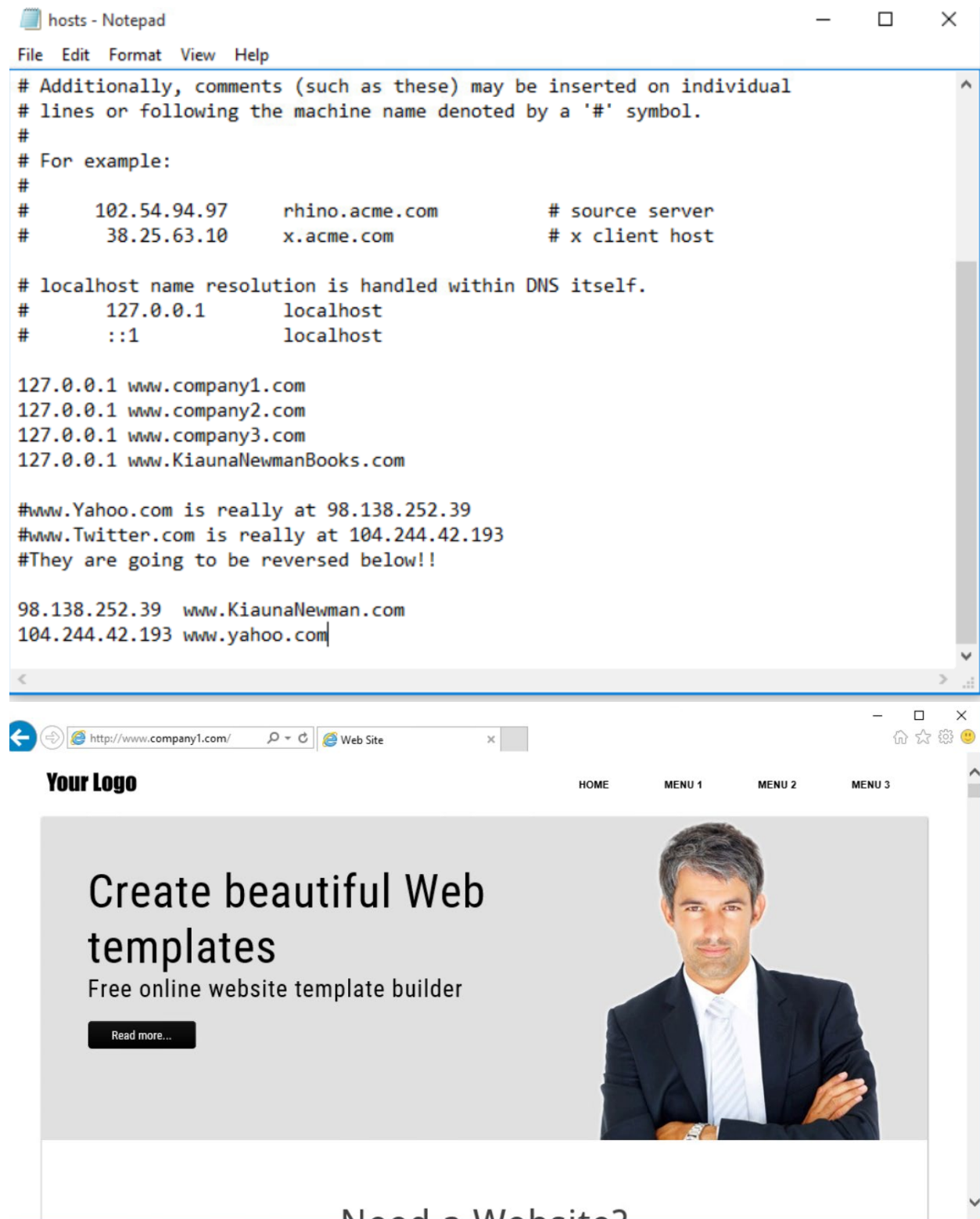


21.3 Phishing and Hosts File



The screenshot shows a Windows desktop with two windows. The top window is a Notepad application titled "hosts - Notepad". It contains the following text:

```
File Edit Format View Help
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com       # source server
