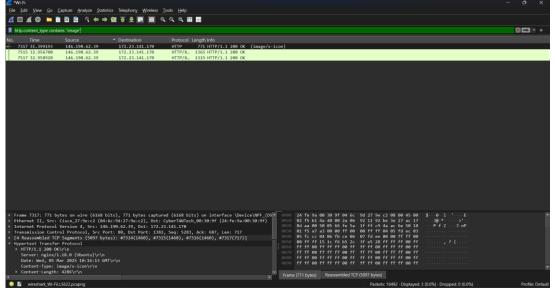


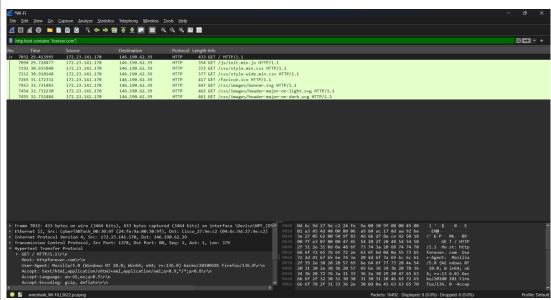
فرم گزارش کار آزمایشگاه شبکه



| - 4 | نام و شماره | 40133014 | شماره دانشجویی | حسين تاتار | نام ونام |
|---|--|--|--|----------------------------------|-----------|
| تحليل http با | آزمایش | | | | خانوادگی |
| استفاده از نرم افزار | | | | | |
| WireShark | | | | | |
| VIIICOIIUIK | | | | | |
| چگونگی استفاده از Wireshark برای ضبط و تحلیل ترافیک HTTP برای درک ارتباطات | | | | | هدف |
| | | | | | _ |
| وب، شناسایی مشکلات امنیتی احتمالی و بررسی ناهنجاریهای ترافیک شبکه | | | | | آزمایش |
| نصب Wireshark روی سیستم شما | | | | | ابزارهای |
| یک مرورگر وب برای ایجاد ترافیک HTTP | | | | | مورد نياز |
| سوال 1: چند نمونه از فیلترهای دیگر را مشخص کرده و توضیح دهید که برای چه کاری استفاده می شوند. | | | | | |
| | | | | جواب: | |
| #WAG | | ىخص كرده ايم: | نه از این فیلتر هارا مش | در اینجا سه نمو | |
| Elle Edit View Go Capture Analyze Statistics Telephony V | | | | | |
| ■ http:// htt | Protocol Length Info | | | ⊠C3 · + | |
| 13153 54.108175 172.23.141.77 239.255.251 13231 55.132707 172.23.141.77 239.255.251 13238 56.157635 172.23.141.77 239.255.251 13254 57.079633 172.23.141.77 239.255.251 | 5.250 SSDP 217 M-SEARCH * HTTI | P/1.1 P/1.1 P/1.1 P/1.1 | | | |
| 19 4.835846 172.23.142.239 239.255.255 27 5.858185 172.23.142.239 239.255.255 36 5.979562 172.23.142.239 239.255.255 | 5.250 SSDP 217 M-SEARCH * HTTI 5.250 SSDP 217 M-SEARCH * HTTI 5.250 SSDP 217 M-SEARCH * HTTI | P/1.1 P/1.1 P/1.1 | | | |
| 93 7.054989 172.23.142.239 239.255.25! 754 10.691933 172.23.143.238 239.255.25! 816 11.714220 172.23.143.238 239.255.25! 971 12.739801 172.23.143.238 239.255.25! | 5.250 SSDP 217 M-SEARCH * HTTI 5.250 SSDP 217 M-SEARCH * HTTI | | | | |
| L 1859 13.763832 172.23.143.238 239.255.25 | 5.250 SSDP 217 M-SEARCH * HTTI | P/1.1 | | | |
| | | | | | شرح |
| | | | | | آزمایش |
| | | | | | |
| | | | | | |
| > Frame 1859: 217 bytes on wire (1736 bits), 217 bytes > Ethernet II, Src: ASUSTekCOMPU_77:c3:44 (2c:56:dc:77 > Internet Protocol Version 4, Src: 172.23.143.238, Ds | :c3:44), Dst: IPv4mcast_7f:ff:fa (01:00 | | dc 77 c3 44 98 99 45 99 | . i | |
| User Datagram Protocol, Src Port: 61909, Dst Port: 1 Simple Service Discovery Protocol M-SEARCH * HTTP/1.1\r\n | 990 | 0030 43 48 20 2a 20 48 54 54 0040 4f 53 54 3a 20 32 33 39 0050 2e 32 35 30 3a 31 39 30 | 50 2f 31 2e 31 0d 0a 48 CH * HTT P/1.1 1 2e 32 35 35 2e 32 35 35 OST: 239 .255.25 30 0d 0a 4d 41 4e 3a 20 .250:190 0 MAN: | 5 | |
| HOST: 239.255.255.258:1900\r\n MMN: "ssdp:discover"\r\n MX: 1\r\n | | 0070 0a 4d 58 3a 20 31 0d 0a 0080 64 69 61 6c 2d 6d 75 6c 0090 2d 6f 72 67 3a 73 65 72 | 73 63 67 76 65 72 22 8d "ssdp:di scover" 53 54 3a 20 75 72 6e 3a MX: 1 ST: urn 74 69 73 63 72 65 65 6e Mail-mul tiscree 76 69 63 65 3a 64 69 61 org:ser vice:di | : n | |
| ST: urn:dial-multiscreen-org:service:dial:1\r\n USER-AGENT: Google Chrome/109.0.5414.120 Windows\ Www.wishark.Wi-FiLLS622.pcapng | r\n | 00a0 6c 3a 31 0d 0a 55 53 45 20 47 6f 6f 67 6c 65 20 | 52 2d 41 47 45 4e 54 3a 1:1 USE R-AGENT 43 68 72 6f 6d 65 2f 31 Google Chrome/: Packets: 16492 - Displayed: 12 (0.1%) - Dropped: 0 (0 | : 1 1.0%) Profile: Default | |
| توضیح :این فیلتر فقط ترافیک HTTP را نشان میدهد که از مرورگر Chrome ارسال شده است. | | | | | |
| کاربرد : زمانی که میخواهید تحلیل کنید کدام کاربران از مرورگر Chrome استفاده میکنند. | | | | | |



