The 3rd International Conference on Vocational Innovation and Applied Sciences (ICVIAS) 2021
Volume 2022
http://dx.doi.org/10.11594/nstp.2022.1610

NST PROCEEDINGS

OPEN ACCESS

Conference Paper

Best Practice Layer 2 Security for remote Vocational Education

Dimas Febriyan Priambodo[1]*, Nurul Syamsiah[2], Hermawan Setiawan[3], Yulandi[2]

[1]Department of Cyber Security, Politeknik Siber dan Sandi Negara, Indonesia
[2]Department of Laboratorium, Politeknik Siber dan Sandi Negara, Indonesia
[3]Department of Cryptography, Politeknik Siber dan Sandi Negara, Indonesia

Corresponding author:
E-mail:
dimas.febriyan@poltekssn.ac.id

ABSTRACT

Open standards especially OSI are built to separate each layer and work without knowledge of each other. This concept also means if one layer is hacked, communication is compromised without another layer alert. In best practice, layer 2 security is underrated as it is considered that security has been built through the application layer. In vocational education who are prepared to work directly in the real world, should not be forgotten to be taught. This method proposed online education for teaching layer 2 security with HyperV virtual machine to build attack and defend scenarios. Hyper V is used because windows have been installed in almost all students. In Defcon was also used HyperV was found to be able to operate to respond to attack scenarios in the second layer of security. This system was implemented in 20 students (all population in class) of security engineering in the polytechnic XYZ and shows a significant increase with normal data in statistical approach with t-test. This approach causes an increase in student scores by 12.307% by implementing a new system.

Keywords: layer 2 security, vocational education, network security

Introduction

Remember Mission Impossible movie? In one of the scene the cast insert tool in the switch so the command center can access all CCTV and override the system. This method is a traditional technique but powerful. System override using the weak internal network. In a technical view, this is the weakness of layer 2 security. Data communication is required to adhere to the open standards for better interoperability, competition, and innovation. There is many standard organization d this job like IEEE, IETF, ITU, TIA, etc. Open standard OSI Layer separate work in layer independently. This concept is good for guidance tools to develop any network device or model.

Layer 2 can cause major downtime (Mehra & Krishnan, 2018). layer 2 attack requires a high level of intelligence and good knowledge of what is going on in the communication actions (Cusack & Lutui, 2015) mostly attack from internal organization. Commonly internal network is a trusted one, attacking from an internal like traitor in the army and giving deep impact on it. Forgiving more awareness from FBI report in (Richardson, 2003), 99% of all enterprises network ports are open. Capability to take action for layer 2 attack must prepare beyond OSI layer weakness. Especially for a student in vocational education that has more practice curriculum than classical ones.

Pandemic covid 19 needs adjustment for any activity like study, work, and entertainment. All activity doing from home. In education ones, there are many solutions for reaching study goal. One of them is facilitating practicum from home. Layer 2 security in many education studies with the

How to cite:
Priambodo, D. F., Syamsiah, N., Setiawan, H., & Yulandi. (2022). Best practice layer 2 security for remote vocational education. *The 3rd International Conference on Vocational Innovation and Applied Sciences (ICVIAS) 2021*. NST Proceedings. pages 65-70. doi: 10.11594/ nstp.2021.1610

native tool, some need a manageable switch. Cisco has the solution of using a virtual environment with a packet tracer. Packet tracer is good for studying fundamental networks for network engineers but can't do cross-platform so practicum network security has boundaries.

Although another virtualized-based education using packet tracer or GNS3, Best practice layer 2 security for remote vocational education using Hyper V in windows. Windows environment applied because it's installed in all students. Transform education close to student tools and behavior giving more acceptance. This system suites for network security students describe from validation with t-test.

Material and Methods

A. Literature review

A literature review is needed to find out the types of attacks at layer 2 and the technology that is being developed to deal with them. layer 2 security has become a major concern in most organizations which can cause major downtime (Mehra & Krishnan, 2018). Concern in layer 2 security is hardening the switch. From Mangut et al.'s (2015) research, Address Resolution Protocol (ARP) cache poisoning attacks most often in the switch. ARP Poisoning is a type of cyberattack that abuses weaknesses in the widely used ARP to disrupt, redirect or spy on network traffic.