#       38.25.63.10       x.acme.com          # x client host

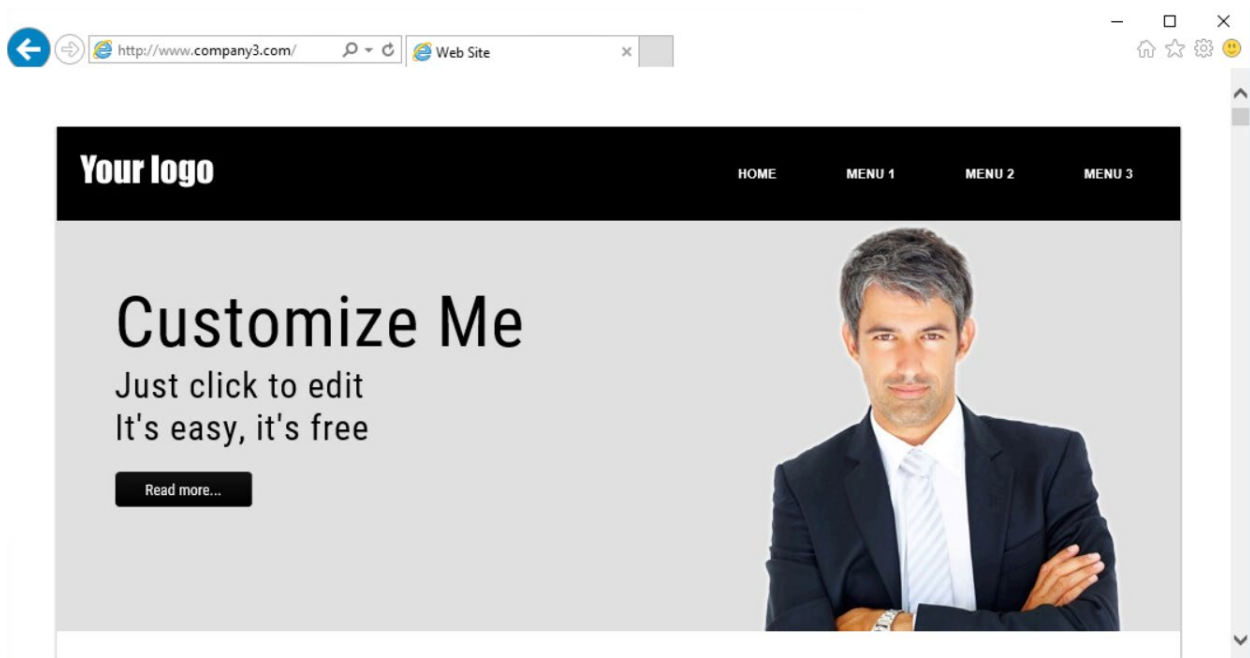
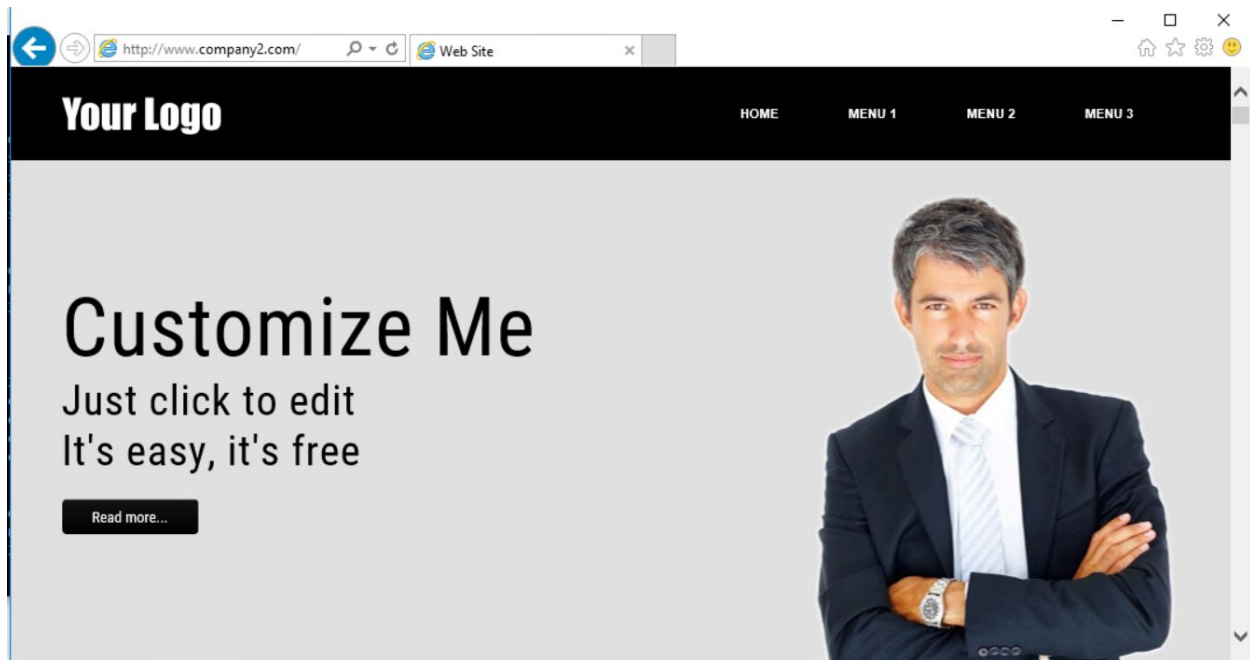
# localhost name resolution is handled within DNS itself.
#       127.0.0.1         localhost
#       ::1               localhost

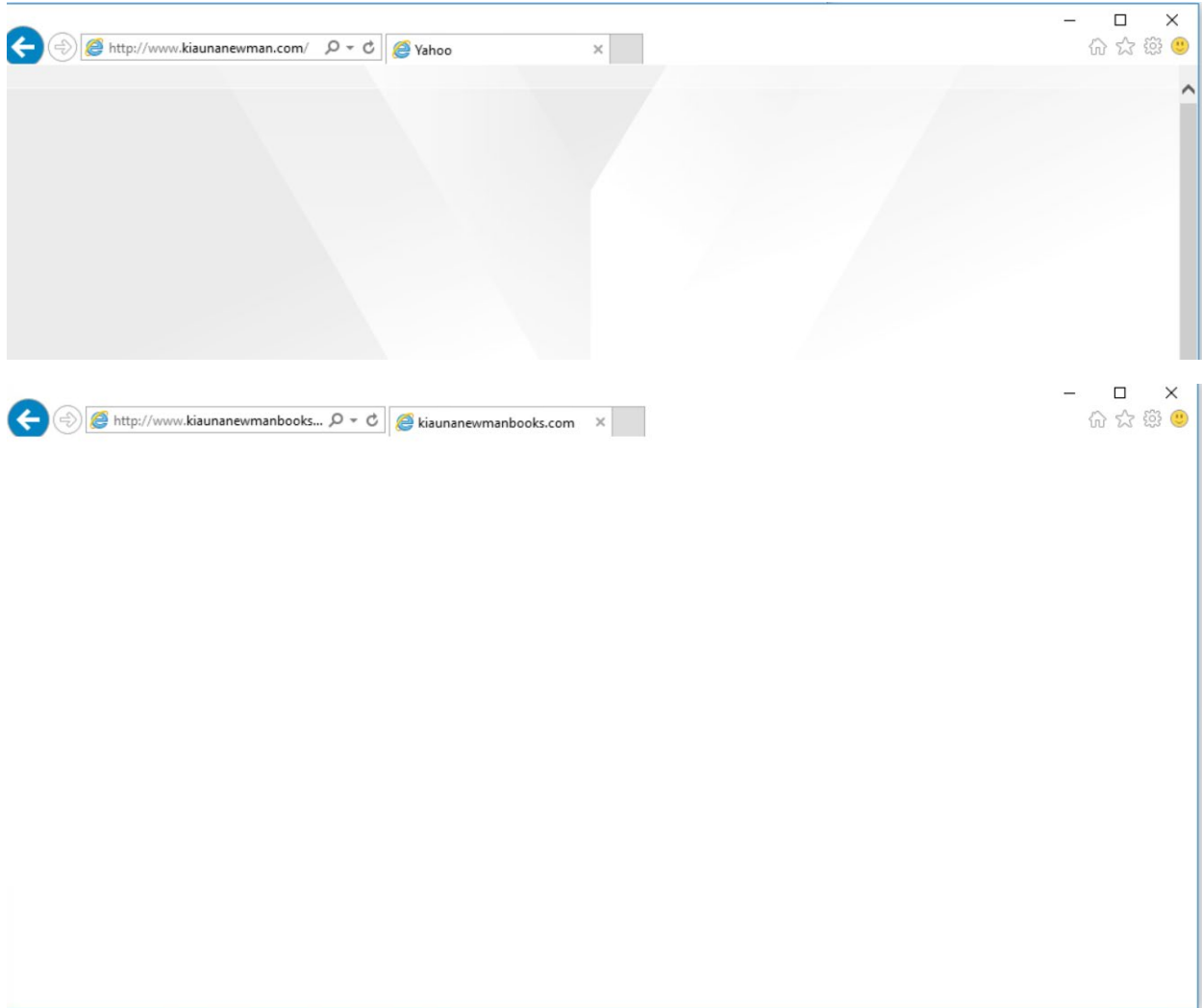
127.0.0.1 www.company1.com
127.0.0.1 www.company2.com
127.0.0.1 www.company3.com
127.0.0.1 www.KiaunaNewmanBooks.com

#www.Yahoo.com is really at 98.138.252.39
#www.Twitter.com is really at 104.244.42.193
#They are going to be reversed below!!

98.138.252.39 www.KiaunaNewman.com
104.244.42.193 www.yahoo.com
```

