خبرنامه الکترونیکی ۶۷

مرکز تخصصی آپا دانشگاه سمنان

شماره شصت و هفتم، سال ششم، دی ۱۴۰۲ | کاری از تیم تولید محتوای مرکز تخصصی آپا دانشگاه سمنان

در این شماره می‌خوانید:

آموزش حمله‌ی پرش VLAN با پروتکل DTP و ابزار yersinia

https://cert.semnan.ac.ir info.cert@semnan.ac.ir 023-31535019 @semcert

مرکز آپا دانشگاه سمنان

سیستم دفاعی بدنِ هر کسب و کاری

امنیت اطلاعات

آن کسب و کار است...

فهرست

خبر

آموزش

مرکز آپا دانشگاه سمنان

خبر

کشف آسیب‌پذیری در Github

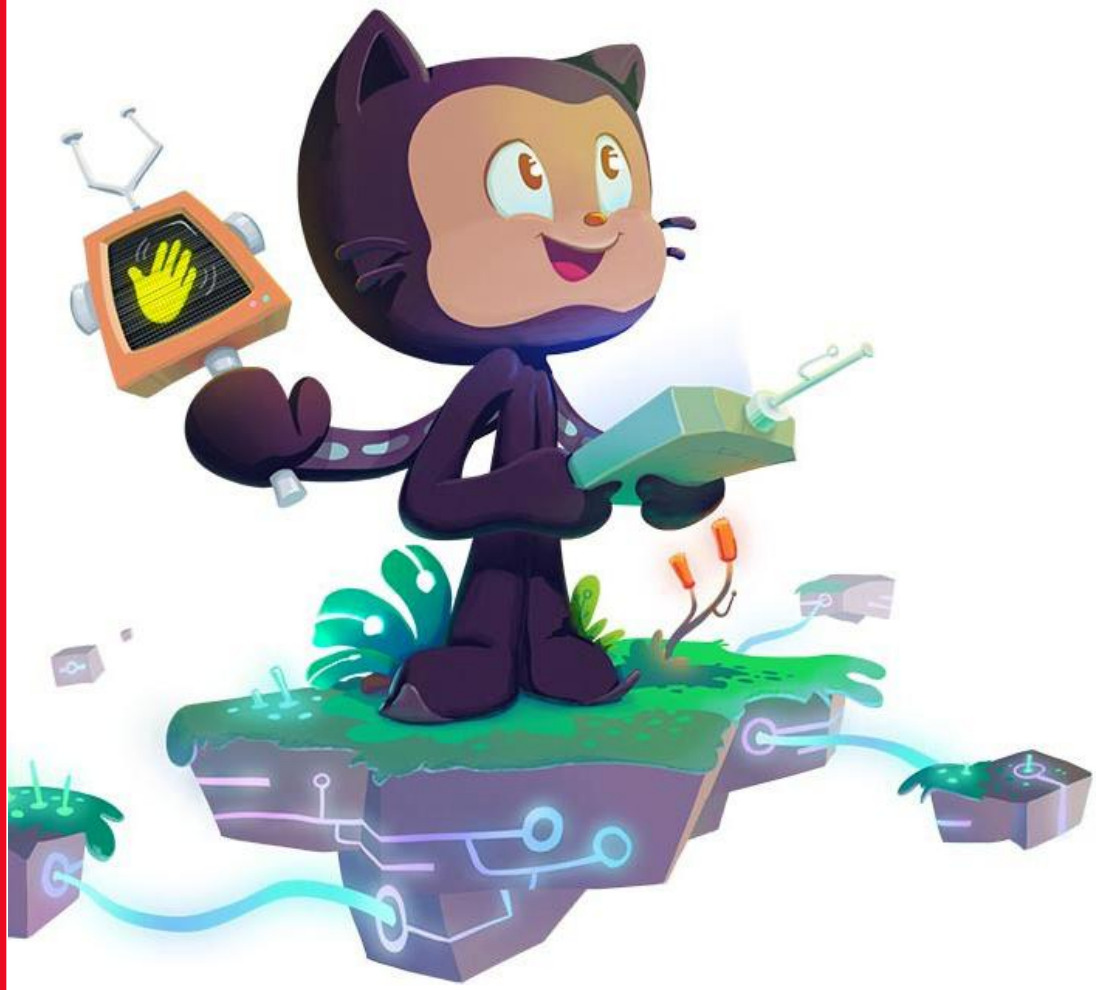
یک آسیب‌پذیری با شناسه CVE-2024-0200 و شدت CVSS score: 7.2 در سرور GitHub Enterprise کشف شده است که به مهاجمان دسترسی غیرمجاز و اجرای کد از راه دور را می‌دهد. برای بهره‌برداری از این نقص امنیتی، یک مهاجم باید به حسابی با نقش مالک سازمان (سطح دسترسی خیلی بالا) به حساب کاربری خود وارد شود. بر اساس بردار حمله این آسیب‌پذیری (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:L/A:L)
بهره‌برداری از طریق شبکه خارجی و از راه دور امکان‌پذیر است (AV:N)، نیازمند پیش‌زمینه‌ای نمی‌باشد و به‌راحتی قابل تکرار است (AC:H)، مهاجم برای انجام حمله نیاز به حساب‌کاربری با سطح دسترسی بالا دارد (PR:H)، به تعامل با کاربر نیز نیاز ندارد (UI:N)، بهره‌برداری از نقص امنیتی مذکور بر سایر منابع امنیتی تأثیر می‌گذارد (S:C) و با بهره‌برداری از آن، یک ضلع از سه ضلع امنیت با شدت زیادی تحت تأثیر قرار می‌گیرند.