توضیح :این فیلتر فقط ترافیک HTTP را که شامل محتوای تصویری مانند JPEG, PNG و غیره نشان میدهد. کاربرد :زمانی که میخواهید تحلیل کنید کدام تصاویر در حال بارگیری هستند.



توضیح: این فیلتر فقط ترافیک HTTP را نشان می دهد که مربوط به میزبان "forever.com" (Host) است. کاربرد: زمانی که می خواهید فقط ترافیک مربوط به یک دامنه خاص را مشاهده کنید، مثلاً برای تحلیل ترافیک یک وبسایت خاص.

سوال 2: چند نمونه از هدرهای HTTP دیگر را بررسی و به طور کامل توضیح دهید.به طور مثال E-tag : جواب:

: Accept

توضیح: این هدر مشخص می کند که کلاینت (مرورگر) چه نوع محتوایی را میتواند دریافت کند. این میتواند شامل انواع MIME مانند text/html، application

· Accent . Ilia

text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8

: Accept-Language

توضیح: این هدر زبانهای ترجیحی کلاینت را مشخص می کند. سرور می تواند از این اطلاعات برای ارائه محتوای مناسب به زبان مورد نظر استفاده کند.

: Accept-Language مثال

en-US,en;q=0.5

: Authorization

توضیح: این هدر برای ارسال اطلاعات احراز هویت به سرور استفاده می شود. این می تواند شامل توکنهای Bearer

: Authorization مثال

Bearer <token>

: ETag

توضیح: ETag مخفف (Entity Tag) یک هدر HTTP است که برای مدیریت کش (Cache) و اعتبار سنجی منابع استفاده می شود. این هدر توسط سرور به یک منبع (مانند یک فایل، تصویر، یا صفحه وب) اختصاص داده می شود و به کلاینت (مرورگر یا کاربر) اجازه می دهد تا بررسی کند که آیا نسخه ای از منبع که در کش ذخیره شده است، هنوز معتبر است یا خیر.

: ETag مثال

ETag: "63754f44-63"\r\n

سوال 3: کدهای 3x,4x,5x را با جزییات بررسی کرده و علت وقوع هرکدام را توضیح دهید.

جواب:

کدهای 3x (هدایتها):

این کدها نشاندهنده این هستند که کلاینت باید اقدامات بیشتری انجام دهد تا درخواست را کامل کند. معمولاً این اقدامات شامل ریدایرکت (هدایت) به یک URL دیگر است.

- :301 Moved Permanently .1
- توضیح: این کد نشاندهنده این است که منبع درخواست شده به طور دائم به یک URL
 جدید منتقل شده است.
 - علت وقوع: تغییر دائمی آدرس یک صفحه وب.

:302 Found .2

- و توضیح: این کد نشان دهنده این است که منبع به طور موقت به یک URL جدید منتقل شده است.
 - o علت وقوع: تغییر موقت آدرس یک صفحه وب.

:304 Not Modified .3

- توضیح: این کد نشاندهنده این است که منبع از زمان آخرین درخواست تغییر نکرده است و کلاینت میتواند از نسخه کش شده استفاده کند.
 - و علت وقوع: استفاده از کش برای کاهش بار سرور و بهبود عملکرد.

کدهای 4x (خطاهای کلاینت):

این کدها نشاندهنده این هستند که خطایی در سمت کلاینت رخ داده است و سرور نمیتواند درخواست را پردازش کند.