Norma Pilamunga et al. (2018) one type of attack that is quite famous is VLAN hopping. VLAN hopping used the benefit of trunk ports that have access to all VLANs by default for route traffic in multiple VLANs. Generally, trunk port used across switches so can be named as switch spoofing and often happens in cisco switches (https://www.cvedetails.com/cve/CVE-1999-1129/).

B. Design play role scene

Playrole scene has been built using vurnabillity that shown in the literature review step. Payroll scene builds in practicum paper. Step by step what the team must do and where to be set and analyzed detail write down in there.

C. Remote education scheme

The payroll scene can be transformed using virtual tools like packet tracer like (Data, 2016). Packet tracer is the lightweight ones but in this research, we use Microsoft virtualization with hyperV and cisco virtual switch (https://www.cisco.com/c/en/us/support/switches/nexus-1000v-switch-microsoft-hyper-v/series.html). Hyper V has been selected because in Politecnic XYZ most students use the Windows platform. Hyper V presented simplicity and gave more operability than another virtualization engine. Hypervisor type 1 uses the microkernel concept so giving more speed than others as seen in Fayyad Kazan et al research. Table 1 shows a summary of the virtual machine and virtual switch that was used. Students use the system for teaching proses by downloading the export VM file.

Table 1. summary of virtual machine

No	Virtual Machine	Virtual Switch
1	MS Server 2012	Cisco Nexus 1000V
2	MS Server 2012	Open vSwitch
3	Kali 2.0 Standalone	No virtual switch
4	Ubuntu	Open vSwitch

D. System Validation

Validation of Best Practice Layer 2 Security for remote Vocational Education carried out by statistical t-test.

Results and Discussion

VLAN Hopping is one of the VLAN attacks in layer 2 peripheral. It can be a scene with two scenes one of them as shown in figure 1. This exploit is only successful when the legitimate switch is configured to negotiate a trunk. This occurs when an interface is configured with either "dynamic desirable", "dynamic auto" or "trunk" mode. Figure 1 shows attacker connects to the port and sends a DTP message. Yenersia can be used to send it (https://tools.kali.org/vulnerability-analysis/yersinia) seen in figure 2.

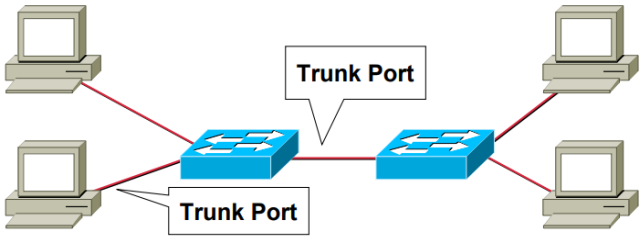

Figure 1. Switch sproofing

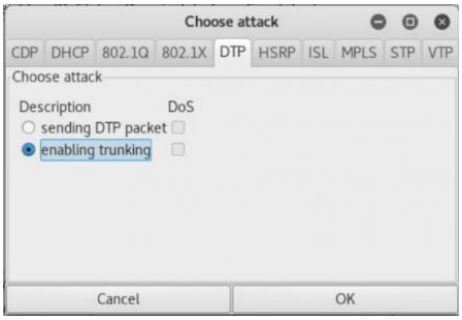

Figure 2. Yenersia dashboard

VLAN Hopping can be mitigated by manually setting Cisco Virtual Switch and disabling dynamic desirable, dynamic auto in cisco can be set with switchport mode nonegotiate. For next-level and mitigate double tagging attacks keep native VLAN of all trunks different from user and default ones. In this hyper V, the virtualization scene can be transformed in two cases one with cisco and noncisco for another. Describe above cisco have default trunking port and dynamic setting for automatic configuration, this is the weakness of it. In another case with open vswitch all ports are always hybrid ports, there is no matter for VLAN hopping just defining that VLAN tagged or untagged. This scene gives better scope of layer 2 peripheral from another brand.

