hat USA by Daniel Mende, Rene

References and credits

- Python security community
- Scapy
- THC (The Hacker’s Choice)

Questions?

- thuya@hacktilizer.com

- http://www.facebook.com/hacktilizer

- https://www.linkedin.com/in/thuya