The bottom window is a web browser displaying a phishing website. The address bar shows "http://www.company1.com/". The website has a navigation bar with "HOME", "MENU 1", "MENU 2", and "MENU 3". The main content area features a large banner with the text "Create beautiful Web templates" and "Free online website template builder". There is a "Read more..." button. On the right side of the banner is a photo of a man in a suit. At the bottom of the page, the text "Need a Website?" is visible.







21.5 Request Filtering and Logs



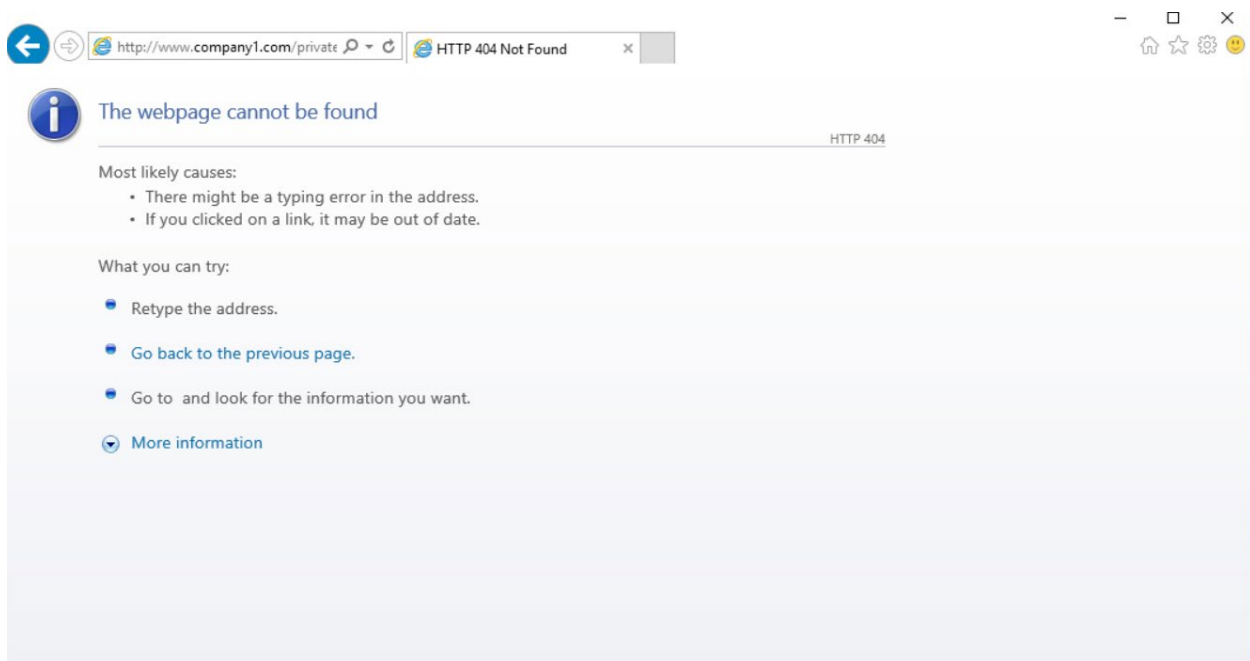
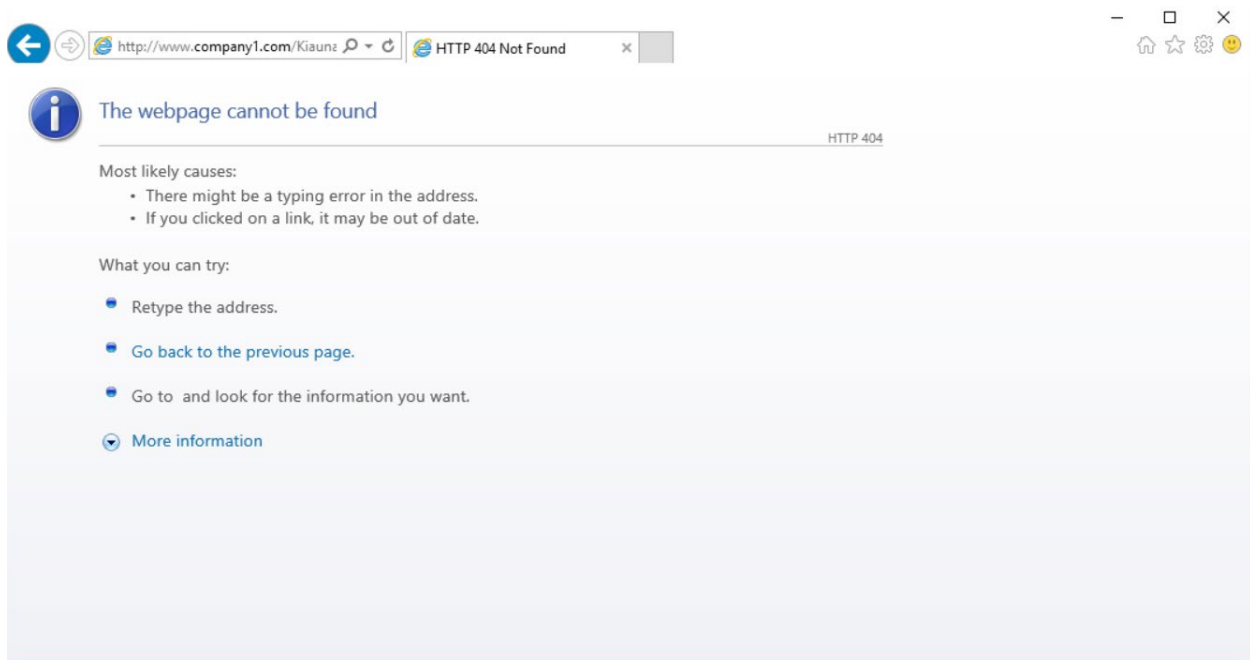
Server Error in '/' Application.