There are many MAC attacks, one of them is Content Addressable Memory (CAM) overflow. In normal conditions, CAM tables store information MAC addresses available on the physical port. It has fixed sized in hacker view this is a weakness so can be flooded. The switch learns the new MAC attach on the switch by broadcasting ARP for new ones to all ports, as fast as MAC responds this switch will update this address soon. An attacker using mac of tool, 100 lines of Perl exploiting size limit on CAM tables. Mac sends random source MAC and IP addresses approximately 155000 MAC addresses in a minute causing drop packets. For vocational education, this is a basic scenario that must be learned. Using port security in real conditions gives a better experience and understanding of why using port security. In real conditions using Access Point (AP) can be a solution too. Protocol 802.11 rule that association to an AP is MAC-based, this mean translational bridge traffic coming only from or going to known MACs.

Spoofing can be split in two big scope one is Medium Access Control (MAC) sproofing and another one is IP sproofing. MAC Address spoofing scene is sending a single frame with the other

host's source Ethernet address, the network attacker overwrites MAC Address table entry so that the switch forwards packets destined for the host to attacker. In another word, attacker sends packets with the incorrect source of mac address so it looks like a target as a shadow (binding). Mitigation for this scene is using option 82 DHCP relay agent, unfortunately, this is a different virtual switch with physical ones. The virtual switch does not have a way to dynamically assign IPv4 configurations to connected VM (https://petri.com/configuring-vm-networking-hyper-v-nat-switch). So, we need to rely on something else. That something else is usually a DHCP server on the LAN. VM connected to a NAT virtual switch are in an isolated broadcast domain, a different one to the LAN. The NAT switch does not have 2-way routing to the LAN that the host is connected to. The virtual switch is an internal virtual switch that the host NATs to the LAN, by default, the VM can connect to the LAN, but the LAN can connect to the virtual machines. And even if we do create NAT rules, the virtual switch remains a separate broadcast domain from the LAN.

Virtual machines that are connected to a NAT virtual switch are in an isolated broadcast domain, a different one to the LAN. The NAT switch does not have flat, 2-way routing to the LAN that the host is connected to. The virtual switch is an internal virtual switch that the host NATs to the LAN. This means that, by default, the virtual machines can connect to the LAN, but the LAN cannot connect to the virtual machines. And even if we do create NAT rules, the virtual switch remains a separate broadcast domain from the LAN.

The next scene that has been built in the ARP attack. Before the host can talk to another, it must do an ARP request to map the IP address to mac address. In this situation anyone can claim to be the owner of any IP/MAC address they like, attacker use this to redirect traffic. ARP Poisoning scene was built as shown in figure 3 and figure 4. Two tools can be used in this scenario as dsniff and ettercap all tools have the same concept poison ARP tables so MAC address and IP pointing in another one like in figure 4. Dynamic ARP inspection. In this system, the ARP poisoning scene delivers successfully shown with the result of the test score.

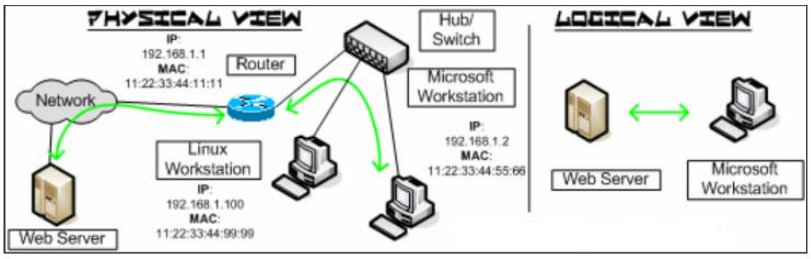

Figure 3. ARP distribution before ARP Poisoning

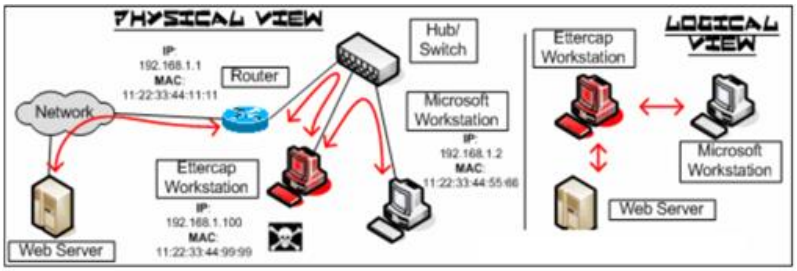

Figure 4. ARP distribution after ARP Poisoning

Table 2. T-Table

Pr	0.25	0.10	0.05	0.025	0.01	0.005	0.001

df	0.50	0.20	0.10	0.050	0.02	0.010	0.002
1	1.00000	3.07768	6.31375	12.70620	31.82052	63.65674	318.30884
2	0.81650	1.88562	2.91999	4.30265	6.96456	9.92484	22.32712
3	0.76389	1.63774	2.35336	3.18245	4.54070	5.84091	10.21453
4	0.74070	1.53321	2.13185	2.77645	3.74695	4.60409	7.17318
5	0.72669	1.47588	2.01505	2.57058	3.36493	4.03214	5.89343
6	0.71756	1.43976	1.94318	2.44691	3.14267	3.70743	5.20763
7	0.71114	1.41492	1.89458	2.36462	2.99795	3.44948	4.78529
8	0.70639	1.39682	1.85955	2.30600	2.89646	3.35539	4.50079
9	0.70272	1.38303	1.83311	2.26216	2.82144	3.24984	4.29681
10	0.69981	1.37218	1.81246	2.22814	2.76377	3.16927	4.14370
11	0.69745	1.36343	1.79588	2.20099	2.71808	3.10581	4.02470
12	0.69548	1.35622	1.78229	2.17881	2.68100	3.05454	3.92963
13	0.69383	1.35017	1.77093	2.16037	2.65031	3.01228	3.85198
14	0.69242	1.34503	1.76131	2.14479	2.62449	2.97684	3.78739
15	0.69120	1.34061	1.75305	2.13145	2.60248	2.94671	3.73283
16	0.69013	1.33676	1.74588	2.11991	2.58349	2.92078	3.68615
17	0.68920	1.33338	1.73961	2.10982	2.56693	2.89823	3.64577
18	0.68836	1.33039	1.73406	2.10092	2.55238	2.87844	3.61048
19	0.68762	1.32773	1.72913	2.09302	2.53948	2.86093	3.57940
20	0.68695	1.32534	1.72472	2.08596	2.52798	2.84535	3.55181
21	0.68635	1.32319	1.72074	2.07961	2.51765	2.83136	3.52715
22	0.68581	1.32124	1.71714	2.07387	2.50832	2.81876	3.50499
23	0.68531	1.31946	1.71387	2.06866	2.49987	2.80734	3.48496
24	0.68485	1.31784	1.71088	2.06390	2.49216	2.79694	3.46678
25	0.68443	1.31635	1.70814	2.05954	2.48511	2.78744	3.45019
26	0.68404	1.31497	1.70562	2.05553	2.47863	2.77871	3.43500
27	0.68368	1.31370	1.70329	2.05183	2.47266	2.77068	3.42103
28	0.68335	1.31253	1.70113	2.04841	2.46714	2.76326	3.40816
29	1.31143	1.69913	1.69913	2.04523	2.46202	2.75639	3.39624
30	0.68276	1.31042	1.69726	2.04227	2.45726	2.75000	3.38518
31	0.68249	1.30946	1.69552	2.03951	2.45282	2.77404	3.37490
32	0.68223	1.30857	1.69389	2.03693	2.44858	2.73848	3.36531
33	0.68200	1.30774	1.69236	2.03452	2.44479	2.73328	3.35634
34	0.68177	1.30695	1.69092	2.03224	2.44115	2.72839	2.34793
35	0.68156	1.30621	1.68957	2.03011	2.43772	2.72381	3.34005
36	0.68137	1.30551	1.68830	2.02809	2.43449	2.71948	3.33262
37	0.68118	1.30485	1.68709	2.02619	2.43145	2.71541	3.32563
38	0.68100	1.30423	1.68595	2.02439	2.42857	2.71156	3.31903
39	0.68083	1.30364	1.68488	2.02269	2.42584	2.70791	3.31279
40	0.68067	1.30308	1.68385	2.02108	2.42326	2.70446	3.30688

