Project 1 - CSCI 3403: Modern Cybersecurity Fundamentals

Group:
Jacob Christiansen (jach7037@colorado.edu), Nick Price (Nicholas.Price-1@colorado.edu), Devin Murray (Devin.Murray@colorado.edu)

Event:

CISCO Devices Vulnerabilities

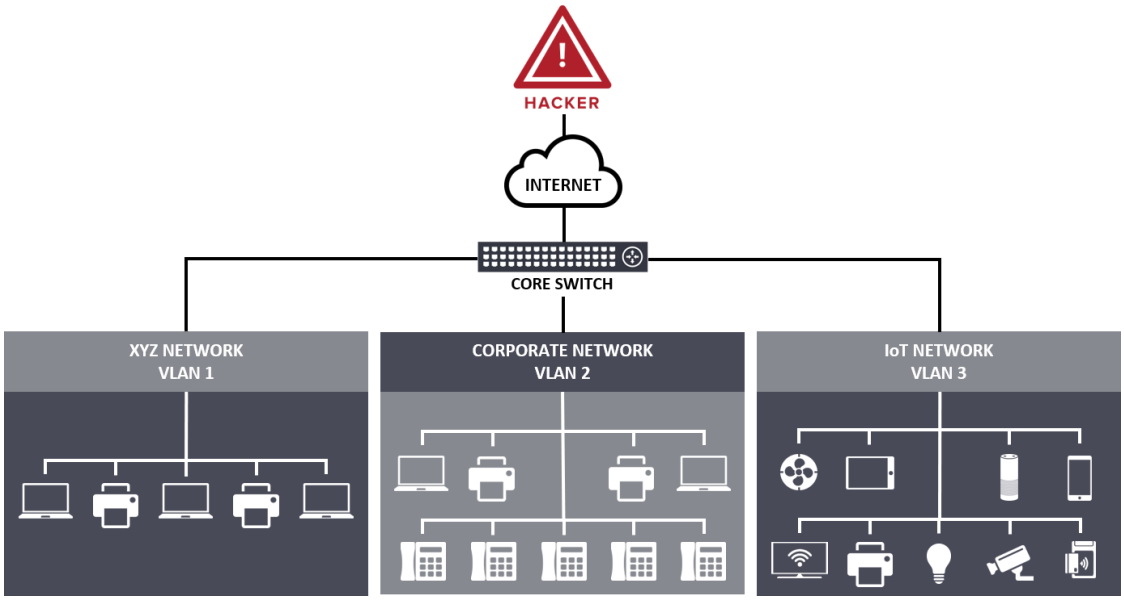
Questions:

1. (5 points) In 2-3 sentences, explain what your event was about at a conceptual level. In this, explain how it relates to cybersecurity

Security firm Armis has discovered that CISCO, a dominant manufacturer of enterprise IoT products, has a software flaw included in most (if not all) of its devices. The flaw lies within a communications mechanism of the devices called Cisco Discovery Protocol (CDP). If an attacker gains access to a network, this one vulnerability can be used to target many CISCO devices at once, and then potentially grant access to more restrictive parts of the network.

2. (5 points) In 2-3 sentences, explain some of the technical details of your event.

The aforementioned CDP, once breached, makes it extremely easy for attackers to locate other Cisco products on the same network. From this, one vulnerability can be used to target many other devices or seek out crucial devices such as network switches. While you will still need an initial attack, the CDP creates an extremely efficient route to take control of an entire network.



3. (5 points) What is the most interesting thing you took away from reading about your article?

Something that stood out to me particularly is the concept of “segmentation”. The idea is that in a network of connected devices, sections of them are blocked off, essentially restricting everything from talking to everything, limiting the amount of damage an attack could pose. This CISCO flaw essentially bypasses that restriction. Much like a boat’s hull in order to avoid the entire ship sinking to a single breach.

4. (5 points) Analyze some impacts from your event on each of the CIA triad in 1-2 sentences each.

a. Confidentiality:

The ability for the breach of a single vulnerability to easily cause breaches to many other devices on that network gives people access who otherwise shouldn’t have access to that information.

b. Integrity:

The breach in confidentiality above creates the ability for attackers to view and potentially alter data in transit between devices, creating an impact on integrity.

c. Availability:

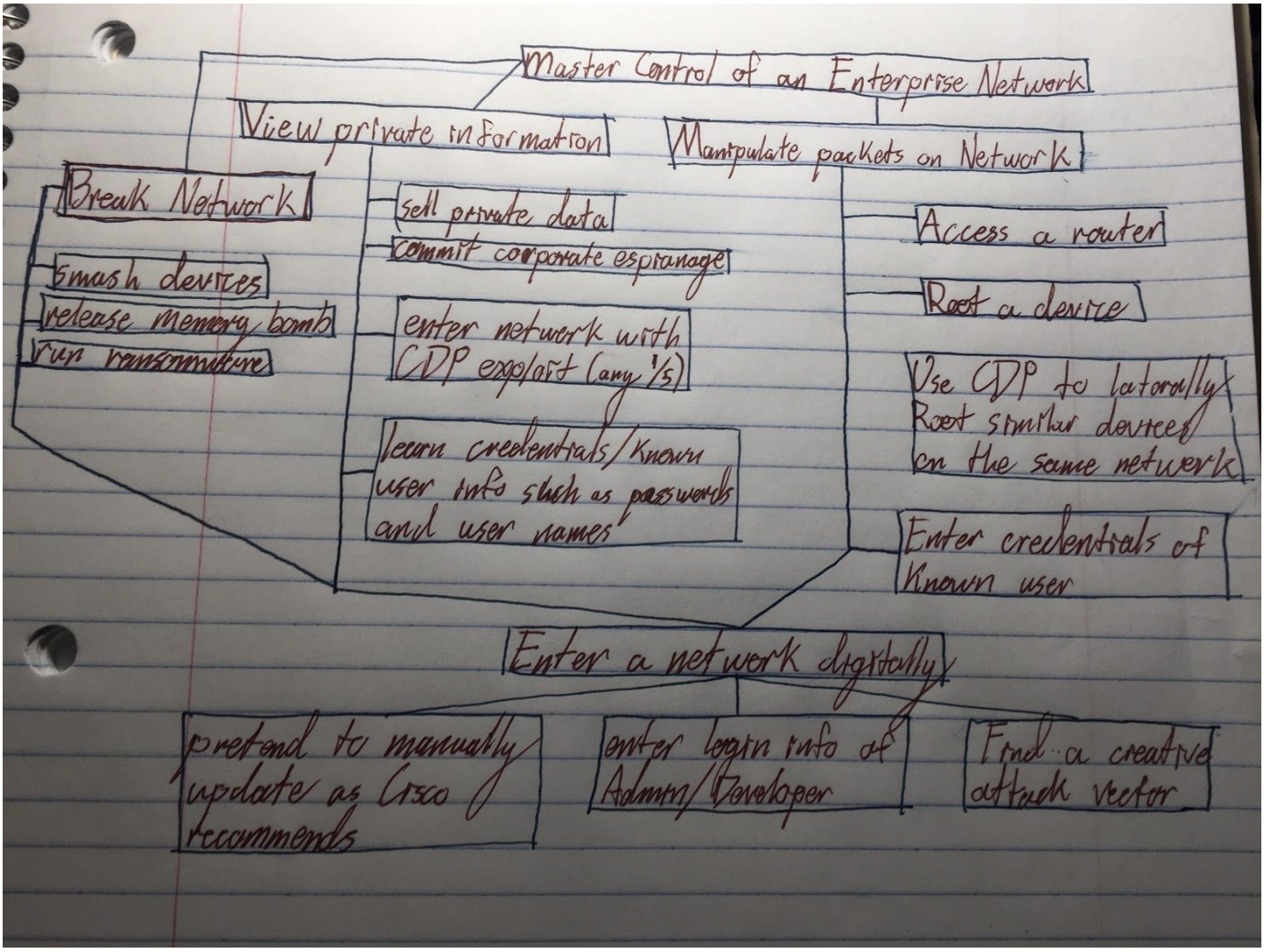
The article also touches on how most devices that suffer from this specific vulnerability need to be updated manually, and at specific times to avoid any downtime. A vulnerability as a direct effect of devices not being updated is a significant negative impact on Availability.

5. (5 points) Pick 3 common design principles and explain the impact on your event in 1-2 sentences each.

- Minimize The Attack Surface Area: The attack area for this variability is huge; literally every CISCO-made phone, web cam, network switch, etc. However, they all run off CDP, so security measures can be implemented immediately at a higher level to restrict further access, while individual firmware updates and software updates to CBP can be rolled out over time.
- Record Participants: Cisco may not feel the need or the moral compulsion to record the details but the actions of all known participants should be logged off-network. A send only ledger of participants and their generalized can make it more clear where a breach was. Who employed an exploit. As well as roughly when such events took place. If these event logs remain solely on a private network then the escalation of compromised devices through CDP can eventually lead to a loss of integrity of every aspect of companies’ digital presence.
- Make Compromise Difficult: While a single device may lead to an avalanche of breaches in a Cisco-based network it is not impossible to bar an attacker from the premises

entirely. By keeping routers and phone systems at a physically far distance with barriers to entry such as gates and locked doors. Any potential attacker would need to rely on wireless attacks on phones or internet-connected devices. This should be many enterprises' biggest priority until they manually patch their devices as any one exploit immediately has the known vulnerability of compromising the entire network.

6. **EXTRA CREDIT** (3 points) Create an attack tree of your current event (15-20 leaf nodes is fine). You
may create it digitally or write it neatly and scan it in – whichever is easier for you.



Sources:

- https://www.wired.com/story/cisco-cdp-flaws-enterprise-hacking/
- https://threatpost.com/critical-cisco-cdpwn-flaws-network-segmentation/152546/
- https://www.forbes.com/sites/daveywinder/2020/02/05/cisco-confirms-5-serious-security-threats-to-tens-of-millions-of-network-devices/#4cf2463213e8
- https://www.armis.com/cdpwn/

Contributions:

Jacob: Article/Sources, Problems 1, 3, 5

Nick: Problems 2, 4, 5

Devin: Problems 5, 6 (sketch)