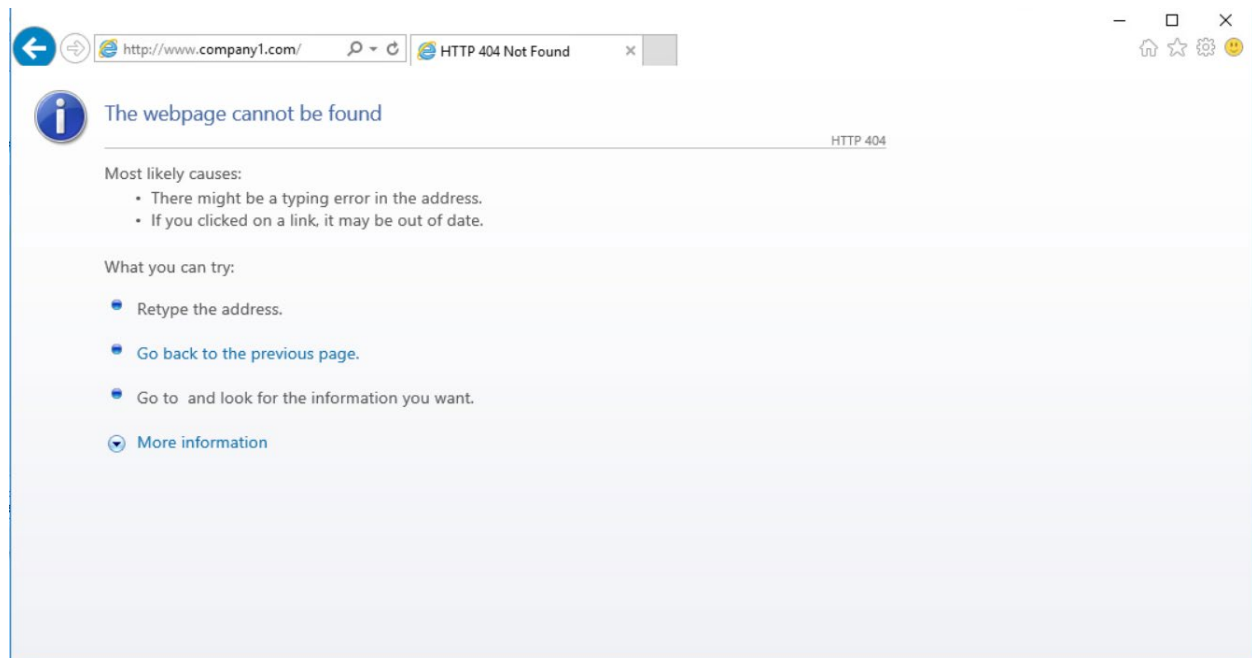
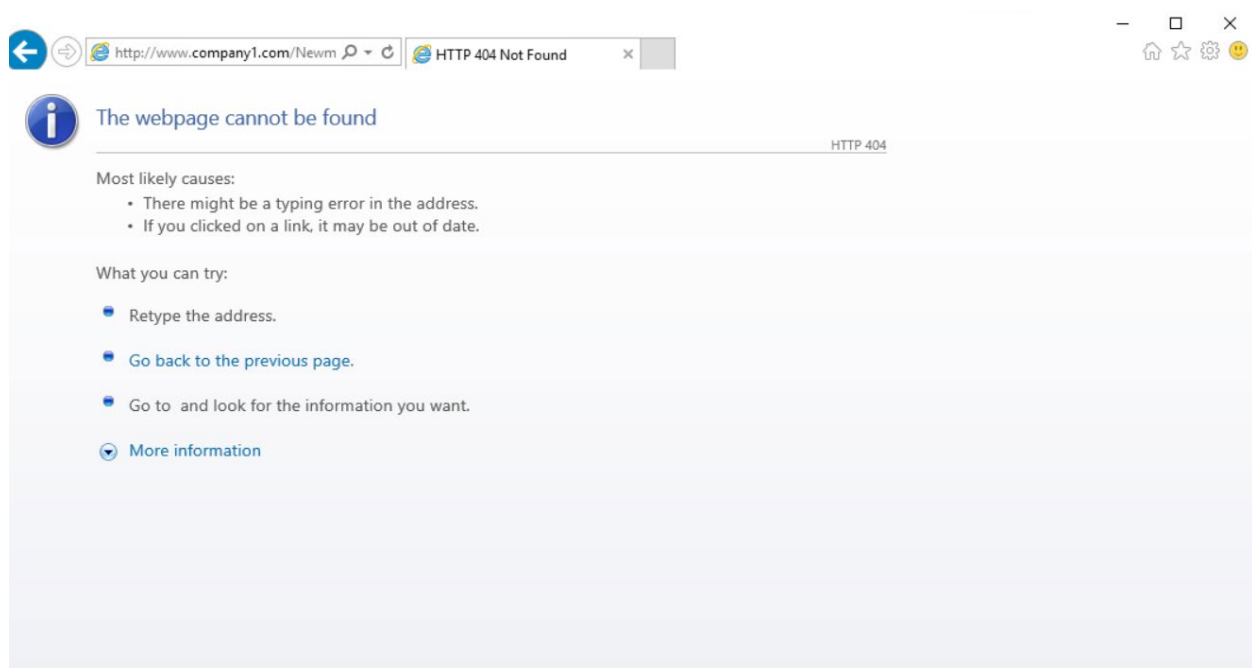
The resource cannot be found.