Table 2 is a T table that will be used as a basis for comparison of t-count which determines the significance of the method using Best Practice Layer 2 Security for remote Vocational Education. The table reading uses DK or degrees of freedom which is read by reducing the value of n with the number of hypotheses. In this study, it was obtained that DK of 17 came from the data value of 19 minus 2 which symbolizes the 2-way test. To compare using the t-test, it is required to compare the t value in the table and the t value from the calculation if the results are obtained t-count < t-tabel then H0 is accepted and H1 rejected. To determine t count First, we need to calculate the standard deviation. The standard deviation formula can be seen in formula 1 and formula t count listed in formula 2.

$$s = \sqrt{\frac{1}{n-1}\left\{\sum D^2 - \frac{(\sum D)^2}{n}\right\}} \quad (1)$$

$$t = \frac{\frac{\sum D}{n}}{\frac{s}{\sqrt{n}}} \quad (2)$$

There is 2 hypothesis in this research H0 is there is no significance after implementing a new system and H1 is there is significance. 2 hypotheses will be analyzed in two way better or not

Conclusion

For the summary in before and after there is margin of summary, before shown 71,842 and before give 80,684 so there is the better value from the summary. T-count has been calculated from S in formula 1 gives 9,651 so t-count gives 3,99375 as result. In this case, H0 rejected and adopted H1 that implemeting a new system is significant so this system is smooth can be implemented.

References

Cusack, B., & Lutui, R. (2015). Innovating additional layer 2 security requirements for a protected stack. *Aust. Inf. Secur. Manag. Conf. 2015*, 81–86, 2015, doi: 10.4225/75/57b69e28d938f.

Data, M. (2016). Perancangan mobile virtual computer laboratory untuk kegiatan praktikum mahasiswa ilmu komputer. *Semin. Nas. Ris. Terap., 1*, 180–188.

Mangut, H. A., Al-Nemrat, A., Benzaïd, C., & Tawil, A. R. H. (2015). ARP cache poisoning mitigation and forensics investigation. *Proc. - 14th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. Trust., 1*(8), 1392–1397, 2015, doi: 10.1109/Trustcom.2015.536.

Mehra, R., & Krishnan, K. V. (2018). Analyzing security attack on layer 2 and comparing the performance of different routing protocols. *3rd IEEE Int. Conf. Recent Trends Electron. Inf. Commun. Technol. RTEICT 2018 - Proc.*, 611–616. doi: 10.1109/RTEICT42901.2018.9012126.

Pilamunga, N., Mantilla, C., Arellano, A., Vaca, B., & Mendez, P. (2018). Security policies to mitigate attacks VLAN hopping in the data link layer of LA networks. *KnE Engineering, 3*(9), 111. doi: 10.18502/keg.v3i9.3649.

Richardson, R. (2003). CSI/FBI 2003 computer crime and security survey. *Comput. Secur. J.*, 19(2), 21–40.

Website:

Configuring VM Networking on a Hyper-V NAT Switch | Petri IT Knowledgebase." https://petri.com/configuring-vm-networking-hyper-v-nat-switch (accessed Oct. 08, 2021).

CVE-1999-1129: Cisco Catalyst 2900 Virtual LAN (VLAN) switches allow remote attackers to inject 802.1q frames into another VLAN by forg." https://www.cvedetails.com/cve/CVE-1999-1129/ (accessed Aug. 20, 2021).

Switches - Cisco Nexus 1000V Switch for Microsoft Hyper-V - Cisco." https://www.cisco.com/c/en/us/support/switches/nexus-1000v-switch-microsoft-hyper-v/series.html (accessed Aug. 23, 2021).

Yersinia | Penetration Testing Tools." https://tools.kali.org/vulnerability-analysis/yersinia (accessed Aug. 20, 2021).