بسمه‌تعالی

دانشگاه صنعتی اصفهان
دانشکده مهندسی برق و کامپیوتر
آزمایشگاه شبکه

زمستان ۱۴۰۳

دکتر فانیان، دکتر حیدرپور

مقدمات شبکه، پروتکل‌ها، wireshark و مجازی‌سازی

فهرست مطالب

عنوان	صفحه
فهرست مطالب	۲
۱ هدف آزمایش	۳
۲ مدیریت تنظیمات شبکه (با استفاده از GUI)	۳
۲-۱ گام اول: بررسی آدرس‌ها	۳
۲-۲ گام دوم: اشتراک‌گذاری فایل	۳
۳ بررسی اطلاعات شبکه (از طریق خط فرمان)	۳
۳-۱ گام سوم: بررسی اطلاعات شبکه از طریق خط فرمان	۳
۳-۲ گام چهارم: تست ارتباطات شبکه	۳
۴ دستورات کاربردی شبکه	۴
۴-۱ گام پنجم: بررسی مسیرها و تحلیل ارتباطات	۴
۴-۲ گام ششم: تنظیمات پیشرفته‌ی شبکه (امتیازی)	۴
۴-۳ گام هفتم: تنظیمات اضافی شبکه	۴
۵ تحلیل ترافیک شبکه با Wireshark	۵
۵-۱ گام هفتم: بررسی ترافیک شبکه	۵

۱ هدف آزمایش

در این آزمایش سعی داریم با کنترل شبکه‌ی هر کدام از ماشین‌ها، دستورات کاربردی شبکه در سیستم‌عامل لینوکس آشنا شویم.

۲ مدیریت تنظیمات شبکه (با استفاده از GUI)

۲-۱ گام اول: بررسی آدرس‌ها

- آدرس سیستم و Gateway را از طریق تنظیمات شبکه مشاهده کنید.
- مشخص کنید این آدرس‌ها مربوط به کدام کلاس IP هستند.

۲-۲ گام دوم: اشتراک‌گذاری فایل

- یک پوشه را روی سیستم خود به اشتراک بگذارید.
- فایلی با نام خود ایجاد کرده و در آن یک متن دلخواه قرار دهید.
- به پوشه‌ی به اشتراک گذاشته‌ی هم‌گروهی خود بروید و فایل داخل آن را بررسی نمایید.
- در صورت استفاده از لینوکس، می‌توانید از سرویس Samba استفاده کنید.

۳ بررسی اطلاعات شبکه (از طریق خط فرمان)

۳-۱ گام سوم: بررسی اطلاعات شبکه از طریق خط فرمان

- آدرس سیستم خود را مشاهده کنید.
- بررسی کنید که IP شما به‌صورت دستی تنظیم شده است یا اتوماتیک.
- آدرس‌های فیزیکی (MAC Address) را استخراج نمایید.

۳-۲ گام چهارم: تست ارتباطات شبکه

- کامپیوتر هم‌گروهی خود را Ping کنید و اطلاعات پاسخ‌ها را تحلیل نمایید.
- از آپشن مناسب برای Ping استفاده کنید تا فقط ۸ بسته‌ی ICMP ارسال و دریافت شود.
- صحت ارتباط خود با www.google.com را بررسی نمایید.

۴ دستورات کاربردی شبکه

۴-۱ گام پنجم: بررسی مسیرها و تحلیل ارتباطات

- با nslookup آدرس DNS سرورهای Yahoo و Google را بیابید.
- جدول ARP را نمایش داده و اطلاعات آن را تحلیل کنید.
- از دستور netstat برای مشاهده‌ی جداول Routing، وضعیت Interfaceها و پورت‌ها استفاده کنید.
- عملکرد آپشن‌های **-n**، **-p** و **-a** را بررسی کنید.
- مسیر بسته‌ها به google.com را با traceroute بررسی نمایید.

۴-۲ گام ششم: تنظیمات پیشرفته‌ی شبکه (امتیازی)

- آدرس IP سیستم خود را به‌صورت استاتیک **192.168.58.3** تنظیم کنید.
- یک IP جدید از DHCP Server دریافت کنید.
- DNS Server خود را به **18.72.0.3** تغییر دهید.
- یک DNS Server جدید از DHCP بخواهید.
- با استفاده از hping۳ سه بسته که فلگ‌های ACK، SYN، FIN آنها ۱ باشد را بر روی پورت و آدرس دلخواه ارسال نمایید. (برای بررسی پورت‌های باز از nmap استفاده کنید.) (امتیازی)

۴-۳ گام هفتم: تنظیمات اضافی شبکه

- جدول مسیریابی سیستم خود را بررسی نموده و خروجی آن‌را تحلیل فرمایید.
- با استفاده از دستور **route**، دروازه‌ی پیش‌فرض (**gateway default**) سیستم را به آدرس **192.168.1.10** تنظیم نموده و سپس با استفاده از دستور مناسب این تغییر را مشاهده نمایید.
- با دستور مناسب IP خود را به حالت قبل بر گردانید تا ارتباط شما با سیستم مجاور بر قرار باشد
- فرض کنید می‌خواهیم سناریوی شبکه به گونه‌ای باشد که دسترسی شما به سیستم مجاور برقرار نباشد؛ با استفاده از دستور **route** این سناریو را ایجاد نمایید.

۵ تحلیل ترافیک شبکه با Wireshark

۵-۱ گام هفتم: بررسی ترافیک شبکه

- کش سیستم و مرورگر خود را پاک کنید.
- آدرس فرستنده‌ی DNS Query و پاسخ‌های دریافتی را مشاهده کنید.
- نوع پروتکل (TCP / UDP) در بسته‌های DNS را تحلیل کنید.
- بررسی کنید مرورگر از کدام نسخه‌ی HTTP استفاده می‌کند.
- عملیات Three-Way Handshake را تحلیل کنید.
- فقط بسته‌های ICMP را ذخیره کنید.
- با ابزار tcpdump ترافیک کارت شبکه را در فایل **traffic.pcap** ذخیره کرده و سپس در Wireshark تحلیل کنید.

خسته نباشید!