Description: HTTP 404. The resource you are looking for (or one of its dependencies) could have been removed, had its name changed, or is temporarily unavailable. Please review the following URL and make sure that it is spelled correctly.

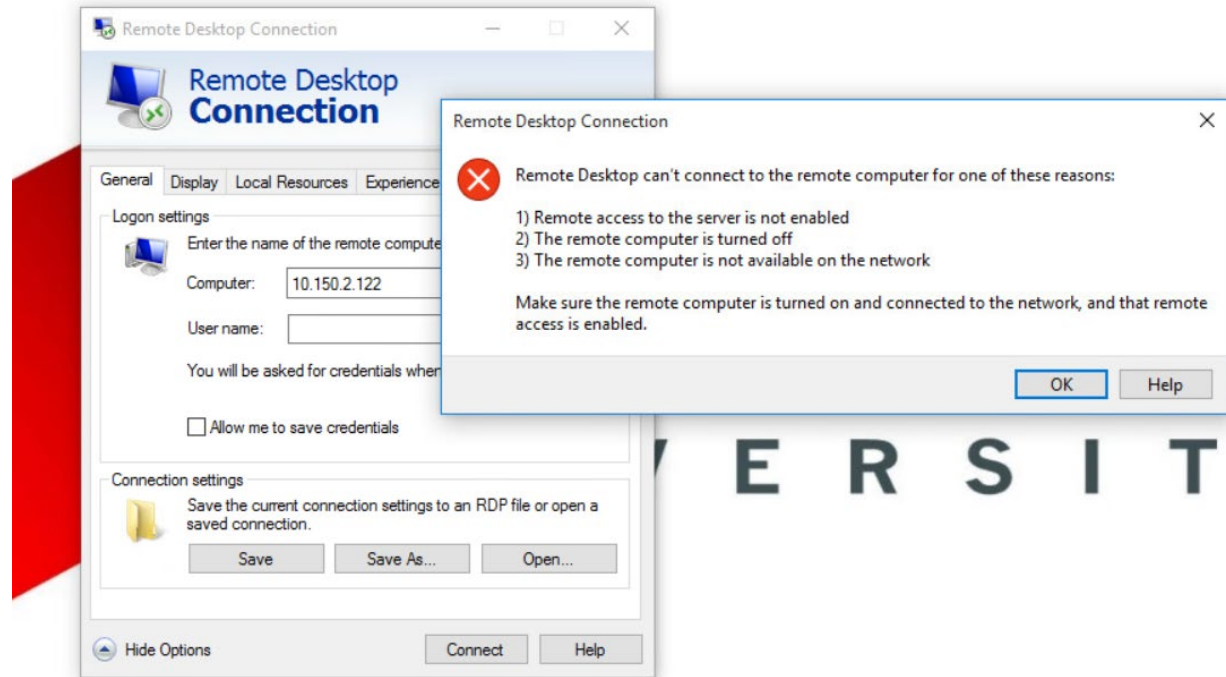
Requested URL: /KiaunaNewman...

Version Information: Microsoft .NET Framework Version:4.0.30319; ASP.NET Version:4.6.1590.0





22.2 Remote Desktop



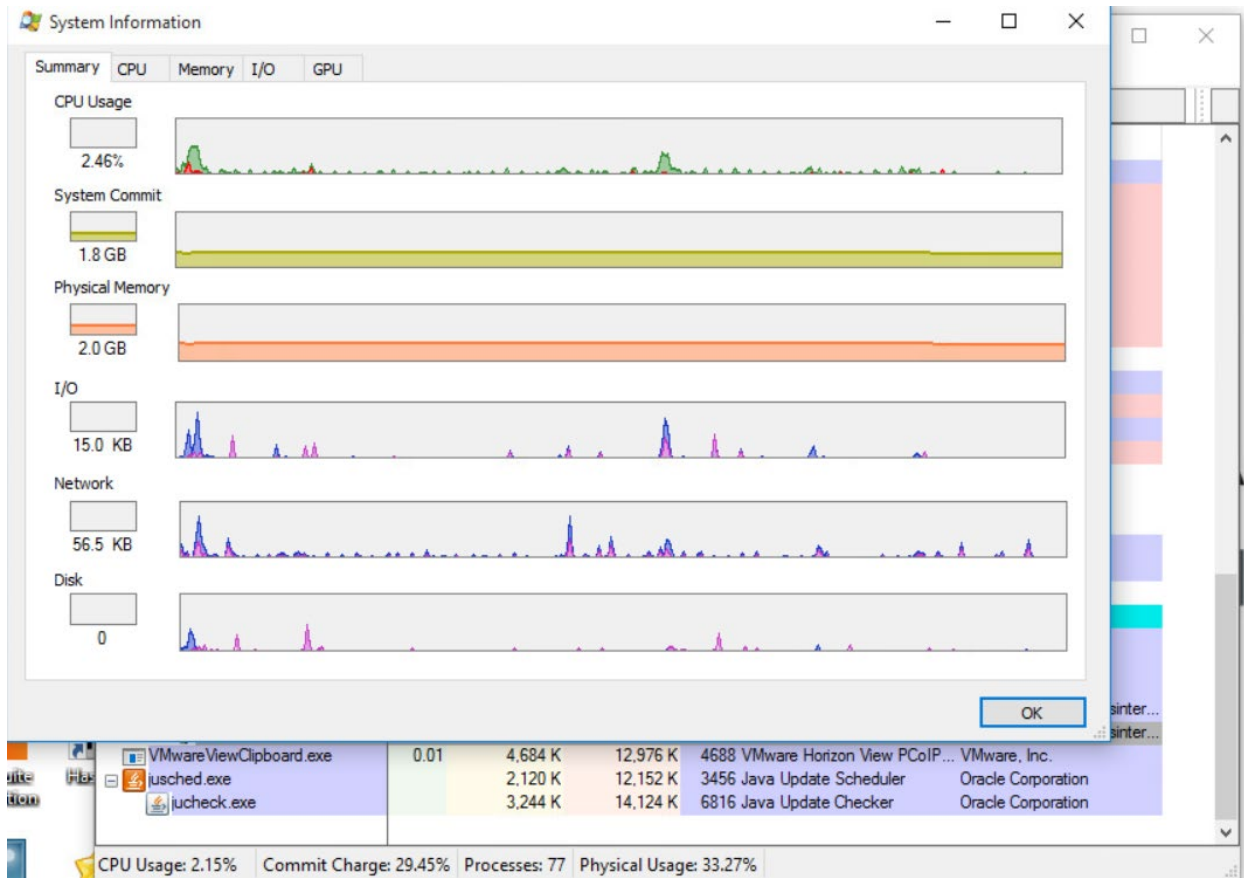
22.3 Process Explorer

Process Explorer - Sysinternals: www.sysinternals.com [MARYVILLE\knewman1]

File Options View Process Find Users Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
msdtc.exe		2,400 K	2,472 K	4012	Microsoft Distributed Transa...	Microsoft Corporation
NisSrv.exe		12,792 K	4,220 K	4856	Microsoft Network Realtime I...	Microsoft Corporation
SearchIndexer.exe		28,356 K	27,032 K	1424	Microsoft Windows Search I...	Microsoft Corporation
SearchProtocolHost.exe		1,964 K	10,084 K	4020	Microsoft Windows Search P...	Microsoft Corporation
SearchFilterHost.exe		1,252 K	6,300 K	6512	Microsoft Windows Search F...	Microsoft Corporation
svchost.exe		1,632 K	5,688 K	3132	Host Process for Windows S...	Microsoft Corporation
v4pa_agent.exe	0.01	122,348 K	77,332 K	3276	vRealize Operations for Publi...	VMware, Inc.
v4pa_Horizon_compo...		1,236 K	6,436 K	4124	vRealize Operations Horizon ...	VMware, Inc.
vmwAgent.exe		652 K	3,440 K	2192		
svchost.exe		8,492 K	18,748 K	4780	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,204 K	12,520 K	1832	Host Process for Windows S...	Microsoft Corporation
lsass.exe		6,944 K	14,576 K	668	Local Security Authority Proc...	Microsoft Corporation
csrss.exe	0.03	1,612 K	7,612 K	6224	Client Server Runtime Process	Microsoft Corporation
winlogon.exe		1,672 K	7,424 K	5348	Windows Logon Application	Microsoft Corporation
dwm.exe	0.34	35,492 K	62,948 K	6352	Desktop Window Manager	Microsoft Corporation
wssm.exe		9,088 K	18,456 K	6740	VMware Horizon View Frame...	VMware, Inc.
fontdrvhost.exe		1,116 K	3,620 K	5580	Usemode Font Driver Host	Microsoft Corporation
MpCmdRun.exe		3,864 K	11,796 K	4232	Microsoft Malware Protection...	Microsoft Corporation
explorer.exe	0.79	37,852 K	99,860 K	376	Windows Explorer	Microsoft Corporation
vmtoolsd.exe	0.03	4,184 K	14,720 K	1360	VMware Tools Core Service	VMware, Inc.
VMWVphelper.exe		1,996 K	7,448 K	6596	VMware Horizon View Perso...	VMware, Inc.
OneDrive.exe		10,464 K	33,052 K	1228	Microsoft OneDrive	Microsoft Corporation
procexp.exe		2,672 K	9,292 K	2380	Sysinternals Process Explorer	Sysinternals - www.sysinter...
procexp64.exe	0.71	15,996 K	38,204 K	5460	Sysinternals Process Explorer	Sysinternals - www.sysinter...
explore.exe	0.20	9,652 K	35,780 K	4884	Internet Explorer	Microsoft Corporation
explore.exe	2.30	99,160 K	161,968 K	6928	Internet Explorer	Microsoft Corporation
VMwareViewClipboard.exe	0.01	4,684 K	12,976 K	4688	VMware Horizon View PCoIP...	VMware, Inc.
jusched.exe		2,120 K	12,152 K	3456	Java Update Scheduler	Oracle Corporation
jucheck.exe		3,244 K	14,124 K	6816	Java Update Checker	Oracle Corporation