محصولات تحت تأثیر

این آسیب‌پذیری تمامی نسخه‌های قبل از 3.12 سرور GitHub Enterprise را تحت تأثیر قرار می‌دهد.

توصیه‌های امنیتی

GitHub این نقص امنیتی را در نسخه‌های 3.8.13, 3.9.8, 3.10.5 و 3.11.3 سرور GitHub Enterprise رفع کرده‌است و اعمال سریع وصله‌های امنیتی جهت کاهش مخاطرات احتمالی، بسیار مهم می‌باشد.



امکان دسترسی غیرمجاز در گوگل!

محققان امنیتی اخیراً یک نقص امنیتی مهم را در گوگل کشف کرده‌اند که به مهاجمان اجازه می‌دهد بدون نیاز به رمز عبور، به حساب‌های گوگل افراد دسترسی پیدا کنند. این نقص از یک آسیب‌پذیری در پروتکل احراز هویت دو مرحله‌ای گوگل[1] ناشی می‌شود. در این حمله، آن‌ها ابتدا یک وب‌سایت مخرب ایجاد می‌کنند که می‌تواند کوکی‌های شخص ثالث را در مرورگر کاربران ذخیره کند، سپس قربانیان را فریب می‌دهند تا از آن وب‌سایت بازدید کنند. هنگامی که قربانی از وب‌سایت مخرب بازدید می‌کند، مهاجم می‌تواند کوکی‌های شخص ثالث را از مرورگر قربانی بدست آورد. این کوکی‌ها حاوی اطلاعات احراز هویت کاربر، از جمله رمز عبور و کد تأیید هویت دو مرحله‌ای هستند. با داشتن این اطلاعات، آن‌ها می‌توانند به حساب‌های گوگل قربانی دسترسی پیدا کنند، حتی اگر قربانی رمز عبور خود را تغییر داده باشد.

در صورت موفقیت‌آمیز بودن عملیات، این حمله یک تهدید جدی برای کاربر به شمار می‌آید، زیرا به مهاجم امکان می‌دهد بدون هیچ مشکلی به اطلاعات شخصی کاربران، از جمله ایمیل‌ها، مخاطبین، عکس‌ها، فیلم‌ها، و سایر اطلاعات دسترسی پیدا کند. وی همچنین می‌تواند از این اطلاعات برای اهداف مجرمانه، مانند کلاهبرداری، سرقت هویت، یا انتشار اطلاعات حساس، سوءاستفاده کند.

توصیه‌های امنیتی

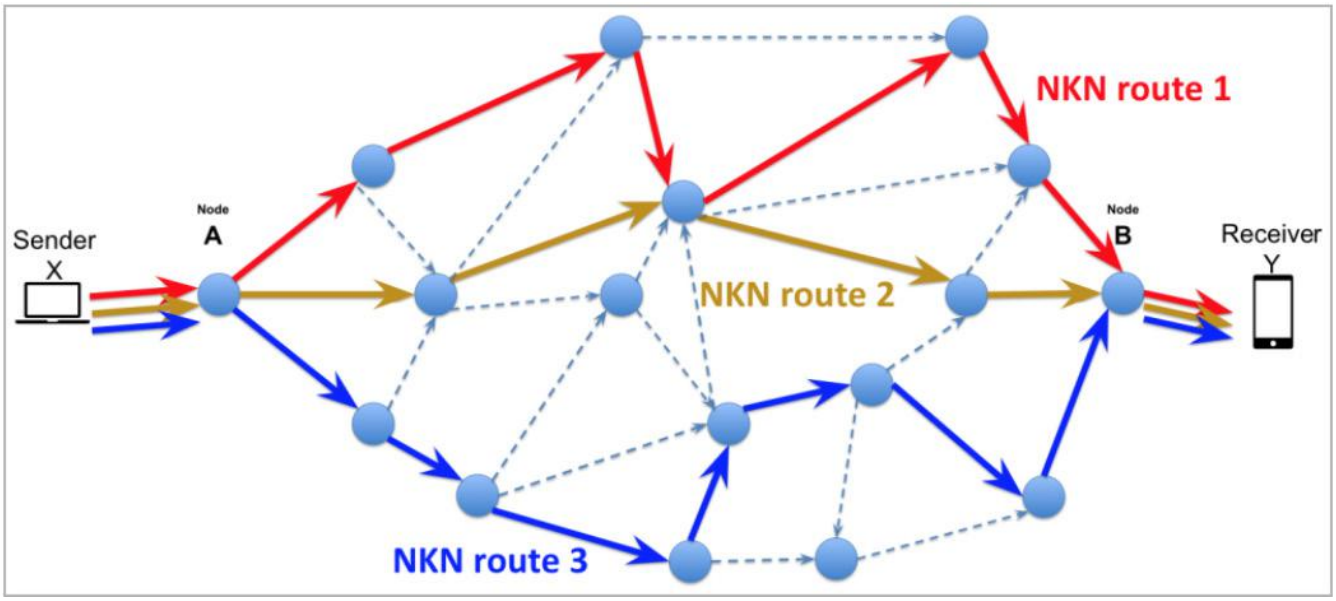
کاربران باید به طور مداوم اقداماتی جهت حذف هرگونه بدافزار از رایانه خود انجام دهند. این اقدامات می‌تواند شامل موارد زیر باشد:

- استفاده از یک برنامه آنتی‌ویروس یا ضد بدافزار معتبر جهت اسکن رایانه به طور منظم.
- حذف هرگونه نرم‌افزار یا برنامه مشکوک از رایانه.

1-OAuth2

کشف بدافزار مخرب NKAbuse

یک بدافزار مخرب چندپلتفرمی با زبان برنامه‌نویسی Go به نام "NKAbuse"، به‌عنوان اولین بدافزار مخرب استفاده‌کننده از تکنولوژی NKN (New Kind of Network) جهت تبادل اطلاعات شناسایی شده است و این امر آن را به یک تهدید پنهان برای کاربران تبدیل کرده است. NKN یک پروتکل نسبتاً جدید از شبکه peer-to-peer غیرمتمرکز است که از تکنولوژی blockchain برای مدیریت منابع و ایجاد یک مدل امن و شفاف در عملیات شبکه استفاده می‌کند. یکی از اهداف NKN بهینه‌سازی سرعت انتقال داده و تاخیر در سراسر شبکه است که با محاسبه مسیرهای کارآمد برای انتقال بسته‌های داده، قابل دستیابی می‌باشد.



انتقال داده‌ها از طریق NKN

اصلی‌ترین هدف این بدافزار مخرب، سیستم‌های لینوکسی می‌باشد. حمله NKAbuse با بهره‌گیری از یک آسیب‌پذیری قدیمی در Apache Struts با شناسه CVE-2017-5638 برای حمله به یک شرکت مالی استفاده شده است. اگرچه اکثر حملات به کامپیوترهای لینوکس متمرکز هستند، این نرم‌افزار مخرب می‌تواند دستگاه‌های اینترنت اشیاء را دربرگیرد و از معماری‌های MIPS، ARM و 386 پشتیبانی کند.

NKAbuse از تکنولوژی NKN به عنوان ابزاری جهت اجرای حملات DDoS[1] استفاده می‌کند و احتمال دارد به دلیل استفاده از یک پروتکل نوآورانه تشخیص داده نشود. این تهدید از پروتکل عمومی blockchain NKN به عنوان ابزاری جهت انجام یک مجموعه گسترده از حملات flood-ing به عنوان یک backdoor در سیستم‌های لینوکس استفاده می‌کند. همچنین، بدافزار با استفاده از پروتکل NKN[2] با مهاجمان ارتباط برقرار می‌کند تا اطلاعات را ارسال و دریافت کند.

دستورات حمله ارسال شده توسط سرور کنترل و فرمان (C2)، شامل انواع حملات شبکه از جمله TCP، HTTP، ICMP، PING، UDP و SSL می‌باشد. این حملات با هدف تخریب ساختار شبکه و ایجاد اختلال یا حمله منع سرویس[3] انجام می‌شود. در جدول زیر لیستی از دستورات حمله آورده شده است:

1- حمله منع سرویس توزیع‌شده
2- New Kind of Network
3- Denial of Service

دستور	حمله
Default/0	http_flood_HTTPGetFloodPayload
۱	http_flood_HTTPPostFloodPayload
۲	tcp_flood_TCPFloodPayload
۳	udp_flood_UDPFloodPayload
۴	ping_flood_PINGFloodPayload
۵	tcp_syn_flood_TCPSynFloodPayload
۶	ssl_flood_SSLFloodPayload
۷	http_slowloris_HTTPSlowlorisPayload
۸	http_slow_body_HTTPSlowBodyPayload
۹	http_slow_read_HTTPSlowReadPayload
۱۰	icmp_flood_ICMPFloodPayload
۱۱	dns_nxdomain_DNSNXDOMAINPayload

دستورات حمله DDo

بدافزار مذکور علاوه بر قابلیت‌های DDoS، می‌تواند به عنوان یک تروجان دسترسی از راه دور[1] عمل کند که این امکان را به اپراتورهای خود می‌دهد تا اجرای دستورات، انتقال داده را انجام داده و از صفحه نمایش عکس بگیرند.