:400 Bad Request .1

- توضیح: این کد نشاندهنده این است که درخواست کلاینت نامعتبر یا ناقص است.
 - علت وقوع:فرمت نادرست درخواست، پارامترهای نامعتبر.

:401 Unauthorized .2

توضیح: این کد نشاندهنده این است که کلاینت باید خود را احراز هویت کند تا به منبع
 دسترسی پیدا کند.

o علت وقوع :عدم ارائه اطلاعات احراز هویت یا اطلاعات نامعتبر.

:403 Forbidden .3

- و توضیح: این کد نشاندهنده این است که کلاینت مجوز دسترسی به منبع درخواست شده را ندارد.
 - o علت وقوع: محدودیتهای دسترسی، ممنوعیت دسترسی به منبع.

:404 Not Found .4

- o توضیح: این کد نشان دهنده این است که منبع درخواست شده یافت نشده است.
 - علت وقوع URL :نامعتبر، حذف شدن منبع.

کدهای 5x (خطاهای سرور):

این کدها نشاندهنده این هستند که خطایی در سمت سرور رخ داده است و سرور نمیتواند درخواست معتبر کلاینت را پردازش کند.

:500 Internal Server Error .1

- توضیح: این کد نشاندهنده این است که سرور با یک شرایط غیرمنتظره مواجه شده است
 که مانع از انجام درخواست می شود.
 - o علت وقوع:خطاهای داخلی سرور، مشکلات در کد سرور.

:502 Bad Gateway .2

- توضیح : این کد نشان دهنده این است که سرور به عنوان یک گیتوی یا پروکسی، پاسخ نامعتبری از سرور بالادستی دریافت کرده است.
 - علت وقوع: مشكلات در ارتباط بين سرورها، سرور بالادستي در دسترس نيست.

:503 Service Unavailable .3

- توضیح :این کد نشاندهنده این است که سرور موقتاً قادر به پردازش درخواست نیست، معمولاً به دلیل overload یا تعمیرات.
 - علت وقوع: ترافیک زباد، تعمیرات سرور.

:504 Gateway Timeout .4

- توضیح : این کد نشان دهنده این است که سرور به عنوان یک گیتوی یا پروکسی، در زمان
 مشخص شده پاسخی از سرور بالادستی دریافت نکرده است.
 - علت وقوع : زمان بندى پاسخ سرور بالادستى، مشكلات شبكه.

سوال 4: سه نمونه از حملات که از طریق Payload انجام میشود را توضیح دهید؛ مثلا Sql injection. **جواب:**

۱- Command Injection (تزریق دستور):

توضیح : در این حمله، مهاجم یک دستور مخرب را در Payload ارسال می کند تا آن را در سیستم عامل سرور اجرا کند. این حمله معمولاً زمانی اتفاق می افتد که ورودی کاربر به درستی اعتبارسنجی نشده باشد.

; Is -la; echo "Hacked"

- این Payload دستور ls -la را اجرا می کند تا لیست فایل ها و دایرکتوری ها را نمایش دهد
 و سپس پیام "Hacked" را چاپ می کند.
 - اثرات : اجراي دستورات دلخواه روى سرور، سرقت اطلاعات، حذف يا تغيير فايلها.

۲- SQL Injection (تزریق SQL):

• توضیح : در این حمله، مهاجم یک Payload حاوی دستورات SQL مخرب را به پایگاه داده ارسال می کند تا دسترسی غیرمجاز به داده ها یا تغییر آن ها را امکانپذیر کند.

' OR '1'='1

 این Payload باعث می شود کوئری SQL همیشه true برگرداند و مهاجم بتواند به تمام دادههای جدول دسترسی پیدا کند.

۳- (Cross-Site Scripting (XSS) (اسکربیتنویسی بین سایتها):

• توضیح :در این حمله، مهاجم یک Payload حاوی کدهای JavaScript مخرب را در یک وبسایت تزریق میکند. وقتی کاربران دیگر این صفحه را باز میکنند، کد مخرب در مرورگر آنها اجرا می شود.

<script>alert('XSS Attack!');</script>

- o این Payload یک پیام هشدار (alert) در مرورگر کاربر نمایش میدهد.
- ، علت وقوع :عدم اعتبارسنجی و escape کردن ورودیهای کاربر در وبسایت.
- اثرات این نوع حمله سرقت کوکیها، جعل هویت، تغییر محتوای صفحه، ریدایرکت کاربران به سایتهای مخرب.

سوال 5: استخراج داده های حساس از HTTP.

جواب:

حال در Wireshark، از فیلتر زیر استفاده میکنیم تا فقط درخواستهای POST را مشاهده کنیم: http.request.method == "POST"

سپس می توانیم جزئیات درخواست را بررسی کرده و نام کاربری و رمز عبور را در بخش Form Data مشاهده کنیم مانند تصویر زیر:

