

Network Pentesting

Vivek Ramachandran


SWSE, SMFE, SPSE, SISE, SLAE, SGDE Course Instructor

Certifications: <http://www.securitytube-training.com>

Pentester Academy: <http://www.PentesterAcademy.com>

Pentesting Routers: Attacking the Web Admin Interface

Vyatta Web not available in Free version


 <https://192.168.1.101/Vyatta/main.html>



The Vyatta web-based management interface is available in the Subscription Edition of the Vyatta Network OS. Please contact Vyatta if you wish to obtain a license.

Home Router Web Interface

Authentication Required

 A username and password are being requested by http://192.168.1.1. The site says: "DT 850W"

User Name:

Password:

Basic or Digest Authentication

Default Router Passwords

RouterPasswords.com

Select Router Make:

3COM

Find Password

Manufacturer	Model	Protocol	Username	Password
3COM	COREBUILDER Rev. 7000/6000/3500/2500	TELNET	debug	synnet
3COM	COREBUILDER Rev. 7000/6000/3500/2500	TELNET	tech	tech
3COM	HIPERARC Rev. V4.1.X	TELNET	adm	(none)
3COM	LANPLEX Rev. 2500	TELNET	debug	synnet
3COM	LANPLEX Rev. 2500	TELNET	tech	tech
3COM	LINKSWITCH Rev. 2000/2700	TELNET	tech	tech
3COM	NETBUILDER	SNMP		ANYCOM
3COM	NETBUILDER	SNMP		ILMI
3COM	NETBUILDER	MULTI	admin	(none)
3COM	OFFICE CONNECT ISDN ROUTERS Rev. 5X0	TELNET	n/a	PASSWORD
3COM	SUPERSTACK II SWITCH Rev. 2200	TELNET	debug	synnet
3COM	SUPERSTACK II SWITCH Rev. 2700	TELNET	tech	tech
3COM	OFFICECONNECT 812 ADSL	MULTI	adminttd	adminttd
3COM	WIRELESS AP Rev. ANY	MULTI	admin	comcomcom
3COM	CELLPLEX Rev. 7000	TELNET	tech	tech
3COM	CELLPLEX Rev. 7000	TELNET	admin	admin
3COM	HIPERARC Rev. V4.1.X	TELNET	adm	(none)
3COM	LANPLEX Rev. 2500	TELNET	tech	(none)
3COM	CELLPLEX	HTTP	admin	synnet

Bruteforce / Dictionary Attacks



Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type de

Attack type:

```
GET / HTTP/1.1
Host: 192.168.1.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:22.0) Gecko/20100101 Firefox/22.0 Iceweasel/22.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Authorization: Basic $YWRtaW46YWJj$
```

Pentester Academy

PentesterAcademy

a SecurityTube.net initiative



TOPICS

PRICING

WHY SUBSCRIBE

MEMBER ACCESS



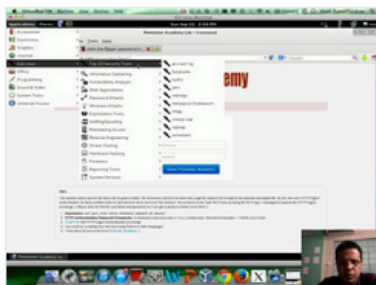
Revolutionizing Infosec Training

Highly Technical, Hands-on, Affordable

Start Learning Today!

Latest Videos

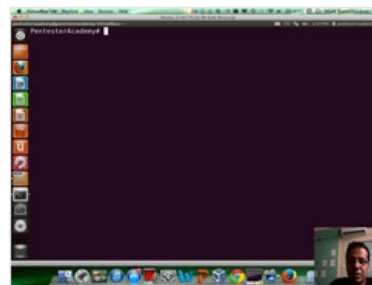
New content added weekly!



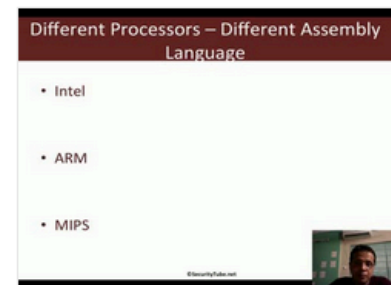
Challenge 7: Cracking Digest Authentication Solution in WAP Challenges



Challenge 7: Cracking Digest Authentication in WAP Challenges



Module 1: GDB Test Solution in x86_64 Assembly Language and Shellcoding on Linux



Module 1: CPU Information in x86_64 Assembly Language and Shellcoding on Linux