1-RAT

کشف آسیب‌پذیری در سرورهای SSH لینوکس

سرورهای SSH لینوکس یک هدف مورد توجه برای حملات سایبری می‌باشند. این پروتکل جهت مدیریت و نگهداری سرورها ضروری است، همچنین می‌تواند برای دسترسی غیرمجاز به سرور استفاده شود. مهاجمان برای حمله به سرورهای SSH لینوکس، مراحل زیر را دنبال می‌کنند:

1. شناسایی سرورها: اولین قدم، شناسایی سرورهای SSH لینوکس است. مهاجمان می‌توانند این کار را با اسکن IP انجام دهند. اسکن IP به مهاجمان اجازه می‌دهد تا تمام سرورهایی که پورت SSH را روی آن‌ها باز کرده‌اند، شناسایی کنند.
2. جمع‌آوری مجوزها و اطلاعات حساب: پس از شناسایی سرورها، مهاجمان باید مجوزها و اطلاعات حساب SSH را برای دسترسی به آن‌ها جمع‌آوری کنند. مهاجمان می‌توانند این کار را با استفاده از حملات brute-force انجام دهند.
   - حملات brute-force از مجموعه بزرگی از کلمات از پیش تعریف شده به عنوان رمزهای عبور احتمالی استفاده و تمام ترکیبات ممکن از رمزهای عبور را امتحان می‌کنند تا زمانی که رمز عبور صحیح پیدا شود.
3. نصب ابزارها: پس از اینکه مهاجم به سرور دسترسی پیدا کرد، ابزارهای مورد نیاز جهت انجام حمله را نصب می‌کنند. این ابزارها می‌توانند برای اهداف مختلفی مانند حدس زدن مجوزها و اطلاعات حساب، انتخاب سرورهای دیگر و راه‌اندازی استخراج ارز دیجیتال و حملات DDoS استفاده شوند.

مهاجمان می‌توانند از سرورهای SSH لینوکس برای اهداف مختلفی استفاده کنند. برخی از اهداف رایج عبارتند از:

- سرقت اطلاعات: مهاجمان می‌توانند از سرورهای SSH جهت سرقت اطلاعات حساس مانند اطلاعات مشتری، اطلاعات مالی یا اسرار تجاری استفاده کنند.
- انتشار بدافزار: مهاجمان می‌توانند از سرورهای SSH جهت انتشار بدافزار مانند ویروس‌ها، کرم‌ها و تروجان‌ها استفاده کنند.
- حملات DDoS: مهاجمان می‌توانند از سرورهای SSH جهت انجام حملات DDoS استفاده کنند که به طور عمدی ترافیک شبکه را مسدود می‌کنند تا وب سایت‌ها یا خدمات آنلاین را از دسترس خارج کنند.

توصیه‌های امنیتی

جهت محافظت از سرورهای SSH لینوکس در برابر حملات سایبری، می‌توان اقدامات زیر را انجام داد:

- استفاده از رمزهای عبور قوی: یک رمز عبور قوی باید حداقل 12 کاراکتر داشته باشد و شامل ترکیبی از حروف بزرگ، حروف کوچک، اعداد و نمادها باشد.
- تغییر پورت SSH: پورت پیش فرض SSH 22 است. تغییر پورت SSH می تواند از حملات brute force جلوگیری کند زیرا مهاجمان باید پورت جدید را نیز اسکن کنند.
- غیرفعال کردن ورود غیرمجاز کاربر با دسترسی root: کاربر با دسترسی root دارای بیشترین دسترسی در سیستم است و غیرفعال کردن ورود با دسترسی root می‌تواند از دسترسی غیرمجاز مهاجمان به سیستم جلوگیری کند.
- استفاده از فایروال: فایروال می‌تواند جهت مسدود کردن ترافیک غیرمجاز به سرور استفاده شود.

چه مدت طول می‌کشد رمز عبور شما بشکند؟

طول رمز (کاراکتر)	فقط عدد	ترکیب حروف بزرگ و کوچک	ترکیب اعداد و حروف بزرگ و کوچک	ترکیب اعداد و حروف بزرگ و کوچک و نمادها
۳	فوری	فوری	فوری	فوری
۴	فوری	فوری	فوری	فوری
۵	فوری	فوری	۳ ثانیه	۱۰ ثانیه
۶	فوری	۸ ثانیه	۳ دقیقه	۱۳ دقیقه
۷	فوری	۵ دقیقه	۳ ساعت	۱۷ ساعت
۸	فوری	۳ ساعت	۱۰ روز	۵۷ روز
۹	۴ ثانیه	۴ روز	۱۵۳ روز	۱۲ سال
۱۰	۴۰ ثانیه	۱۶۹ روز	۱ سال	۹۲۸ سال
۱۱	۶ دقیقه	۱۶ سال	۱۰۶ سال	۷۱ هزار سال
۱۲	۱ ساعت	۶۰۰ سال	۶ هزار سال	۶ میلیون سال
۱۳	۱۱ ساعت	۲۱ هزار سال	۱۰۸ هزار سال	۴۲۳ میلیون سال
۱۴	۴ روز	۷۷۸ هزار سال	۲۵ میلیون سال	۵ میلیارد سال
۱۵	۴۶ روز	۲۸ میلیون سال	۱ میلیارد سال	۲ تریلیون سال
۱۶	۱ سال	۱ میلیارد سال	۹۷ میلیارد سال	۱۹۳ تریلیون سال
۱۷	۱۲ سال	۳۶ میلیارد سال	۶ تریلیون سال	۱۴ کوآدریلیون سال
۱۸	۱۲۶ سال	۱ تریلیون سال	۳۷۴ تریلیون سال	۱ کوینتیلیون سال

مرکز آپا دانشگاه سمنان

آموزش

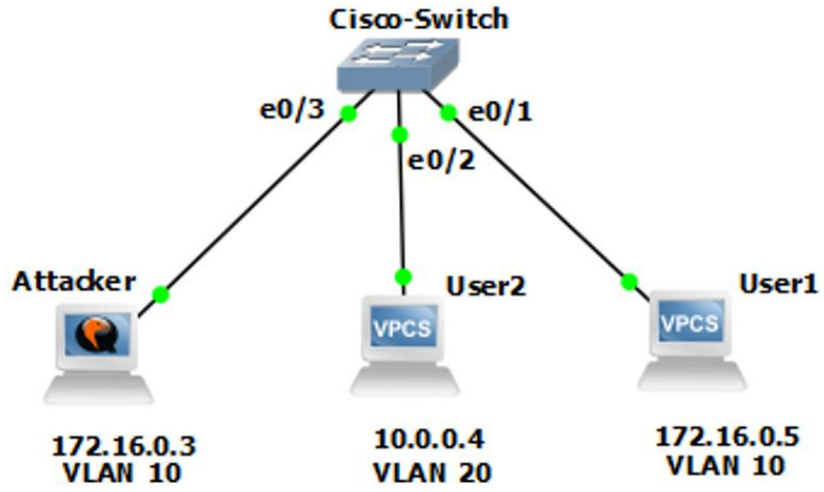
آموزش حمله‌ی پرش VLAN با پروتکل DTP و ابزار yersinia

در این سناریوی آموزشی قصد داریم نحوه‌ی حمله به پروتکل DTP[1] را با استفاده از ابزار yersinia آموزش دهیم. از پروتکل DTP برای خودکار سازی ارتباط Trunk استفاده می‌شود. پس از پیکربندی VLAN[2] ها، برای انتقال ترافیک بین دو سوییچ که دارای VLANهای مختلفی هستند از درگاه Trunk استفاده می‌شود، این درگاه با کپسوله‌سازی[3] بسته، آن را منتقل می‌کند. به کمک پروتکل DTP دو سوییچ سیسکو بر سر ایجاد ارتباط Trunk و روش کپسوله‌سازی آن با یکدیگر مذاکره می‌کنند و در نتیجه Access و یا Trunk بودن ارتباط توافق می‌شود که باتوجه به ترکیب و حالت درگاه‌های شرکت کننده در مذاکره، نتیجه‌ی آن متفاوت خواهد بود. جدول 1 حالات مختلف درگاه‌های شرکت کننده و نتایج آن را به نمایش می‌گذارد.

	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic Auto	Access	Trunk	Trunk	Access
Dynamic Desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	Limited connectivity
Access	Access	Access	Limited connectivity	Access

جدول ۱: حالات توافقی DTP

برای انجام حمله‌ی پرش VLAN با استفاده از ابزار yersinia، ابتدا سناریوی رسم شده در شکل 1 را در نرم‌افزار GNS3 رسم می‌کنیم و مطابق با آن، واسط[4] های مسیریاب‌ها و کارت شبکه‌ی کامپیوترها را آدرس‌دهی می‌کنیم. همان‌طور که در شکل 1 روشن است سیستم‌های Attackrt و User1 در یک VLAN قرار دارد و مهاجم قصد پرش از VLAN و دسترسی به سیستم User2 که در VLAN دیگری است را دارد.