CPU Usage: 6.82% Commit Charge: 32.15% Processes: 81 Physical Usage: 35.91%



Process Explorer - Sysinternals: www.sysinternals.com [MARYVILLE\knewman1]

File Options View Process Find DLL Users Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
lsass.exe	< 0.01	6,644 K	14,288 K	668	Local Security Authority Proc...	Microsoft Corporation
csrss.exe	< 0.01	1,608 K	7,604 K	6224	Client Server Runtime Process	Microsoft Corporation
winlogon.exe	< 0.01	1,672 K	7,424 K	5348	Windows Logon Application	Microsoft Corporation
dwm.exe	0.04	35,500 K	54,348 K	6352	Desktop Window Manager	Microsoft Corporation
wssm.exe	0.04	9,088 K	18,456 K	6740	VMware Horizon View Frame...	VMware, Inc.
fontdrvhost.exe	0.04	1,116 K	3,588 K	5580	Usermode Font Driver Host	Microsoft Corporation
MpCmdRun.exe	0.04	3,848 K	11,784 K	4232	Microsoft Malware Protection...	Microsoft Corporation
explorer.exe	0.06	31,644 K	94,304 K	376	Windows Explorer	Microsoft Corporation
vmtoolsd.exe	0.03	4,188 K	14,724 K	1360	VMware Tools Core Service	VMware, Inc.
VMWVphelper.exe	0.03	1,996 K	7,448 K	6596	VMware Horizon View Perso...	VMware, Inc.
OneDrive.exe	0.03	10,464 K	33,052 K	1228	Microsoft OneDrive	Microsoft Corporation
procexp.exe	0.03	2,672 K	9,292 K	2380	Sysinternals Process Explorer	Sysinternals - www.sysinter...
procexp64.exe	1.30	17,448 K	40,920 K	5460	Sysinternals Process Explorer	Sysinternals - www.sysinter...

Name	Description	Company Name	Path
{6AF0698E-D558-4...			C:\ProgramData\Microsoft\Windows\Caches\{6AF0698E-D...
{AFBF9F1A-8EE8-4...			D:\Users\knewman1\AppData\Local\Microsoft\Windows\...
{DDF571F2-BE98-4...			C:\ProgramData\Microsoft\Windows\Caches\{DDF571F2-...
aclui.dll	Security Descriptor Editor	Microsoft Corporation	C:\Windows\System32\aclui.dll
aclui.dll.mui	Security Descriptor Editor	Microsoft Corporation	C:\Windows\System32\en-US\aclui.dll.mui
actxprxy.dll	ActiveX Interface Marshaling Library	Microsoft Corporation	C:\Windows\System32\actxprxy.dll
advapi32.dll	Advanced Windows 32 Base API	Microsoft Corporation	C:\Windows\System32\advapi32.dll
advapi32.dll.mui	Advanced Windows 32 Base API	Microsoft Corporation	C:\Windows\System32\en-US\advapi32.dll.mui
apphelp.dll	Application Compatibility Client Libr...	Microsoft Corporation	C:\Windows\System32\apphelp.dll
apphelp.dll.mui	Application Compatibility Client Libr...	Microsoft Corporation	C:\Windows\System32\en-US\apphelp.dll.mui
bcrypt.dll	Windows Cryptographic Primitives ...	Microsoft Corporation	C:\Windows\System32\bcrypt.dll
bcrypt.dll.mui	Windows Cryptographic Primitives ...	Microsoft Corporation	C:\Windows\System32\en-US\bcrypt.dll.mui
bcryptprimitives.dll	Windows Cryptographic Primitives ...	Microsoft Corporation	C:\Windows\System32\bcryptprimitives.dll
cfgmgr32.dll	Configuration Manager DLL	Microsoft Corporation	C:\Windows\System32\cfgmgr32.dll
clbcatq.dll	COM+ Configuration Catalog	Microsoft Corporation	C:\Windows\System32\clbcatq.dll

CPU Usage: 2.72% Commit Charge: 29.42% Processes: 76 Physical Usage: 33.27%

22.4 Change MAC Address