شکل ۱: سناریوی پیاده‌سازی پروتکل DTP

1- Dynamic Trunking Protocol
2- Virtual LAN
3- Encapsulation
4- Interface

برای پیکربندی حالات مختلف DTP در حالت پیکربندی رابط[1]، یکی از دستورات زیر را وارد می‌نماییم.

```
Switch(config-if)# switchport mode dynamic desirable
Switch(config-if)# switchport mode dynamic auto
```

دستورات بالا دو حالت مختلف پیکربندی DTP را نمایش می‌دهد. درگاهی که در حالت dynamic desirable تنظیم شده باشد شروع کننده‌ی مذاکره بوده و اقدام به ارسال بسته‌ی DTP می‌کند و باتوجه به حالتی که رابط مقابل در آن قرار دارد سعی در ایجاد ارتباط Trunk دارد همچنین درگاهی که در حالت dynamic auto قرار گرفته باشد به صورت غیرفعّال برای دریافت بسته‌ی DTP گوش می‌دهد و خود را با آن وفق می‌دهد. این پروتکل به صورت پیش‌فرض بر روی درگاه سوییچ‌های سیسکو فعال بوده و در حالت dynamic auto قرار دارد. پس از آدرس‌دهی به سیستم‌ها پیکربندی‌های زیر را در Cisco_Switch وارد می‌نماییم.

```
Switch> enable
Switch# configure terminal
Switch(config)# interface Ethernet0/1
Switch(config-if)# switchport access vlan 10
Switch(config-if)# exit
Switch(config)# interface Ethernet0/2
Switch(config-if)# switchport access vlan 20
Switch(config-if)# exit
Switch(config)# interface Ethernet0/3
Switch(config-if)# switchport access vlan 10
```

پس از واردکردن دستورات فوق درگاه متصل به سیستم User1 و Attacker عضو VLAN 10 شده و درگاه متّصل به کامپیوتر User2 در VLAN 20 قرار می‌گیرد و با دستور show interface status از عضویت آنها اطمینان می‌یابیم (شکل 2).

```
switch#show interface status

Port      Name               Status       Vlan       Duplex  Speed Type
Et0/0                        connected    1            auto   auto unknown
Et0/1                        connected    10           auto   auto unknown
Et0/2                        connected    20           auto   auto unknown
Et0/3                        connected    10           auto   auto unknown
Et1/0                        connected    1            auto   auto unknown
```

شکل ۲: نمایش عضویت رابط‌ها در VLAN

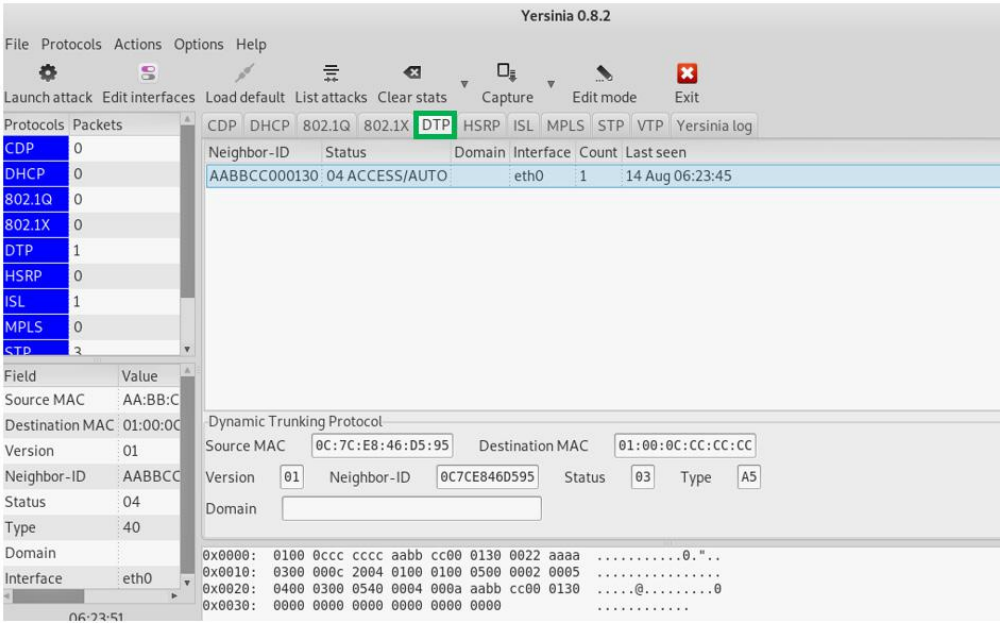
در Cisco_Switch، با واردکردن دستور show interfaces ethernet 0/3 switchport در محیط Privileged EXEC، می‌توانید از پیکربندی DTP در آن درگاه آگاه شوید (شکل 3).

```
switch#show interfaces ethernet 0/3 switchport
Name: Et0/3
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 10 (VLAN0010)
Trunking Native Mode VLAN: 1 (default)
```

شکل ۳: نمایش تنظیمات DTP

1- Interface Configuration

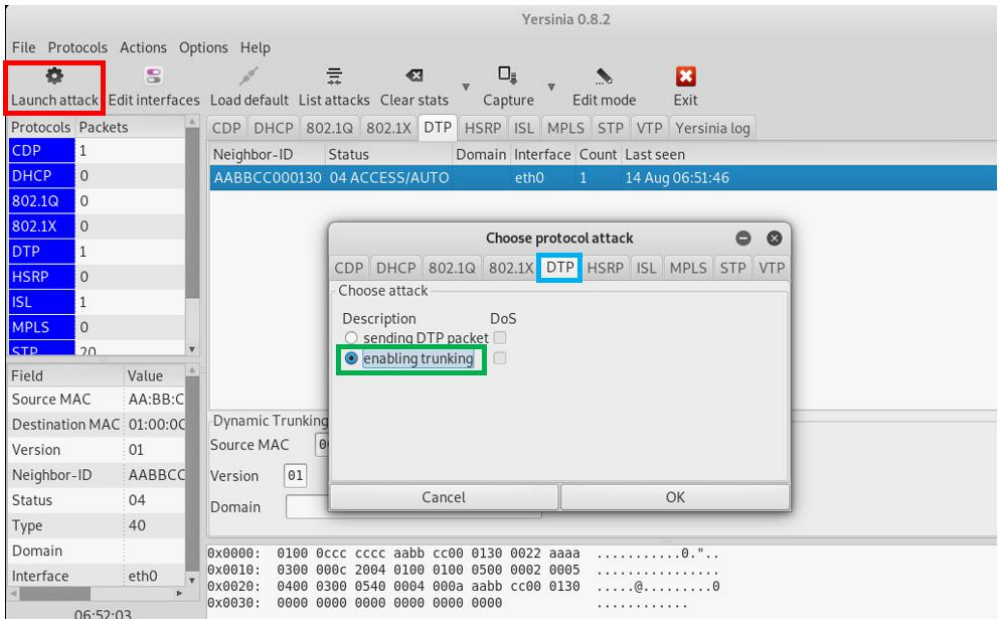
همچنین با دستور debug dtp event می‌توانیم رخدادهای dtp را مشاهده کنیم. برای انجام حمله‌ی پرش VLAN، کافی است مهاجم درگاه سوییچ را که به سیستم خود متصل است به حالت Trunk برگرداند، به این ترتیب قادر به عبور از VLANها و دسترسی به دستگاه‌های دیگر است. برای انجام این حمله، در سیستمی که در شکل 1، Attacker نام‌گذاری شده، نرم‌افزار yersinia را اجرا کرده و به سراغ زبانه‌ی DTP می‌رویم.



شکل ٤: انتخاب زیانه‌ی DTP در نرم‌افزار yersinia

به محض ورود به زبانه‌ی DTP، نرم‌افزار yersinia اقدام به دریافت بسته‌های DTP ارسال شده می‌کند. همانطور که در شکل٤ مشاهده می‌کنید، نرم‌افزار درگاهی که از آن بسته را دریافت نموده، نوع ارتباط سوییچ مقابل و نوع پیکربندی DTP خود را نشان داده است.

با انتخاب هر یک از سطرهای این لیست و فشردن دکمه‌ی Launch attack که در شکل ۵ با کادر قرمز مشخص شده است و سپس رفتن به زبانه‌ی DTP و انتخاب حمله‌ی enabling trunking اقدام به ارسال بسته‌ی DTP می‌کند. با انجام این حمله توافق برای ارتباط Trunk شروع می‌شود (شکل ۵).



شکل ۵: انتخاب زیانه‌ی DTP در نرم‌افزار yersinia

با آغاز حمله در سوییچ دستور debug dtp event را دوباره وارد می‌نماییم (شکل ٦).

```
switch#debug dtp event
*Aug 14 07:17:00.292: DTP-queue:Et0/3:Queuing DTP packet ../dyntrk/dyntrk_process.c:1365
*Aug 14 07:17:00.293: DTP-pkt:Et0/3:Good DTP packet received: ../dyntrk/dyntrk_core.c:1500
*Aug 14 07:17:00.293: DTP-pkt:Et0/3:  Domain:  ../dyntrk/dyntrk_core.c:1503
*Aug 14 07:17:00.293: DTP-pkt:Et0/3:  Status: TOS/TAS = ACCESS/DESIRABLE ../dyntrk/dyntrk_core.c:1505
*Aug 14 07:17:00.293: DTP-pkt:Et0/3:  Type: TOT/TAT = 802.1Q/802.1Q ../dyntrk/dyntrk_core.c:1507
*Aug 14 07:17:00.293: DTP-pkt:Et0/3:  ID: 0C7CE846D595 ../dyntrk/dyntrk_core.c:1510
*Aug 14 07:17:00.293: DTP-decision:Et0/3:old NS/NT = 0x00/0x01
 ../dyntrk/dyntrk_core.c:677
```

شکل ٦: دریافت بسته‌های DTP بعد از آغاز حمله توسط نرم‌افزار yersinia

بادقّت در شکل 6 در می‌یابیم که مهاجم بسته‌ی DTP را ارسال کرده و درگاه خود و نوع پیکربندی DTP خود را به ترتیب Access و Desirable معرفی می‌کند. همچنین نوع کپسوله‌سازی ارتباط 802.1q تعیین می‌شود. بدین ترتیب نوع ارتباط به Trunk تغییر می‌کند. برای مشخص شدن نوع ارتباط مجدداً دستور show interface status را وارد می‌کنیم، باتوجه به جدول VLAN نمایش داده شده ارتباط درگاه Et0/3 به Trunk تغییر یافته است (شکل 7).

```
switch#show interfaces status

Port      Name               Status       Vlan       Duplex  Speed Type
Et0/0                        connected    1            auto   auto unknown
Et0/1                        connected    10           auto   auto unknown
Et0/2                        connected    20           auto   auto unknown
Et0/3                        connected    trunk        auto   auto unknown
Et1/0                        connected    1            auto   auto unknown
```

شکل ۷: نمایش تغییر نوع ارتباط به Trunk

با کمک دستور show interfaces ethernet 0/3 trunk، VLANهایی که اجازه‌ی عبور از درگاه Trunk را دارند نمایش داده می‌شود و سیستمی که می‌خواهیم به آن دست‌یابیم در VLAN دیگری قرار دارد (شکل 8).

```
switch#show interfaces ethernet 0/3 trunk

Port        Mode             Encapsulation  Status        Native vlan
Et0/3       auto             n-802.1q       trunking      1

Port        Vlans allowed on trunk
Et0/3       1-4094

Port        Vlans allowed and active in management domain
Et0/3       1,10,20
```

شکل ۸: نمایش VLANهای مجاز برای عبور از درگاه Trunk

حال با Trunk شدن درگاه سوییچ، برای انتقال ترافیک به سیستم مورد نظر نیاز به برچسب‌گذاری بسته‌ها با VLAN 20 می‌باشد، برای دستیابی به این امر از ماژول 8021q استفاده می‌نماییم. سپس برای قرارگیری در شبکه‌ی قربانی، از آدرسی هم محدوده با شبکه‌ی قربانی استفاده می‌کنیم پس درگاهی مجازی ایجاد کرده و آن را آدرس‌دهی می‌کینم (شکل ۱۰).

```
root@semcert:~# modprobe 8021q
root@semcert:~# vconfig add eth0 20
Added VLAN with VID == 20 to IF -:eth0:-
root@semcert:~# ifconfig eth0.20 up
root@semcert:~# ifconfig eth0.20 10.0.0.6 up
```

شکل ۹: پیکربندی VLAN20 در سیستم مهاجم

بدین ترتیب مهاجم با تغییر نوع ارتباط و سپس پیکربندی VLAN به شبکه‌ی قربانی نفوذ کرده و دسترسی کاملی را می‌یابد (شکل 11).

```
root@semcert:~# ping 10.0.0.4
PING 10.0.0.4 (10.0.0.4) 56(84) bytes of data.
64 bytes from 10.0.0.4: icmp_seq=1 ttl=64 time=1.09 ms
64 bytes from 10.0.0.4: icmp_seq=2 ttl=64 time=1.18 ms
64 bytes from 10.0.0.4: icmp_seq=3 ttl=64 time=1.11 ms
64 bytes from 10.0.0.4: icmp_seq=4 ttl=64 time=1.26 ms
```

شکل ۱۰: دسترسی به شبکه User2

همان‌طور که مشاهده کردید با وجود کاربردهای فراوانی که VLAN در شبکه‌های امروزی دارند و امنیت ظاهری که برای ما فراهم می‌سازند، بسیار شکننده است. برای جلوگیری از حمله‌ی پرش VLAN یا کاهش آسیب آن می‌توان اقدامات زیر را انجام داد:

- این حمله در صورتی آغاز می‌شود که درگاه متصل به مهاجم یا در حالت Trunk قرار بگیرد. برای غیرفعال‌سازی DTP از دستور switchport nonegotiate استفاده نمایید.
- درگاه‌های بدون استفاده را خاموش کرده و آنها را در VLAN بلا استفاده‌ای عضو نمایید.

تلاش ما
حفظ امنیت
شماست...